kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

Inhalt

Übersicht über Kaspersky Endpoint Security

Neuerungen in dieser Version

Vergleich der Funktionen von Kaspersky Endpoint Security, abhängig von dem Verwaltungstool für Kaspersky Security Center

App installieren und deinstallieren

- Lieferumfang
- Hardware- und Softwarevoraussetzungen
- Installation vorbereiten
- Kaspersky Endpoint Security installieren
- Anwendung für die Verwendung vorbereiten
- Kaspersky Endpoint Security deinstallieren

Erstmaliger Start der Anwendung

Anwendungsoberfläche von Kaspersky Endpoint Security

- Hauptfenster der Anwendung
- Symbol von Kaspersky Endpoint Security
- Fenster mit Anwendungseinstellungen

Über Benachrichtigungen

Lizenzverwaltung für die Anwendung Kaspersky Endpoint Security

- Über den Endbenutzer-Lizenzvertrag
- Über die Lizenz
- Über das Abo
- Über das Lizenzzertifikat
- Über den Schlüssel
- Über den Aktivierungscode
- Über die Schlüsseldatei
- Über die Bereitstellung von Daten
- Kaspersky Endpoint Security aktivieren
- Informationen zur Lizenz anzeigen
- Lizenzen und Abonnements verwalten
- Vergleich der Anwendungsfunktionalität abhängig vom Lizenztyp für Workstations

Typische Aufgaben ausführen

- Anwendung öffnen und beenden
- Status des Computerschutzes anzeigen
- Betriebsstatus der installierten Komponenten anzeigen
- Computerschutz deaktivieren und fortsetzen
- Schutz-Center verwenden
- Untersuchungsaufgaben ausführen
- Automatischen Start einer geplanten Untersuchungsaufgabe anpassen
- Anwendungsdatenbanken aktualisieren
- Vorgehen, wenn der Zugriff auf eine Datei blockiert ist
- Datei wiederherstellen, die von der Anwendung gelöscht oder desinfiziert wurde
- Anwendungsbericht anzeigen
- Was tun, wenn ein Benachrichtigungsfenster erscheint?

Erweiterte Konfiguration der Anwendung
- Schutzbereich des Computers
- Schutz vor bedrohlichen Dateien
- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Schutz vor Netzwerkbedrohungen
- Firewall
- Verhaltensanalyse
- Virensuche
- Update-Aufgaben
- Lokale Aufgaben
  - Aufgabe zur Untersuchung externer Datenträger
- Backup
- Berichte
- Managed Detection and Response
- Endpoint Detection and Response (KATA)
- Endpoint Detection and Response Optimum
  - Integration mit Endpoint Detection and Response Optimum
  - Nach Kompromittierungsindikatoren suchen
  - Datei in Quarantäne verschieben
  - Datei abrufen
  - Datei löschen
  - Prozess starten
  - Prozess beenden
  - Ausführungsprävention
  - Netzwerkisolation eines Computers
  - Cloud Sandbox
- FileVault-Volume-Verschlüsselung
- Kennwortschutz
- Exploit-Prävention
- Rollback von schädlichen Aktionen
- Web-Kontrolle
- Gerätekontrolle

An Kaspersky Security Network teilnehmen

Integrität der Anwendungskomponenten überprüfen

Anwendung über die Kaspersky Security Center Verwaltungskonsole verwalten
- Kaspersky Endpoint Security im Unternehmensnetzwerk verteilen
- Kaspersky Endpoint Security Version 11.1 oder höher auf Version 12.2 aktualisieren
- Installation von Kaspersky Endpoint Security per Fernzugriff vorbereiten
  - Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren
  - Administrationsagenten lokal installieren
  - Installieren des Administrationsagenten mithilfe von „Apple Remote Desktop“
  - Installation des Administrationsagenten unter Verwendung von Kaspersky Security Center
  - Administrationsagenten mit dem SSH-Protokoll installieren
  - Administrationsagenten lokal deinstallieren

- Administrationsagent über die Befehlszeile verwalten
  - Administrationsagent auf einem Remote-Computer starten/beenden
  - Testen Sie die Verbindung zwischen Client-Computer und Administrationsserver manuell. Tool Klnagchk
  - Einen Remote-Computer manuell mit dem Administrationsserver verbinden. Tool Klmover
  - Deinstallieren des Administrationsagenten
- Kaspersky Endpoint Security installieren und deinstallieren
  - Installation der Anwendung über das SSH-Protokoll
  - Installation der Anwendung über Kaspersky Security Center
  - Installationspaket erstellen
  - Deinstallation der Anwendung über Kaspersky Security Center
- Anwendung über Kaspersky Security Center starten oder beenden
- Aufgaben erstellen und verwalten
  - Aufgaben erstellen
  - Aufgaben manuell starten und beenden
  - Aufgaben importieren und exportieren
  - Aufgaben anzeigen
  - Aufgabenspezifische Einstellungen verwalten
- Richtlinien erstellen und verwalten
  - Richtlinie erstellen
  - Liste der Richtlinien anzeigen
  - Richtlinieneinstellungen konfigurieren
  - Richtlinienstatus ändern
  - Richtlinie in eine KLP-Datei exportieren
  - Richtlinie aus einer KLP-Datei importieren
- Richtlinienprofile erstellen und verwalten
- Bericht über erkannte Objekte generieren
- Wiederherstellungsschlüssel für einen verschlüsselten Datenträger anfordern

Remote-Verwaltung der Anwendung über Kaspersky Security Center Web Console und Cloud Console

- Web-Plug-in für Kaspersky Endpoint Security installieren
- Richtlinien erstellen
  - Einstellungen für den „Erweiterten Schutz“ anpassen
  - Einstellungen für den „Basisschutz“ anpassen
    - Einstellungen für den „Schutz vor bedrohlichen Dateien“ anpassen
    - Einstellungen für den „Schutz vor Web-Bedrohungen“ anpassen
    - Einstellungen für den „Schutz vor Netzwerkbedrohungen“ anpassen
  - Sicherheitskontrolle anpassen
  - Datenverschlüsselung anpassen
  - Einstellungen für Detection and Response konfigurieren
    - Managed Detection and Response konfigurieren
    - Endpoint Detection and Response konfigurieren
    - Endpoint Detection and Response (KATA) konfigurieren
  - Update-Einstellungen anpassen
  - Weitere Einstellungen anpassen

- Aufgaben erstellen
  - Einstellungen der Aufgabe „Untersuchung“ anpassen
  - Einstellungen der Aufgabe „Schlüssel hinzufügen“ anpassen
  - Update-Aufgabe anpassen
- Wiederherstellungsschlüssel für ein verschlüsseltes Laufwerk anfordern

Anwendung über die Befehlszeile verwalten

- Hilfe zu Befehlszeilen anzeigen
- Schadsoftware-Untersuchung ausführen
- Anwendung aktualisieren
- Rollback des letzten Updates
- Komponente oder Aufgabe starten/beenden
- Status und Statistik für eine Komponente oder Aufgabe anzeigen
- Schutzeinstellungen exportieren
- Anwendung aktivieren
- Systemerweiterung installieren
- Netzwerkverbindungen konfigurieren
- Lizenzschlüssel löschen
- Rückgabecodes der Befehlszeile
- Anwendung beenden
- Anwendung deinstallieren
- Befehle zur Verwaltung von Detection and Response
  - Ausführungsprävention verwalten
  - Netzwerkisolation verwalten

Kontaktaufnahme mit dem Technischen Support

- So erhalten Sie technische Unterstützung
- Technischer Support über Kaspersky CompanyAccount
- Informationen für den Technischen Support abrufen
- Protokolldatei verwenden
- Protokolldatei erstellen

Informationsquellen für die Anwendung

Anhänge

- Bekannte Probleme und Beschränkungen
- Liste der Objekte, die nach Erweiterung untersucht werden
- Masken für die Pfade von Dateien und Ordnern
- Anforderungen an IOC-Dateien
- Unterstützte Skriptinterpreter der Ausführungsprävention
- Zertifikat von Kaspersky Endpoint Security dem Zertifikatspeicher von Mozilla Firefox hinzufügen

Informationen über den Code von Drittherstellern

Markenrechtliche Hinweise

Übersicht über Kaspersky Endpoint Security

Kaspersky Endpoint Security schützt Computer mit dem Betriebssystem macOS vor Malware und anderen Sicherheitsbedrohungen.

Schutz vor bedrohlichen Dateien

Der „Schutz vor bedrohlichen Dateien“ schützt das Dateisystem des Computers in Echtzeit. Dazu werden alle Zugriffsversuche auf Dateien abgefangen und analysiert. Erfahren Sie mehr.

Schutz vor Web-Bedrohungen

Der „Schutz vor Web-Bedrohungen“ schützt die Informationen, die der Computer in Safari, Google Chrome™ oder Firefox™ über das HTTP- und HTTPS-Protokoll sendet und empfängt. Erfahren Sie mehr.

Schutz vor E-Mail-Bedrohungen

Der Schutz vor E-Mail-Bedrohungen untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Schadsoftware und andere bedrohliche Programme enthalten sind. Die Komponente verwendet die Anti-Malware-Datenbanken, den Cloud-Dienst Kaspersky Security Network und die heuristische Analyse, um den Computer zu schützen. Erfahren Sie mehr.

Schutz vor Netzwerkbedrohungen

Der „Schutz vor Netzwerkangriffen“ schützt das Betriebssystem vor Invasionsversuchen. Diese Komponente schützt vor Cyber-Angreifern (die Port-Scans oder Brute-Force-Methoden verwenden) und vor Schadsoftware, die von solchen Angreifern installiert wird (einschließlich Schadsoftware, die versucht, persönliche Daten an Kriminelle zu senden). Erfahren Sie mehr.

Firewall

Die Firewall blockiert nicht autorisierte Verbindungen mit dem Computer, während das Internet oder ein lokales Netzwerk verwendet wird. Außerdem kontrolliert die Firewall auch die Netzwerkaktivität von Programmen auf dem Computer. Auf diese Weise können Sie Ihr lokales Unternehmensnetzwerk vor Identitätsdiebstahl und anderen Angriffen schützen. Die Komponente verwendet die Anti-Malware-Datenbanken, den Cloud-Dienst Kaspersky Security Network sowie vordefinierte Netzwerkregeln. Erfahren Sie mehr.

Verhaltensanalyse

Die Komponente Verhaltensanalyse empfängt Informationen über die Aktionen der auf Ihrem Computer installierten Programme und stellt diese Informationen anderen Schutzkomponenten zur Verfügung, um deren Leistung zu verbessern. Außerdem führt sie die ausgewählte Aktion als Reaktion auf Malware-Aktivitäten aus. Erfahren Sie mehr.

Exploit-Prävention

Die Komponente Exploit-Prävention erkennt Programmcode, der Schwachstellen auf dem Computer ausnutzt, um Administratorrechte zu erhalten oder bösartige Aktivitäten auszuführen. Erfahren Sie mehr.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden. Erfahren Sie mehr.

Virensuche

Kaspersky Endpoint Security erkennt und neutralisiert auf Befehl Malware und andere Sicherheitsbedrohungen in einem festgelegten Untersuchungsbereich. Kaspersky Endpoint Security bietet eine vollständige Untersuchung des Computers, eine schnelle Untersuchung wichtiger Computerbereiche und die Untersuchung eines festgelegten Bereichs. Erfahren Sie mehr.

Aktualisieren

Kaspersky Endpoint Security aktualisiert die Anwendungsdatenbanken und Module von den Kaspersky-Update-Servern, den Verteilungspunkten oder aus anderen von Ihrem Systemadministrator angegebenen Quellen. Alle aktualisierten Dateien werden gesichert, damit das letzte Update bei Bedarf rückgängig gemacht werden kann. Erfahren Sie mehr.

Backup

Bevor eine infizierte Datei desinfiziert oder gelöscht wird, legt Kaspersky Endpoint Security eine Sicherheitskopie an. Dadurch können Sie diese Datei gegebenenfalls wiederherstellen. Erfahren Sie mehr.

Berichte

Kaspersky Endpoint Security erstellt Berichte über Ereignisse und Aktionen, welche die Anwendungskomponenten betreffen. Erfahren Sie mehr.

Benachrichtigungen

Kaspersky Endpoint Security informiert Sie durch Benachrichtigungen über bestimmte Ereignisse, die in Kaspersky Endpoint Security auftreten. Benachrichtigungen können von einem Tonsignal begleitet werden. Erfahren Sie mehr.

Schutz-Center

Kaspersky Endpoint Security zeigt im Schutz-Center Meldungen über den Schutzstatus an. Das Schutz-Center bietet Informationen über den Status des Computerschutzes und darüber, wie Probleme behoben und Sicherheitsbedrohungen neutralisiert werden können. Erfahren Sie mehr.

Remote-Verwaltung der Anwendung über Kaspersky Security Center

Sie können den Schutz von Computern, auf denen Kaspersky Endpoint Security installiert ist, wie folgt verwalten: Informationen über den aktuellen Schutzstatus des Computers abfragen, per Fernzugriff Probleme beheben, auf Computersicherheitsbedrohungen reagieren, Schutzkomponenten aktivieren oder deaktivieren (Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Verhaltensanalyse), Web-Kontrolle, Managed Detection and Response, Endpoint Detection and Response und Endpoint Detection and Response (KATA) aktivieren oder deaktivieren, Untersuchungsaufgaben ausführen, die Anwendungsdatenbanken aktualisieren, Startvolume-Verschlüsselung ausführen und Lizenzen und Abos für Kaspersky Endpoint Security verwalten. Sie können die folgenden Tools verwenden, um Kaspersky Endpoint Security zu verwalten:

- Kaspersky Security Center Verwaltungskonsole. Erfahren Sie mehr.
- Kaspersky Security Center Web Console und Cloud Console. Erfahren Sie mehr.

Hinweis: Die Funktionalität, die von Kaspersky Endpoint Security unterstützt wird, ist davon abhängig, welches Verwaltungstool Sie verwenden.

FileVault-Volume-Verschlüsselung

Kaspersky Endpoint Security erlaubt es, die FileVault-Verschlüsselung per Fernzugriff zu verwalten. Die Verschlüsselung verhindert, dass unbefugte Benutzer auf sensible Daten zugreifen, die sich auf dem Startvolume des Computers befinden.

Hinweis: Die Funktion FileVault-Volume-Verschlüsselung ist in Kaspersky Security Center 10 SP3 oder höher verfügbar. Weitere Informationen erhalten Sie vom Technischen Support von Kaspersky.

Web-Kontrolle

Sie können den Zugriff auf Websites, die von Benutzern besucht werden, per Fernzugriff verwalten. Sie können den Zugriff auf bestimmte Webadressen oder auf Gruppen von Webadressen erlauben oder blockieren. Außerdem können Sie den Zugriff auf bestimmte Kategorien von Websites unter Berücksichtigung des Inhalts erlauben oder blockieren. Erfahren Sie mehr.

Gerätekontrolle

Die Gerätekontrolle verwaltet den Benutzerzugriff auf Geräte, die auf dem Computer installiert oder mit dem Computer verbunden sind. Auf diese Weise können Sie den Computer vor Infektionen schützen, wenn solche Geräte angeschlossen werden, und den Verlust oder das Abfließen von Daten verhindern. Erfahren Sie mehr.

Managed Detection and Response

Die Komponente Managed Detection and Response vereinfacht die Interaktion mit dem Dienst Kaspersky Managed Detection and Response. Dieser Dienst erkennt und beseitigt kontinuierlich Sicherheitsbedrohungen, die gegen Ihr Unternehmen gerichtet sind. Erfahren Sie mehr.

Endpoint Detection and Response

Die Komponente Endpoint Detection and Response vereinfacht die Interaktion mit der Lösung Kaspersky Endpoint Detection and Response. Diese Lösung kombiniert die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren. Auf diese Weise werden fortschrittliche Angriffe effektiv abgewehrt. Zu diesen gehören neuartige Exploits, Ransomware, dateilose Angriffe sowie Methoden, die legitime Systemtools ausnutzen. Erfahren Sie mehr.

Endpoint Detection and Response (KATA)

Die Komponente Endpoint Detection and Response (KATA) vereinfacht die Interaktion mit der Lösung Kaspersky Anti Targeted Attack Platform. Diese Lösung kann komplexe Bedrohungen sofort erkennen. Dazu zählen beispielsweise gezielte Angriffe, hochentwickelte, hartnäckige Bedrohungen und Zero-Day-Angriffe. Erfahren Sie mehr.

Neuerungen in dieser Version

Diese Hilfe bezieht sich auf Kaspersky Endpoint Security for Mac Version 12.2.

Kaspersky Endpoint Security bietet die folgenden neuen Funktionen und Verbesserungen:

- Das neue macOS 27 Golden Gate wird jetzt unterstützt.
- Das neue macOS 26 Tahoe wird jetzt unterstützt.
- Wir haben die folgenden Komponenten hinzugefügt: Schutz vor E-Mail-Bedrohungen, Gerätekontrolle, Firewall, Rollback von schädlichen Aktionen und die Exploit-Prävention.
- Sie können jetzt die Komponente “Managed Detection and Response“ direkt in Kaspersky Endpoint Security aktivieren.
- Für die Alarmdetails wurde die Sichtbarkeit von Reaktionsmaßnahmen verbessert.
- Sie können jetzt die Komponente „Verhaltensanalyse“ in der Web Console verwalten.
- Wir haben Zusammenfassungen für die Alarme hinzugefügt.
- Bevor eine Reaktionsmaßnahme angewendet wird, werden Sie jetzt informiert, wenn es sich bei einem Objekt um ein systemkritisches Objekt handelt.
- Wenn Sie eine Aufgabe zur IOC-Untersuchung erstellen oder bearbeiten, können Sie die IOC-Dateien jetzt direkt in der Web Console bearbeiten.
- Sie können jetzt erkannte Objekte von den Alarmdetails in die Quarantäne verschieben.
- Für die Aufgabe zur Netzwerkisolation haben wir für eingeschränkte Aktionen Warnungen hinzugefügt.
- Allgemeine Fehlerbehebungen und Verbesserungen.

Vergleich der Funktionen von Kaspersky Endpoint Security, abhängig von dem Verwaltungstool für Kaspersky Security Center

Die Funktionalität, die von Kaspersky Endpoint Security unterstützt wird, ist davon abhängig, welches Verwaltungstool Sie verwenden (siehe folgende Tabelle).

Sie können die folgenden Tools verwenden, um Kaspersky Endpoint Security zu verwalten:

- Kaspersky Security Center Verwaltungskonsole. Snap-in für Microsoft Management Console (MMC), das am Arbeitsplatz des Administrators von Kaspersky Security Center installiert wird.
- Kaspersky Security Center Web Console. Komponente von Kaspersky Security Center, die auf dem Administrationsserver installiert wird. Für die Arbeit mit „Web Console“ können Sie einen Browser auf einem beliebigen Computer verwenden, der Zugriff auf den Administrationsserver hat.
- Kaspersky Security Center Cloud Console. Cloud-Version von Kaspersky Security Center.

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Kaspersky Security Center		
	Verwaltungskonsole	Web Console	Cloud Console
Erweiterter Schutz			
Kaspersky Security Network	✓	✓	✓
Verhaltensanalyse	✓	✓	
Exploit-Prävention	✓	✓	
Rollback von schädlichen Aktionen	✓	✓	
Basisschutz			
Schutz vor bedrohlichen Dateien	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	
Firewall	✓	✓	
Sicherheitskontrolle			
Web-Kontrolle	✓	✓	✓
Gerätekontrolle	✓	✓	
Datenverschlüsselung			
FileVault-Volume-Verschlüsselung	✓	✓	✓
Wiederherstellungsschlüssel	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	

Funktion	Kaspersky Security Center		
	Verwaltungskonsole	Web Console	Cloud Console
Endpoint Detection and Response (KATA)	✓	✓	✓
Aufgaben			
Schlüssel hinzufügen	✓	✓	✓
Aktualisieren	✓	✓	✓
Schnelle Untersuchung	✓	✓	
Rollback	✓	✓	✓
Virensuche	✓	✓	✓

App installieren und deinstallieren

Lieferumfang

Der Lieferumfang umfasst das Installationspaket für Kaspersky Endpoint Security mit folgenden Dateien:

- Dateien, mit denen die Anwendung auf unterschiedliche Weise installiert werden kann.
- Die Datei license_<loc>.txt mit dem Endbenutzer-Lizenzvertrag.
  Im Endbenutzer-Lizenzvertrag sind die Nutzungsbedingungen für die Anwendung festgelegt.

Entpacken Sie das komprimierte Installationspaket, um auf die Dateien zuzugreifen.

Hardware- und Softwarevoraussetzungen

Für Kaspersky Endpoint Security gelten folgende Hard- und Softwarevoraussetzungen:

- Prozessortyp: Intel, Apple silicon
- 4 GB Arbeitsspeicher (RAM)
- 5 GB freier Speicherplatz auf der Festplatte
- Betriebssystem macOS 13, 14, 15, 26 oder 27
- Internetverbindung

Unterstützte Browser:

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security ist mit der folgenden Virtualisierungs-Software kompatibel:

- Parallels Desktop 16 for Mac Business Edition oder höher
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

MDM-Profile können über Jamf- und Apple-Server bereitgestellt werden. Informationen zur Verwendung anderer Server finden Sie im Artikel auf der Website des Technischen Supports (Wissensdatenbank).

Sie können Kaspersky Endpoint Security per Fernzugriff über Kaspersky Security Center verwalten. Kaspersky Security Center 14.2 oder höher ist erforderlich für die Verwaltung von Kaspersky Endpoint Security mithilfe des Verwaltungs-Plug-ins für die Kaspersky Security Center-Verwaltungskonsole und des Web-Plug-ins für Kaspersky Security Center Web Console.

Hinweis: Um Kaspersky Endpoint Security for Mac 12.2 über Kaspersky Security Center zu verwalten, müssen Sie auf Remote-Computern den Administrationsagenten Version 15 installieren.

Installation vorbereiten

Bevor das Programm auf Ihrem Computer installiert wird, sind folgende Vorbereitungen erforderlich:

- Stellen Sie sicher, dass Ihr Computer die Hardware- und Softwarevoraussetzungen erfüllt.
- Entfernen Sie Kaspersky Internet Security for Mac oder andere Anti-Malware-Anwendungen, um Systemkonflikte zu vermeiden und eine maximale Systemleistung zu erzielen.

Hinweis: Bevor Kaspersky Endpoint Security per Fernzugriff installiert wird, empfehlen wir folgendes Vorgehen: Laden Sie das Archiv KES_for_macOS11_and_later.zip von der Kaspersky-Website für Technischen Support herunter und installieren Sie mithilfe des Tools Apple Remote Management das Konfigurationsprofil KES_for_macOS11_and_later_profile.mobileconfig auf dem Client-Computer. Dadurch erhält Kaspersky Endpoint Security die folgenden Berechtigungen: Berechtigungen zum Installieren der Kernel-Erweiterung und der Systemerweiterung, Festplattenvollzugriff und Berechtigungen zum Konfigurieren von Netzwerkverbindungen. Weitere Informationen über das Konfigurationsprofil und andere Optionen entnehmen Sie bitte der Webseite des Technischen Supports.

Kaspersky Endpoint Security installieren

Wichtig: Die Kaspersky-Experten empfehlen, Kaspersky Endpoint Security nur wie in dieser Hilfe beschrieben zu installieren.

Für die Installation von Kaspersky Endpoint Security bestehen folgende Möglichkeiten:

- Lokal, aus dem Installationspaket, das von der Kaspersky-Website heruntergeladen wurde.
- „Apple Remote Desktop“ per Fernzugriff verwenden.
- Per Fernzugriff über die Kaspersky Security Center Verwaltungskonsole.
- Per Fernzugriff über Kaspersky Security Center Web Console oder Kaspersky Security Center Cloud Console.

  Ausführliche Informationen über die Bereitstellung von Kaspersky-Anwendungen über die Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center. Ausführliche Informationen über die Bereitstellung von Kaspersky-Anwendungen mithilfe der Kaspersky Security Center Cloud Console finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console.

Standardinstallation von Kaspersky Endpoint Security ausführen

1. Entpacken Sie das ZIP-Archiv aus dem Installationspaket.
2. Öffnen Sie im entpackten Archiv die .dmg-Datei.
3. Doppelklicken Sie im folgenden Fenster auf **Kaspersky Endpoint Security installieren**.

   Der Installations-Assistent für Kaspersky Endpoint Security wird geöffnet.
4. Klicken Sie auf **Installieren**.
5. Um die Installation abzuschließen, folgen Sie den Schritten des Installations-Assistenten.

Nach dem Abschluss der Installation wird Kaspersky Endpoint Security automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

Hinweis: Wenn diese Installationsmethode verwendet wird, werden die Komponenten Endpoint Detection and Response (KATA), Endpoint Detection and Response (Optimum) und Cloud Sandbox nicht installiert.

Benutzerdefinierte Installation von Kaspersky Endpoint Security ausführen

1. Entpacken Sie das ZIP-Archiv aus dem Installationspaket.
2. Öffnen Sie im entpackten Archiv die .dmg-Datei.
3. Doppelklicken Sie im folgenden Fenster auf **Kaspersky Endpoint Security installieren**.

   Der Installations-Assistent für Kaspersky Endpoint Security wird geöffnet.
4. Klicken Sie auf **Anpassen**, aktivieren oder deaktivieren Sie die Kontrollkästchen der Komponenten, die nicht installiert werden sollen, und klicken Sie auf **Weiter**.
5. Um die Installation abzuschließen, folgen Sie den Schritten des Installations-Assistenten.

Nach dem Abschluss der Installation wird Kaspersky Endpoint Security automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

Kaspersky Endpoint Security mithilfe von „Apple Remote Desktop“ per Fernzugriff installieren

1. Wählen Sie auf Ihrem Mac **Apple-Menü** > **Systemeinstellungen** > **Allgemein** > **Freigaben**.
2. Aktivieren Sie das Kontrollkästchen **Entfernte Verwaltung**.
3. Installieren Sie „Apple Remote Desktop“ auf einem anderen Mac, den Sie als Server verwenden möchten. Weitere Informationen über „Apple Remote Desktop“ finden Sie bei Apple Support.
4. Öffnen Sie „Apple Remote Desktop“.
5. Klicken Sie im Fenster **Remote Desktop** auf der linken Seite auf **Scanner** und wählen Sie die Geräte aus, auf denen Sie Kaspersky Endpoint Security installieren möchten.
6. Klicken Sie auf die Schaltfläche **Installieren**.
7. Geben Sie in der Abfrage für die Anmeldedaten des Administrators einen Administratornamen und das Kennwort ein, und klicken Sie auf **Hinzufügen**.

8. Klicken Sie auf + und wählen Sie die .dmg-Datei mit dem Installationspaket für Kaspersky Endpoint Security aus.
9. Klicken Sie auf die Schaltfläche **Installieren**.

Auf den ausgewählten Geräten beginnt die Installation von Kaspersky Endpoint Security.

Anwendung für die Verwendung vorbereiten

Nach der Installation von Kaspersky Endpoint Security können Sie folgende Aktionen ausführen:

- Kaspersky Endpoint Security aktivieren. Nachdem die Anwendung aktiviert wurde, beginnt Kaspersky Endpoint Security mit dem Schutz Ihres Computers, Sie können nun die Datenbanken und Module der Anwendung regelmäßig aktualisieren, Untersuchungsaufgaben ausführen und Anfragen an den Technischen Support richten.

  Die Komponente Managed Detection and Response wird separat in der Kaspersky Security Center-Verwaltungskonsole oder Web Console aktiviert.

  Wenn die Komponente Endpoint Detection and Response von Ihrer aktuellen Lizenz nicht unterstützt wird, müssen Sie Kaspersky Endpoint Detection and Response separat aktivieren.
- Status des Computerschutzes beurteilen.
- Kaspersky Endpoint Security aktualisieren.
- Ihren Computer auf Malware untersuchen.

Kaspersky Endpoint Security deinstallieren

1. Öffnen Sie die DMG-Datei des Installationspakets der Anwendung.
2. Doppelklicken Sie im Fenster mit dem Installationspaket auf **Kaspersky Endpoint Security deinstallieren**.

   Der Uninstaller für Kaspersky Endpoint Security wird gestartet.
3. Klicken Sie im Fenster des Uninstallers auf **Löschen**.
4. Die Administrator-Anmeldedaten werden abgefragt. Geben Sie den Benutzernamen und das Kennwort des Administrators ein und bestätigen Sie, dass Sie Kaspersky Endpoint Security entfernen möchten.

   Die Deinstallation von Kaspersky Endpoint Security startet.
5. Lesen Sie die Informationen über den Abschluss der Deinstallation und klicken Sie auf **Beenden**, um den Uninstaller zu beenden.

Kaspersky Endpoint Security wurde von Ihrem Computer deinstalliert. Nachdem die Anwendung deinstalliert wurde, muss der Computer nicht neu gestartet werden.

Erstmaliger Start der Anwendung

Kaspersky Endpoint Security startet auf Ihrem Computer sofort nach der Installation. Um Ihren Mac sofort zu schützen, fordert die Anwendung Sie auf, die Grundeinstellungen anzupassen:

- Erteilen Sie die erforderlichen Berechtigungen an Kaspersky Endpoint Security, um Ihren Mac gegen Schadsoftware, Netzwerkangriffe und Internetbedrohungen zu schützen.

  Weitere Informationen über die Berechtigungen, die Sie zuteilen, erhalten Sie durch Klick auf ?.

- Kaspersky Endpoint Security aktivieren.

Wichtig: Um die Grundeinstellungen von Kaspersky Endpoint Security anzupassen, ist eine Internetverwendung erforderlich.

Kaspersky Endpoint Security zum ersten Mal starten

1. Gehen Sie im Fenster **Basisschutz** wie folgt vor, damit der „Schutz vor bedrohlichen Dateien“ und der „Schutz vor Web-Bedrohungen“ ordnungsgemäß funktionieren:

   - Wenn Sie möchten, dass die Anwendung Kaspersky Endpoint Security ordnungsgemäß funktioniert, erlauben Sie der Anwendung, alle Dateien auf Ihrem Mac zu untersuchen. Klicken Sie dazu auf **Erlauben** neben dem Eintrag Festplattenvollzugriff und folgen Sie den Anweisungen auf dem Bildschirm.

   - Wenn Sie möchten, dass Kaspersky Endpoint Security URLs und Netzwerkpakete untersucht, bevor diese Ihren Mac beschädigen können, installieren Sie die Systemerweiterung. Klicken Sie dazu auf **Installieren** neben dem Eintrag **Systemerweiterung** und folgen Sie den Anweisungen auf dem Bildschirm.

   - Erlauben Sie die Filterung von Netzwerkinhalten, damit die Systemerweiterung ordnungsgemäß funktioniert. Klicken Sie dazu auf **Erlauben** neben dem Eintrag **Filterung von Netzwerkinhalten** und folgen Sie den Anweisungen auf dem Bildschirm.

   - Wenn Sie möchten, dass Kaspersky Endpoint Security den verschlüsselten HTTPS-Datenverkehr auf Malware und Internetbedrohungen untersucht, installieren Sie das vertrauenswürdige Zertifikat. Klicken Sie dazu auf **Installieren** neben dem Eintrag **Vertrauenswürdiges Zertifikat** und folgen Sie den Anweisungen auf dem Bildschirm.

   Wichtig: Die Anwendung Kaspersky Endpoint Security wird nicht ordnungsgemäß funktionieren, wenn Sie diese Berechtigungen nicht gewähren. Sie müssen alle Berechtigungen im Fenster **Basisschutz** gewähren.

2. Klicken Sie auf **Weiter**.

Das Hauptfenster der Anwendung wird geöffnet.

Anwendungsoberfläche von Kaspersky Endpoint Security

Hauptfenster der Anwendung

Hauptfenster der Anwendung öffnen

Klicken Sie in der Menüleiste auf das Anwendungssymbol und wählen Sie **Kaspersky Endpoint Security**.

Das App-Hauptfenster von Kaspersky Endpoint Security enthält Schnittstellen-Elemente, mit denen Sie auf die wichtigsten Funktionen der App zugreifen können.

Das App-Hauptfenster ist in zwei Teile unterteilt:

- Der linke Teil enthält die Seitenleiste, mit der Sie durch die App navigieren und schnell auf die wichtigsten Funktionen zugreifen können.
- Im zentralen Bereich wird der Inhalt des Abschnitts, der in der Seitenleiste ausgewählt ist, angezeigt, und Sie können die Daten verwalten.

Seitenleiste

Die Seitenleiste des App-Hauptfensters bietet folgende Optionen:

Überwachung	Klicken Sie hier, um die Seite **Überwachung** zu öffnen. Dort finden Sie Informationen darüber, was Kaspersky Endpoint Security zum Schutz Ihres Computers unternimmt.
Schutz-Center	Klicken Sie hier, um den Schutzstatus Ihres Computers anzusehen. Erfahren Sie mehr.
Sicherheit	Klicken Sie hier, um den Betriebsstatus der installierten Komponenten anzuzeigen. Erfahren Sie mehr.
Untersuchung	Klicken Sie hier, um Untersuchungsaufgaben zu verwalten. Erfahren Sie mehr.
Update	Klicken Sie hier, um Update-Aufgaben zu verwalten. Erfahren Sie mehr.
Lizenz	Klicken Sie hier, um die App zu aktivieren oder Informationen über Ihre Lizenz anzuzeigen. Erfahren Sie mehr.

Steuerelemente der Seite **Überwachung**

Die Seite **Überwachung** zeigt den Indikator für den Schutzstatus an, informiert über die Maßnahmen von Kaspersky Endpoint Security zum Schutz Ihres Computers und enthält die unten genannten Steuerelemente.

Schutz-Center	Informiert über Probleme, die im Computerschutz vorliegen. Erfahren Sie mehr.
Berichte	Hier können Sie die Ereignisse anzeigen, die während des Betriebs der App, einzelner Komponenten und Aufgaben aufgetreten sind. Erfahren Sie mehr.

Backup	Hier können Sie eine Liste der gespeicherten Kopien von infizierten Dateien anzeigen, die von der App gelöscht wurden. Erfahren Sie mehr. Erfahren Sie mehr.
Bedrohungs-erkennung	Hier können Sie Informationen über Technologien anzeigen, die Kaspersky Endpoint Security zur Bedrohungserkennung verwendet, sowie die Anzahl der von diesen Technologien erkannten Bedrohungen.
Kaspersky Security Network	Zeigt den Status der Verbindung zwischen Kaspersky Endpoint Security und Kaspersky Security Network sowie eine globale Statistik von Kaspersky Security Network an.

Symbol von Kaspersky Endpoint Security

Das Symbol von Kaspersky Endpoint Security erscheint sofort nach der Installation in der Menüleiste. Wenn die Anwendung aktiviert ist, zeigt das Anwendungssymbol des Anwendungsstatus an. Das aktive Anwendungssymbol ( ) bedeutet, dass alle oder bestimmte Schutzkomponenten aktiviert sind. Das inaktive Anwendungssymbol ( ) bedeutet, dass alle Schutzkomponenten deaktiviert sind.

Das Menü des Anwendungssymbols öffnen

Klicken Sie in der Menüleiste auf das Anwendungssymbol.

Das Anwendungssymbol wird standardmäßig immer in der Menüleiste angezeigt. Sie können das Anwendungssymbol aus der Menüleiste entfernen.

Anwendungssymbol aus der Menüleiste entfernen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **App-Symbol** das Kontrollkästchen **In Menüleiste anzeigen**.

Wenn Sie das Anwendungsfenster öffnen, erscheint das Anwendungssymbol auch im **Dock**.

Aus dem Menü des Anwendungssymbols können Sie auf das Hauptfenster der Anwendung zugreifen und folgende Aktionen ausführen:

- Computerschutz deaktivieren.
- Computerschutz fortsetzen.
- Schutz-Center öffnen.
- Schnelle Untersuchung starten.
- Update ausführen.
- Fenster mit den Anwendungseinstellungen öffnen.
- Kaspersky Endpoint Security beenden.

Fenster mit Anwendungseinstellungen

Fenster mit den Anwendungseinstellungen öffnen

Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.
- Klicken Sie in der Menüleiste auf **Kaspersky Endpoint Security** > **Einstellungen**.
- Wenn Kaspersky Endpoint Security ausgeführt wird, klicken Sie auf das Anwendungssymbol im **Dock** und wählen Sie **Einstellungen** aus.

Schnellen Zugriff auf die Anwendungseinstellungen bieten folgende Registerkarten, die sich oben im Konfigurationsfenster befinden:

- **Basis**. Auf dieser Registerkarte können Sie den Computerschutz aktivieren oder deaktivieren und die Einstellungen für den „Schutz vor bedrohlichen Dateien“, für den „Schutz vor Web-Bedrohungen“ und für den „Schutz vor Netzwerkangriffen“ anpassen.
- **Untersuchung**. Auf dieser Registerkarte können Sie die Einstellungen für Untersuchungsaufgaben und den Startzeitplan für Untersuchungsaufgaben anpassen.
- **Bedrohungen**. Auf dieser Registerkarte können Sie die Kategorien für zu untersuchende Objekte auswählen, die Vertrauenswürdige Zone erstellen und die Backup-Einstellungen anpassen.
- **Erweitert**. Auf dieser Registerkarte können Sie der Teilnahme an Kaspersky Security Network zustimmen oder die Teilnahme ablehnen.
- **Update**. Auf dieser Registerkarte können Sie die Einstellungen für das Update der Anwendung anpassen oder zur vorherigen Version der Antiviren-Datenbanken zurückkehren.
- **Benutzeroberfläche**. Auf dieser Registerkarte können Sie die Einstellungen für das Symbol, die Benachrichtigungen und die Berichte von Kaspersky Endpoint Security anpassen sowie die Aufzeichnung von Debug-Informationen in einer Protokolldatei aktivieren oder deaktivieren.

Mit der Schaltfläche können Sie festlegen, dass die Einstellungen für Kaspersky Endpoint Security von Benutzern ohne Administratorrechte nicht bearbeitet werden dürfen. Diese Schaltfläche befindet sich im unteren Bereich des Fensters mit den Anwendungseinstellungen. Um die Einstellungen bearbeiten zu können, müssen Sie die Anmeldedaten des Administrators eingeben.

Durch Klick auf die Schaltfläche ? wird die Hilfe für Kaspersky Endpoint Security geöffnet, in der alle Einstellungen des aktuellen App-Fensters beschrieben sind. Sie können den Hilfeabschnitt für das aktive Anwendungsfenster auch mit dem Punkt **Hilfe für dieses Fenster öffnen** im Menü **Hilfe** öffnen.

Über Benachrichtigungen

Kaspersky Endpoint Security weist Sie mit Benachrichtigungen auf Anwendungsereignisse hin. Je nach Version des Betriebssystems werden die Benachrichtigungen in der Mitteilungszentrale des Betriebssystems angezeigt. Die Benachrichtigungsanzeige ist von den Benachrichtigungseinstellungen des Betriebssystems abhängig.

Ereignisse werden in Kaspersky Endpoint Security in drei Ereigniskategorien unterteilt:

- *Kritisch* – Ereignisse, die eine ernsthafte Bedrohung für die Computersicherheit darstellen (Fund von schädlichen Objekten, Schwachstellen oder Probleme in Kaspersky Endpoint Security). Kritische Ereignisse erfordern eine sofortige Reaktion. Benachrichtigungen über kritische Ereignisse sollten in keinem Fall deaktiviert werden.

- *Wichtig* – Ereignisse, die keine sofortige Reaktion erfordern, jedoch später eine Bedrohung für die Computersicherheit darstellen können.

- *Informativ* – Ereignisse, die zu Ihrer Kenntnisnahme gemeldet werden.

Benachrichtigungen deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Benachrichtigungen** das Kontrollkästchen **Benachrichtigungen aktivieren**.

Protokollierung von nicht-kritischen Ereignissen aktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Berichte** das Kontrollkästchen **Nicht-kritische Ereignisse protokollieren**, um Benachrichtigungen über informative Ereignisse von Kaspersky Endpoint Security zu erhalten.

Unabhängig davon, ob die Benachrichtigungen aktiviert oder deaktiviert sind, enthalten die Anwendungsberichte Informationen über die Ereignisse, die in Kaspersky Endpoint Security auftreten.

Benachrichtigungen können durch Tonsignale begleitet werden (z. B. Benachrichtigungen über erkannte Malware). Sie können das Tonsignal deaktivieren.

Die Aufzeichnung nicht kritischer Ereignisse vergrößert die Gesamtgröße der Berichtsdatei beträchtlich. Beachten Sie, dass diese Einstellung nur für den Schutz vor bedrohlichen Dateien gilt.

Tonsignal beim Erscheinen von Meldungsfenstern deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Benachrichtigungen** das Kontrollkästchen **Alarmton beim Fund von Malware abspielen**.

Falls eine Reaktion auf ein Ereignis erforderlich ist, zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster an. Wenn die Anwendung ein schädliches Objekt findet, können Sie das Objekt entweder löschen oder desinfizieren. Das Benachrichtigungsfenster wird erst nach Auswahl einer Aktion geschlossen.

Lizenzverwaltung für die Anwendung Kaspersky Endpoint Security

Über den Endbenutzer-Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* (Lizenzvertrag) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für die Anwendung.

Wichtig: Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie mit der Nutzung der Anwendung beginnen.

Es gibt folgende Möglichkeiten, um die Bedingungen des Endbenutzer-Lizenzvertrag einzusehen:

- Während der Installation von Kaspersky Endpoint Security.
- Im Dokument license.txt, das sich im Installationsordner der Anwendung befindet.

Wenn Sie Kaspersky Endpoint Security installieren, bestätigen Sie, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags zur Kenntnis genommen haben und akzeptieren. Wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren, brechen Sie die Installation von Kaspersky Endpoint Security ab und nutzen die Anwendung nicht.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich beschränktes Recht auf die Nutzung von Kaspersky Endpoint Security, das Ihnen auf Grundlage der Bedingungen des Lizenzvertrags (Endbenutzer-Lizenzvertrag) gewährt wird.

Der Umfang der verfügbaren Dienste und die Gültigkeitsdauer sind von der Lizenz abhängig, in deren Rahmen die App genutzt wird.

Folgende Lizenztypen sind vorgesehen:

- *Test*

  Eine kostenlose Lizenz, die zum Kennenlernen der Anwendung dient. Die Gültigkeitsdauer einer Testlizenz beträgt normalerweise nur kurze Zeit.

  Nach Ablauf einer Testlizenz werden alle Funktionen von Kaspersky Endpoint Security deaktiviert. Um die Anwendung weiterhin nutzen zu können, müssen Sie eine kommerzielle Lizenz kaufen.

  Sie können die Anwendung nur ein einziges Mal im Rahmen einer Testlizenz verwenden.

- *Kommerziell*

  Eine kostenpflichtige Lizenz.

  Wenn eine kommerzielle Lizenz abläuft, werden wichtige Funktionen der Anwendung deaktiviert. Um Kaspersky Endpoint Security weiterhin nutzen zu können, muss die kommerzielle Lizenz verlängert werden. Nach Ablauf einer kommerziellen Lizenz können Sie die Anwendung nicht mehr verwenden und müssen sie von Ihrem Gerät entfernen.

Wir empfehlen Ihnen, Ihre Lizenz rechtzeitig vor dem Ablaufdatum zu verlängern. Nur dadurch lässt sich ein ununterbrochener Schutz vor Sicherheitsbedrohungen gewährleisten.

Über das Abo

Ein *Abonnement für Kaspersky Endpoint Security* ist eine Bestellung zum Kauf der Anwendung mit bestimmten Einstellungen (Ablaufdatum, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Endpoint Security können Sie bei einem Dienstanbieter (z. B. Internetdienstanbieter) bestellen. Sie können Ihr Abo im privaten Bereich auf der Website des Dienstanbieters verwalten. Sie können Ihr Abonnement beispielsweise verlängern oder beenden, seine Dauer reduzieren oder die Anzahl der unter Ihrem Abonnement geschützten Geräte ändern.

Ein Abo kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt sein (ohne Ablaufdatum). Um Kaspersky Endpoint Security weiter nutzen zu können, nachdem ein beschränktes Abo abgelaufen ist, müssen Sie es manuell verlängern. Ein unbeschränktes Abo wird automatisch verlängert, wenn Sie den vereinbarten Betrag rechtzeitig an den Dienstleister überweisen.

Falls Sie die Anwendung mit einem beschränkten Abo nutzen, wird Ihnen beim Ablauf des Abos eine Nachfrist zur Abo-Verlängerung eingeräumt. Während der Nachfrist funktioniert die Anwendung weiterhin.

Nachdem Ihr Update-Abonnement abgelaufen und die Nachfrist zur Abo-Verlängerung verstrichen ist, funktioniert Kaspersky Endpoint Security auch weiterhin. Allerdings werden die Anwendungsdatenbanken nicht mehr aktualisiert.

Nachdem Ihr Update- und Schutz-Abonnement abgelaufen und die Nachfrist zur Abo-Verlängerung verstrichen ist, schützt Kaspersky Endpoint Security Ihren Computer nicht mehr.

Um Kaspersky Endpoint Security mit einem Abo zu nutzen, müssen Sie den Aktivierungscode hinzufügen, den Sie von Ihrem Dienstanbieter erhalten haben. Wenn Sie die Anwendung im Abo nutzen, können Sie keinen anderen Aktivierungscode verwenden, um Ihr Abo zu verlängern. Sie können erst dann einen anderen Aktivierungscode verwenden, wenn das Abo abgelaufen ist oder wenn Sie Ihr Abo kündigen. Um Ihr Abonnement zu kündigen, wenden Sie sich an den Dienstanbieter, bei dem Sie Kaspersky Endpoint Security erworben haben.

Hinweis: Ein anderer Aktivierungscode kann nur verwendet werden, wenn der aktive Schlüssel gelöscht wird. Das Abonnement enthält keine Schlüsseldatei. Sie können das Abonnement nicht als Reserveschlüssel hinzufügen. Ein Reserveschlüssel kann nicht hinzugefügt werden, wenn ein Abonnement verwendet wird.

Wenn Sie Kaspersky Endpoint Security bereits mit einer gültigen Lizenz nutzen, die Anwendung aber künftig im Abonnement verwenden möchten, dann müssen Sie den aktiven Schlüssel löschen. Anschließend können Sie die Anwendung mit einem Abonnement-Schlüssel aktivieren. Der Aktivierungscode, mit dem die Anwendung zuvor aktiviert wurde, kann auf einem anderen Computer verwendet werden.

Hinweis: Die Abo-Optionen sind vom Dienstanbieter abhängig. Manche Dienstanbieter gewähren keine Nachfrist für die Abo-Verlängerung.

Über das Lizenzzertifikat

Ein *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit einer Schlüsseldatei oder mit einem Aktivierungscode erhalten.

Ein Lizenzzertifikat enthält folgende Informationen zu einer bereitgestellten Lizenz:

- Lizenzschlüssel oder Bestellnummer
- Angaben über den Benutzer, dem die Lizenz gewährt wurde
- Informationen über die Anwendung, die mit der bereitgestellten Lizenz aktiviert werden kann
- Maximale Anzahl der Lizenzierungseinheiten (z. B. Geräte, auf denen die Anwendung mit der Lizenz verwendet werden darf)
- Startdatum der Lizenzgültigkeit
- Datum, an dem die Lizenz abläuft, oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den Schlüssel

Ein *Schlüssel* ist eine Bitsequenz, mit deren Hilfe Sie die Anwendung aktivieren können, um es dann in Übereinstimmung mit dem Endbenutzer-Lizenzvertrag zu nutzen. Schlüssel werden von den Kaspersky-Spezialisten generiert.

Mithilfe einer der folgenden Methoden können Sie der Anwendung einen Schlüssel hinzufügen: Durch Verwendung einer *Schlüsseldatei* oder durch die Eingabe eines *Aktivierungscodes*. Nachdem Sie den Schlüssel zur Anwendung hinzugefügt haben, wird er auf der Anwendungsoberfläche als individuelle alphanumerische Zeichenfolge angezeigt.

Ein Schlüssel kann von Kaspersky gesperrt werden, wenn die Bedingungen des Endbenutzer-Lizenzvertrags verletzt wurden. Falls ein Schlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um die Anwendung weiterhin nutzen zu können.

Ein Schlüssel kann entweder als aktiver Schlüssel oder als Reserveschlüssel dienen.

Ein *aktiver Schlüssel* ist ein Schlüssel, der momentan von der Anwendung verwendet wird. Ein aktiver Schlüssel kann auf eine Testlizenz, eine kommerzielle Lizenz oder ein Abo angewendet werden. Die Anwendung kann nur einen aktiven Schlüssel besitzen.

Ein *Reserveschlüssel* ist ein Schlüssel, der zur Nutzung der Anwendung berechtigt, jedoch momentan nicht verwendet wird. Der Reserveschlüssel wird automatisch aktiviert, sobald die mit dem aktuellen Schlüssel verknüpfte Lizenz abläuft. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Der Schlüssel für eine Testlizenz kann als aktiver Schlüssel hinzugefügt werden. Der Schlüssel für eine Testlizenz kann nicht als Reserveschlüssel hinzugefügt werden. Ein Reserveschlüssel kann nicht hinzugefügt werden, wenn der Testlizenzschlüssel aktiviert ist.

Über den Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Sequenz, die aus 20 Buchstaben und Ziffern besteht. Sie müssen einen Aktivierungscode eingeben, um einen Lizenzschlüssel zum Aktivieren von Kaspersky Endpoint Security hinzuzufügen. Den Aktivierungscode erhalten Sie per E-Mail, nachdem Sie Kaspersky Endpoint Security erworben oder eine Testversion von Kaspersky Endpoint Security angefordert haben.

Um die Anwendung mithilfe eines Aktivierungscodes zu aktivieren, benötigen Sie Internetzugriff für die Verbindung mit den Kaspersky-Aktivierungsservern.

Wenn Sie Ihren Aktivierungscode nach der Installation der Anwendung verloren haben, kontaktieren Sie den Kaspersky-Partner, von dem Sie die Lizenz erworben haben.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung .key, die Ihnen von Kaspersky zur Verfügung gestellt wird. Mit Schlüsseldateien wird ein Lizenzschlüssel hinzugefügt, um die Anwendung zu aktivieren.

Sie erhalten die Schlüsseldatei per E-Mail an die Adresse, die Sie beim Kauf von Kaspersky Endpoint Security oder bei der Bestellung einer Testversion von Kaspersky Endpoint Security angegeben haben.

Um die Anwendung mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung zu den Kaspersky-Aktivierungsservern erforderlich.

Wenn die Schlüsseldatei versehentlich gelöscht wurde, kann sie wiederhergestellt werden. Die Schlüsseldatei kann beispielsweise für eine Registrierung bei Kaspersky CompanyAccount erforderlich sein.

Zur Wiederherstellung der Schlüsseldatei bestehen folgende Möglichkeiten:

- Kontaktaufnahme zum Verkäufer der Lizenz.
- Anfordern einer Schlüsseldatei mithilfe Ihres Aktivierungscodes auf der Kaspersky-Website.

Über die Bereitstellung von Daten

Endbenutzer-Lizenzvertrag

Wenn Sie Kaspersky Endpoint Security mit einem Aktivierungscode aktivieren, erklären Sie sich damit einverstanden, während der Verwendung von Kaspersky Endpoint Security automatisch die folgenden Informationen bereitzustellen, damit die legale Nutzung der Anwendung überprüft werden kann und statistische Informationen über die Verteilung und Verwendung von Kaspersky-Produkten bereitgestellt werden können:

- Typ, Version und Lokalisierung der installierten Software.
- Versionen der installierten Updates.
- ID des Computers und ID der Softwareinstallation auf dem Computer.

- Aktivierungscode und einmalige Aktivierungs-ID für die aktuelle Lizenz.
- Typ, Version und Wortgröße des Betriebssystems.
- Name der virtuellen Umgebung, sofern die Anwendung in einer virtuellen Umgebung installiert ist.
- IDs der Softwarekomponenten, die zum Zeitpunkt der Informationsübermittlung aktiv sind.
- Unterstützte Datenquelle.
- Zeitüberschreitung.
- Datum und Uhrzeit auf dem Benutzercomputer.
- Protokollversion.
- Typ des Protokollinhalts.
- Länge des Protokollinhalts.
- Typ der verwendeten Datenkomprimierung.
- Typ der Signatur auf dem Aktivierungsticket.
- ID des regionalen Aktivierungscenters.
- Hash des Aktivierungscodes, berechnet mit dem SHA1-Algorithmus.
- Hash des Tickettexts, berechnet mit dem SHA1-Algorithmus.
- Erstellungszeitpunkt (Datum und Uhrzeit) des Lizenztickets.
- ID der Lizenzaktivierung.
- ID des Tickets der aktuellen Lizenz.
- Sequenz-ID des Lizenztickets.
- Datum und Uhrzeit der Lizenzaktivierung.
- Datum und Uhrzeit des Lizenzablaufs.
- Lizenzstatus.
- Lizenzversion.
- Einmalige ID des Benutzercomputers.
- Version der Lizenzticketkopfzeile.
- Anwendungsname.
- Typ der übertragenen Daten.
- Version des Schemas der übertragenen Daten.

- Vollständige Version des Betriebssystems.
- Beschreibung der verwendeten virtuellen Maschine.
- ID-Liste für kompatible Anwendungen.

Wenn Sie für den Update-Download die Kaspersky-Update-Server verwenden, stimmen Sie zu, regelmäßig die folgenden Informationen bereitzustellen, um die Effektivität des Update-Vorgangs zu erhöhen und um die Anwendung während der Aktualisierung von Datenbanken und Modulen zu identifizieren:

- Software-ID (AppID).
- ID der aktiven Lizenz.
- Einmalige ID der Software-Installation (InstallationID).
- Einmalige Start-ID der Update-Aufgabe (SessionID).
- Version der Anwendung (BuildInfo).

Erklärung zu Kaspersky Security Network (KSN).

Die Verwendung des KSN kann die Reaktionsgeschwindigkeit der Software auf Informationen sowie auf Gefährdungen der Netzwerksicherheit beschleunigen. Der erklärte Zweck wird erreicht durch:

- Ermittlung der Reputation von untersuchten Objekten.
- Identifizierung neuer und schwer erkennbarer Bedrohungen für die Informationssicherheit und deren Quellen.
- Sofortmaßnahmen zur Verbesserung des Schutzes der Daten, die vom Benutzer mithilfe des Computers gespeichert und verarbeitet werden.
- Reduzierte Wahrscheinlichkeit von Fehlalarmen.
- Erhöhte Effizienz der Anwendungskomponenten.
- Untersuchung einer Infektion auf dem Benutzercomputer.
- Verbesserung der Leistung von Kaspersky-Produkten.
- Erhalt von Referenzinformationen über die Anzahl der Objekte mit bekannter Reputation.
- Schnelle Identifizierung und Korrektur von Fehlern, die mit der Installation, Deinstallation und Aktualisierung des Produkts zusammenhängen.

Während der Verwendung von KSN empfängt und verarbeitet Kaspersky automatisch Daten. Die vom Benutzer übermittelten Daten sind abhängig vom Typ der installierten Lizenz und der angegebenen Nutzungseinstellungen für KSN.

Wenn Sie eine Lizenz für 1 bis 4 Knoten verwenden, erhält und verarbeitet Kaspersky während der KSN-Nutzung automatisch die folgenden Daten:

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; einmalige Geräte-ID Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

Wenn Sie eine Lizenz für 5 oder mehr Knoten verwenden, erhält und verarbeitet Kaspersky während der KSN-Nutzung automatisch die folgenden Daten:

- Informationen über die Version des Betriebssystems (OS) und die auf dem Computer installierten Service Packs, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems, Parameter des Funktionsmodus des Betriebssystems; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Windows Service Packs; Datum und Uhrzeit des Betriebssystemstarts; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Verhaltensanalyse-Subsystem; Anzahl der verzögerten Aktionsereignisse des Betriebssystems des aktuellen Typs; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Subsystem für den proaktiven Schutz; Anzahl der verarbeiteten Aktionsereignisse des Betriebssystems; Anzahl der verarbeiteten synchronen Aktionsereignisse des Betriebssystems; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems des aktuellen Typs; Verarbeitungsverzögerungszeit des Ereignisses über die Betriebssystemaktion im Subsystem für die persistente Ereignisspeicherung; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems; Anzahl der wartenden synchronen Aktionsereignisse des Betriebssystems; Datum und Uhrzeit des empfangenen Ereignisses über eine Aktion im Betriebssystem.

- Informationen über den fehlgeschlagenen letzten Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.

- Informationen über die installierte Anwendung des Rechtsinhabers und den Status des Antiviren-Schutzes: ID der Software-Installation (PCID) Version des Software-Datenbankeintrags; eindeutige ID der Instanz der Anwendungsinstallation auf dem Computer, Anwendungstyp, Anwendungstyp-ID, die Vollversion der installierten Anwendung, ID der Version der Anwendungseinstellungen, ID des Computertyps, eindeutige ID des Computers, auf dem die Anwendung installiert ist, eindeutige Benutzer-ID beim Dienst des Rechteinhabers, lokale Sprache und Betriebszustand, Version der installierten Softwarekomponenten und ihr Betriebszustand, Version des verwendeten Protokolls zur Verbindungsherstellung zum Dienst des Rechteinhabers; Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Anzahl der Update-Anwendungs-Zyklen für die Antiviren-Datenbanken; Zeitpunkt (Datum und Uhrzeit), an dem die Antiviren-Datenbanken zuletzt aktualisiert und angewendet wurden; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version der Software-Komponente; ID des Software-Updates; Typ der installierten Software; Startdatum und -uhrzeit vom Aktivitätsmonitor; Installationsdatum und -uhrzeit der Software; Wahrscheinlichkeit der Übermittlung von Statistiken durch den Aktivitätsmonitor; Code des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Datenbank-Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; maximal zulässige Zeit für die Verarbeitung eines Ereignisses durch den Aktivitätsmonitor; Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Gesamtzahl der Ereignisse, die länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert haben.

- Informationen über alle verarbeiteten Objekte und Vorgänge: Verdikt der Software für das verarbeitete Objekt; Verzeichniscode; Größe des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Anzahl der erkannten Software im Kontext des „Aktivitätsmonitors“; Zeitpunkt (Datum und Uhrzeit), zu dem der „Aktivitätsmonitor“ die Software erkannt hat; Erkennungscharakteristiken; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Grund, aus dem der „Aktivitätsmonitor“ die Software erkannt hat; Prüfsumme (MD5) des verarbeiteten Objekts; Ergebnis der Modul-Integritätsprüfung; Name des verarbeiteten Objekts; Typ des ausgelösten Eintrags der Antiviren-Datenbanken der Software; Speicherpfad des verarbeiteten Objekts; Name des untersuchten Objekts; Datum und Uhrzeit der Untersuchung; URL-Adresse und Referenzadresse, von denen es heruntergeladen wurde; Größe und Pfade der untersuchten Dateien; Zeichen des Archivs; Datum und Uhrzeit der Dateierstellung; Name, Größe und Prüfsummen (MD5, SHA2-256) des Packers (falls die Datei gepackt wurde); Entropie der Datei; Typ der Datei; Code des Dateityps; Zeichen, ID und Format der ausführbaren Datei; Prüfsumme des Objekts (MD5, SHA2-256); Typ und Wert der zusätzlichen Prüfsumme des Objekts; Daten über die digitale Signatur des Objekts (Zertifikat): Daten über den Herausgeber des Zertifikats, Anzahl der Starts des Objekts seit der letzten Übermittlung von Statistiken, ID der Überprüfungsaufgabe der Anwendung, Mittel zum Erhalt von Informationen über den Ruf des Objekts, Wert des Zielfilters, technische Parameter der anwendbaren Erkennungstechnologien; Speicherpfad des verarbeiteten Objekts; Verzeichniscode.

- Für ausführbare Dateien: Entropie der Dateiabschnitte, Kennzeichen der Reputations-Überprüfung oder Kennzeichen der Dateisignatur, Name, Typ, ID-Typ, Prüfsumme (MD5) und Größe der Anwendung, die vom zu validierenden Objekt geladen wurde, Anwendungspfad und Vorlagenpfade, Attribut, das das Vorhandensein in der Autostart-Liste angibt, Datum des Eintrags, Liste mit Attributen, Name des Packers, Informationen über die digitale Signatur der Anwendung: Herausgeberzertifikat, Name der hochgeladenen Datei im MIME-Format, Datum und Uhrzeit der Dateierstellung.

- Informationen über die gestarteten Anwendungen und deren Module: Prüfsummen (MD5, SHA2-256) von ausgeführten Dateien, Größe, Attribute, Erstellungsdatum, Name des Packers (falls die Datei gepackt wurde), Dateinamen, Informationen über die im System ausgeführten Prozesse (Prozess-ID (PID), Prozessname, Informationen über das Benutzerkonto, aus dem der Prozess gestartet wurde, Anwendung und Befehl, mit dem der Prozess gestartet wurde, vollständiger Pfad der Dateien des Prozesses sowie auszuführende Befehlszeile, Beschreibung der Anwendung, zu dem der Prozess gehört (Name der Anwendung und Informationen über den Herausgeber) sowie die verwendeten digitalen Zertifikate und Informationen, die zur Überprüfung ihrer Authentizität dienen, oder Informationen über das Fehlen einer digitalen Signatur einer Datei) und Informationen über die in die Prozesse geladenen Module: deren Namen, Größen, Typen, Erstellungsdaten, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfade, Header-Informationen der PE-Datei, Namen der Packer (falls die Datei gepackt wurde), Informationen über die Verfügbarkeit und Gültigkeit dieser Statistiken, ID des Modus zur Erstellung von zu sendenden Statistiken.

- Falls Bedrohungen oder Schwachstellen erkannt werden, werden zusätzlich zu den Informationen über das erkannte Objekt auch die folgenden Informationen bereitgestellt: ID, Version und Typ des Eintrags in der Antiviren-Datenbank, Name der Bedrohung, basierend auf der Klassifikation von Kaspersky, Datum und Uhrzeit der letzten Aktualisierung der Antiviren-Datenbank, Name der ausführbaren Datei, Prüfsumme (MD5) der Anwendungsdatei, welche die Webadresse, unter der die Bedrohung erkannt wurde, angefordert hat, IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, ID der Schwachstelle und ihre Gefahrenstufe, URL und Referenz der Webseite, auf der die Schwachstelle gefunden wurde.

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt.

- Informationen über einen Netzwerkangriff: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.

- Informationen zu Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, aus der der Prozess gestartet wurde, der den Port geöffnet hat, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Verbindungsports, Verbindungsstatus, Zeitstempel für das Öffnen des Ports.

- URL- und IP-Adresse der Webseite, auf der schädliche oder verdächtige Inhalte erkannt wurden, Name, Größe und Prüfsumme der Datei, die die URL anforderte, Kennung, Priorität und Grad der Regel, die für die Entscheidung verwendet wurde, Ziel des Angriffs.

- Informationen über Updates der installierten App- und Antiviren-Datenbanken: Bearbeitungsstand der Update-Aufgabe, Art des Fehlers, der möglicherweise während des Update-Vorgangs aufgetreten ist, Anzahl der fehlgeschlagenen Updates, ID der Anwendungskomponente, die die Updates ausführt.

- Informationen über die Nutzung von Kaspersky Security Network (KSN): KSN-ID, Anwendungs-ID, vollständige Version der Anwendung, anonymisierte IP-Adresse des Benutzergerätes, Indikatoren für die Qualität der Ausführung von KSN-Anfragen, Indikatoren für die Qualität der Verarbeitung von KSN-Paketen, Indikatoren für die Anzahl der KSN-Anfragen und Informationen über die Arten von KSN-Anfragen, Datum und Uhrzeit für den Beginn des Sendevorgangs von Statistiken, Datum und Uhrzeit für das Ende des Sendevorgangs von Statistiken, Informationen über die Aktualisierung der KSN-Konfiguration: ID der aktiven Konfiguration, ID der empfangenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen zu Systemprotokoll-Ereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.

- Informationen zur Bestimmung der Reputation von Dateien und URL-Adressen: URL-Adresse, unter der die Reputation angefordert wird, und Referrer, Protokolltyp der Verbindung, interne ID des Anwendungstyps, Nummer des verwendeten Ports, Benutzer-ID, Prüfsumme der untersuchten Datei (MD5), Typ der erkannten Bedrohung, Informationen über den Datensatz, der zum Erkennen der Bedrohung verwendet wurde (ID des Datensatzes für die Antiviren-Datenbanken, Zeitstempel und Typ des Datensatzes); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

- Daten zur geografischen Verteilung der Anwendung: Datum der Anwendungsinstallation und -aktivierung, ID des Partners, der die Lizenz für die Anwendungsaktivierung bereitstellt, Anwendungs-ID, Lokalisierungs-ID der Anwendungssprache, Lizenz-Seriennummer für die Anwendungsaktivierung, Merkmal für die KSN-Teilnahme.

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Informationen über die auf dem Computer installierte Hardware: Typ, Name, Modellname, Firmware-Version, Parameter der integrierten und angeschlossenen Geräte.

- Informationen über das Gerät: Geräte-ID.

- Informationen zum Betrieb der Komponente Web-Kontrolle: Komponentenversion, Kategorisierungsgrund, zusätzliche Informationen zum Kategorisierungsgrund, kategorisierte URL, Host-IP-Adresse des blockierten/kategorisierten Objekts.

Um den erklärten Zweck eines verbesserten Schutzes durch die Anwendung zu erreichen, kann Kaspersky zusätzlich Objekte empfangen, die von Angreifern dazu verwendet werden können, um den Computer zu beschädigen und Bedrohungen für die Informationssicherheit zu erstellen. Derartige Objekte sind:

- Ausführbare oder nicht-ausführbare Dateien oder Teile davon

- RAM-Bereiche des Computers

- Sektoren, die am Ladevorgang des Betriebssystems beteiligt sind

- Datenpakete für den Netzverkehr

- Webseiten und E-Mail-Nachrichten, die verdächtige oder schädliche Objekte enthalten

- Beschreibung von Klassen und Klasseninstanzen für den WMI-Speicher

- Berichte über die Anwendungsaktivität

Berichte über die Anwendungsaktivität enthalten die folgenden Informationen über Dateien und Prozesse:

- Name, Größe und Version der zu sendenden Datei, Beschreibung und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Format-ID, Name des Dateiherstellers, Name der Anwendung, zu der die Datei gehört, vollständig qualifizierter Pfad der Datei auf dem Computer und Code der Pfadvorlage, Datum und Uhrzeit der Erstellung und Aktualisierung der Datei.
- Start- und Endzeitpunkt (Datum und Uhrzeit) der Gültigkeit des Zertifikats, falls die gesendete Datei eine digitale Signatur besitzt, Zeitpunkt (Datum und Uhrzeit), zu dem das Zertifikat signiert wurde, Name des Zertifikatausstellers, Informationen zum Zertifikatsinhaber, Impression und öffentlicher Schlüssel des Zertifikats, sowie zu deren Berechnung verwendeter Algorithmus, Seriennummer des Zertifikats.
- Name des Benutzerkontos, das den Prozess ausgeführt hat.
- Prüfsummen (MD5, SHA2-256, SHA1) für den Namen des Computers, der den Prozess ausführt.
- Fenstertitel des Prozesses.
- ID der Antiviren-Datenbanken, Name der identifizierten Bedrohung gemäß der Kaspersky-Klassifizierung.
- Informationen über die für die Anwendung verwendete Lizenz; ID, Typ und Ablaufdatum der Lizenz.
- Lokale Zeit des Computers zum Zeitpunkt, zu dem die Informationen bereitgestellt wurden.
- Namen und Pfade der Dateien, auf die durch den Prozess zugegriffen wurde.
- URL und IP-Adressen, auf die durch den Prozess zugegriffen wurde.
- URL- und IP-Adressen, von denen die ausgeführte Datei heruntergeladen wurde.

Der Rechtsinhaber kann zur Erreichung des erklärten Ziels hinsichtlich der Vermeidung von Falschmeldungen außerdem vertrauenswürdige ausführbare und nicht ausführbare Dateien oder Teile davon erhalten.

Erklärung zu Kaspersky Security Network lesen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Erweitert** auf **KSN-Erklärung anzeigen**.

In einer Protokolldatei für Kaspersky Endpoint Security werden folgende Informationen gespeichert:

- Informationen über das Gerät und das Betriebssystem (einmalige Geräte-ID, Gerätetyp, MAC-Adresse der Netzwerkgeräte, Typ des Betriebssystems, Version des Betriebssystems).
- Informationen über die Funktion der Anwendung und ihrer Module.
- Informationen über das Abonnement (Abonnementtyp, Region).
- Informationen über die Sprache (Gebietsschema), Anwendungs-ID, Anpassung der Anwendung, Anwendungsversion, einmalige Installations-ID der Anwendung, einmalige Computer-ID.

- Informationen über den Status des Anti-Malware-Schutzes auf dem Computer, sowie über alle verarbeiteten und erkannten Objekte (Name des erkannten Objekts, Datum und Uhrzeit des Fundes, Webadresse, von der das Objekt heruntergeladen wurde, Namen, Größen und Pfade von infizierten Dateien, IP-Adresse des angreifenden Computers und Nummer des angegriffenen Ports des Computers, Liste der Schadsoftware-Aktivitäten und unerwünschte Webadressen), und relevante Aktionen und Entscheidungen, die von der Anwendung und vom Benutzer getroffen wurden.

- Informationen über Anwendungen, die vom Benutzer heruntergeladen wurden (Webadresse, Attribute, Dateigröße, und Informationen zum Prozess, der den Download initiiert hat).

- Informationen zu laufenden Anwendungen und Anwendungsmodulen (Größe, Attribute, Erstellungsdatum, Informationen zum PE-Header, Region, Name, Ort und Packprogramme).

- Informationen über Schnittstellenfehler und über die Nutzung der Schnittstelle der installierten Kaspersky-Anwendung.

- Informationen über Netzwerkverbindungen: IP-Adresse des Remote-Computers und des Computers des Endbenutzers, Nummern der Ports, mit denen die Verbindung hergestellt wurde, und Netzwerkprotokoll der Verbindung.

- Informationen über Netzwerkpakete, die der Computer über IT-Netzwerke und Telekommunikationsnetze empfangen und gesendet hat.

- Informationen über gesendete und empfangene E-Mail-Nachrichten und IM-Nachrichten.

- Informationen über besuchte Webadressen: Zeitpunkt, zu dem die Verbindung unter Verwendung eines offenen Protokolls hergestellt wurde, Daten über den Benutzernamen und das Kennwort für die Website, und Inhalt von Cookies.

- Öffentliches Serverzertifikat.

Protokolldateien enthalten nur die Informationen, die erforderlich sind, um Beschädigungen in der Anwendung zu reparieren. Kaspersky verwendet Ablaufverfolgungsdateien, um Ereignisse zu untersuchen, die mit Funktionsfehlern des Programms Kaspersky Endpoint Security zusammenhängen.

Die Erstellung von Protokolldateien ist standardmäßig deaktiviert. Sie können die Erstellung von Protokolldateien in den Anwendungseinstellungen aktivieren.

Ablaufverfolgungsdateien können nur manuell an Kaspersky geschickt werden. Das Programm sendet Ablaufverfolgungsdateien nicht automatisch an Kaspersky.

Sie können auswählen, auf welche Weise Ablaufverfolgungsdateien an Kaspersky geschickt werden sollen.

Bitte überprüfen Sie die Daten, die in Ablaufverfolgungsdateien enthalten sind, bevor Sie solche Dateien an Kaspersky senden.

Wichtig: Protokolldateien können persönliche oder sensible Informationen enthalten. Wenn Sie Ablaufverfolgungsdateien an Kaspersky senden, erklären Sie sich damit einverstanden, Kaspersky alle in den Protokolldateien enthaltenen Daten bereitzustellen, und Sie akzeptieren die entsprechende Versandmethode.

Für eine zusätzliche Untersuchung können außerdem Dateien (oder Dateiteile) an Kaspersky geschickt werden, die von Angreifern zur Beschädigung eines Computers oder von Daten verwendet werden können.

Alle auf diese Weise erhaltenen Informationen werden von Kaspersky entsprechend den gesetzlich vorgeschriebenen Anforderungen und den geltenden Richtlinien von Kaspersky geschützt. Die Daten werden über einen sicheren Kanal übertragen.

Die Teilnahme an Kaspersky Security Network ist freiwillig. Sie entscheiden im Verlauf der Programminstallation über die Teilnahme. Sie können diese Entscheidung jederzeit ändern.

Kaspersky Endpoint Security aktivieren

Wichtig: Vergewissern Sie sich vor der Aktivierung von Kaspersky Endpoint Security, dass das Datum und die Uhrzeit auf Ihrem Computer korrekt eingestellt sind.

Bei der Anwendungsaktivierung wird ein Schlüssel zur Anwendung hinzugefügt. Die Komponente Managed Detection and Response wird separat aktiviert. Um diese Komponente verwenden zu können, müssen Sie Kaspersky Managed Detection and Response in der Kaspersky Security Center-Verwaltungskonsole oder Web Console aktivieren.

Wenn die Komponente Endpoint Detection and Response von Ihrer aktuellen Lizenz nicht unterstützt wird, müssen Sie Kaspersky Endpoint Detection and Response separat aktivieren.

Hinweis: Für die Anwendungsaktivierung ist eine Internetverbindung erforderlich.

Testversion aktivieren

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.
3. Klicken Sie im Fenster **Lizenz** auf **Aktivieren**.

   Kaspersky Endpoint Security stellt eine Verbindung mit den Kaspersky-Aktivierungsservern her und leitet die Daten zur Überprüfung weiter. Wenn die Überprüfung erfolgreich verläuft, erhält die Anwendung einen Schlüssel für die kostenlose Testversion.

   Wichtig: Eine Testversion von Kaspersky Endpoint Security kann nur dann aktiviert werden, wenn die Anwendung auf dem Computer bisher noch nicht aktiviert worden ist.

Anwendung mit einem Aktivierungscode aktivieren

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.
3. Geben Sie im Fenster **Lizenz** den Aktivierungscode ein, den Sie beim Kauf von Kaspersky Endpoint Security erhalten haben.
4. Klicken Sie auf **Aktivieren**.

Hinweis: Der Aktivierungscode ist eine individuelle Zeichenfolge, die aus zwanzig lateinischen Buchstaben und Ziffern im Format xxxxx-xxxxx-xxxxx-xxxxx besteht.

Das Programm stellt eine Verbindung mit den Kaspersky-Aktivierungsservern her und sendet den Aktivierungscode zur Überprüfung. Wenn der Aktivierungscode erfolgreich verifiziert wird, erhält die Anwendung automatisch einen Lizenzschlüssel und fügt diesen hinzu.

Hinweis: Abhängig von dem Aktivierungscode, den Sie erhalten haben, werden Sie möglicherweise dazu aufgefordert, ein Registrierungsformular auszufüllen.

Wenn die Überprüfung des Aktivierungscodes fehlschlägt, wird eine entsprechende Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Händler, von dem Sie den Aktivierungscode erhalten haben.

Nachdem Sie die App mit dem Aktivierungscode aktiviert haben, können Sie im Fenster **Lizenz** die folgenden Informationen ansehen:

- Status der Lizenz oder des Abonnements
- Aktive Schlüssel
- Reserveschlüssel (falls vorhanden)
- Lizenztyp und Anzahl der Computer, auf denen Sie die App im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verwenden können
- App-Funktionen, die im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verfügbar sind
- Zeitpunkt (Datum und Uhrzeit), zu dem die Lizenz abläuft
- Anzahl der Tage bis zum Ablauf der Lizenz

Informationen zur Lizenz anzeigen

Informationen zur Lizenz anzeigen

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

Das Fenster **Lizenz** kann die folgenden Informationen enthalten:

- Status der Lizenz oder des Abonnements
- Aktive Schlüssel
- Reserveschlüssel (falls vorhanden)
- Lizenztyp und Anzahl der Computer, auf denen Sie die App im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verwenden können

- App-Funktionen, die im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verfügbar sind
- Zeitpunkt (Datum und Uhrzeit), zu dem die Lizenz abläuft
- Anzahl der Tage bis zum Ablauf der Lizenz

Lizenzen und Abonnements verwalten

Eine Lizenz muss verlängert werden, wenn die Lizenz, die zum aktiven Schlüssel gehört, abgelaufen und kein Reserveschlüssel vorhanden ist. Nach Ablauf der Lizenz funktioniert die Anwendung weiterhin, wobei der Funktionsumfang eingeschränkt wird (Updates, Kaspersky Security Network, Web-Kontrolle und FileVault-Volume-Verschlüsselung über Kaspersky Security Center sind nicht mehr verfügbar). Sie können weiterhin alle Programmkomponenten nutzen und Schadsoftware-Untersuchungen ausführen, allerdings nur mit den Anti-Malware-Datenbanken, die vor dem Ablauf der Lizenz installiert waren.

Wichtig: Wenn Ihre Anti-Malware-Datenbanken veraltet sind, besteht ein erhöhtes Infektionsrisiko für Ihren Computer.

Lizenz verlängern

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Schutz-Center**.

   Das Fenster **Schutz-Center** wird geöffnet.

2. Klicken Sie im Fenster **Schutz-Center** auf **Verlängern**.

   Die folgende Webseite informiert darüber, wie Sie im Kaspersky-Online-Shop oder bei einem Kaspersky-Partner Ihre Lizenz verlängern können. Wenn Sie die Lizenz über einen Online-Shop verlängern, wird nach Zahlungseingang ein Aktivierungscode für Kaspersky Endpoint Security an die im Bestellformular angegebene E-Mail-Adresse geschickt.

Wenn das Programm im Abo genutzt wird, greift Kaspersky Endpoint Security bis zum Ablauf des Abos in bestimmten Zeitabständen automatisch auf den Aktivierungsserver zu.

Wenn Sie die Anwendung in einem unbefristeten Abonnement nutzen, verlängert Kaspersky Endpoint Security Ihr Abonnement ohne Ihr Eingreifen.

Wenn Sie die Anwendung mit einem eingeschränkten Abo verwenden und die Nachfrist für die Abo-Verlängerung verstrichen ist, benachrichtigt Kaspersky Endpoint Security Sie darüber, versucht künftig nicht mehr, das Abonnement automatisch zu verlängern und aktualisiert die Anwendungsdatenbanken nicht mehr.

Sie können Ihr Abo manuell verlängern. Wenden Sie sich dazu an den Händler, bei dem Sie Kaspersky Endpoint Security erworben haben.

Abonnement verlängern

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

3. Klicken Sie im Fenster **Lizenz** auf **Website des Dienstanbieters besuchen**.

Die Website Ihres Dienstanbieters wird geöffnet.

Es kann vorkommen, dass Ihr Abo-Status veraltet ist. In diesem Fall müssen Sie den Status Ihres Abos manuell aktualisieren. Wenn Sie kein aktuelles Abonnement besitzen, stellt Kaspersky Endpoint Security die Aktualisierung der Anwendungsdatenbanken ein (wenn Sie ein Update-Abonnement besitzen) oder beendet den Computerschutz (wenn Sie ein Update- und Schutz-Abonnement besitzen).

Abo-Status aktualisieren

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.
3. Klicken Sie im Fenster **Lizenz** auf die Schaltfläche .

Vergleich der Anwendungsfunktionalität abhängig vom Lizenztyp für Workstations

Der auf Arbeitsstationen verfügbare Funktionsumfang von Kaspersky Endpoint Security ist vom Lizenztyp abhängig (s. Tabelle unten).

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Erweiterter Schutz						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Verhaltensanalyse	✓	✓	✓	✓	✓	✓
Exploit-Prävention	✓	✓	✓	✓	✓	✓
Rollback von schädlichen Aktionen	✓	✓	✓	✓	✓	✓
Basisschutz						
Schutz vor bedrohlichen Dateien	✓	✓	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓	✓	✓
Sicherheitskontrolle						
Gerätekontrolle	✓	✓	✓	✓	✓	✓
Web-Kontrolle	✓	✓	✓	✓	✓	✓
Datenverschlüsselung						
FileVault-Volume-Verschlüsselung	–	✓	✓	✓	✓	✓

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *(Die Lizenz für Kaspersky Sandbox muss separat erworben werden)*	✓	✓	✓	✓	✓	✓

Typische Aufgaben ausführen

Anwendung öffnen und beenden

Sofort nach der Installation wird das Programm automatisch gestartet und das Programmsymbol erscheint in der Menüleiste.

Anwendung öffnen

Klicken Sie in der Menüleiste auf das Anwendungssymbol und wählen Sie **Kaspersky Endpoint Security**.

Anwendung beenden

Klicken Sie in der Menüleiste auf das Anwendungssymbol und wählen Sie **Beenden**.

Wenn Sie die Anwendung beenden, wird der Anwendungsprozess aus dem Arbeitsspeicher des Computers entfernt.

Wichtig: Wenn Sie das Programm Kaspersky Endpoint Security beenden, ist der Computer nicht mehr geschützt und kann infiziert werden. Dadurch entsteht das Risiko eines Datenverlusts.

Status des Computerschutzes anzeigen

Der Indikator für den Schutzstatus, der als Schild dargestellt ist und sich im Programmhauptfenster befindet, informiert über Probleme, die im Computerschutz vorliegen. Die Farbe des Indikators ist vom Status des Computerschutzes abhängig. Wenn Kaspersky Endpoint Security Sicherheitsbedrohungen findet, erscheint im Programmhauptfenster eine entsprechende Meldung und der Indikator ändert seine Farbe.

Der Indikator kann folgende Farben annehmen:

- **Grün**. Ihr Computer ist ausreichend geschützt.

  Ein grüner Indikator bedeutet: Die Anti-Malware-Datenbanken sind auf dem neuesten Stand und alle App-Komponenten wurden gemäß den Kaspersky-Empfehlungen konfiguriert. Es wurden keine schädlichen Objekte erkannt oder alle gefundenen schädlichen Objekte wurden neutralisiert.

- **Gelb**. Das Sicherheitsniveau Ihres Computers ist eingeschränkt.

  Der gelbe Indikator weist darauf hin, dass Kaspersky Endpoint Security ein Problem erkannt hat. Als solche Probleme gelten kleinere Abweichungen von den empfohlenen Anwendungseinstellungen oder geringfügig veraltete Anwendungsdatenbanken.

- **Rot**. Für Ihren Computer besteht ein Infektionsrisiko.

  Ein roter Indikator bedeutet: Es liegt ein gefährliches Problem vor, das zu einer Infektion des Computers und zu Datenverlust führen kann. Dies kann beispielsweise der Fall sein, wenn die Anti-Malware-Datenbanken stark veraltet sind, die Anwendung nicht aktiviert ist oder schädliche Objekte gefunden wurden.

  Es wird empfohlen, alle Probleme so schnell wie möglich zu beheben und Sicherheitsbedrohungen sofort zu beseitigen.

Betriebsstatus der installierten Komponenten anzeigen

In Kaspersky Endpoint Security können Sie den Status der installierten App-Komponenten im Fenster **Sicherheit** überprüfen. Der Indikator neben dem Namen der einzelnen Komponenten zeigt den jeweiligen Status an.

Komponentenstatus anzeigen

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Sicherheit**.

   Das Fenster **Sicherheit** wird geöffnet.

Für den Indikator gibt es folgende Statusvarianten:

●	Die Komponente wird ausgeführt.
🔒	Die Komponente wird ausgeführt und wird durch eine Sicherheitsrichtlinie verwaltet.
●	Die Komponente funktioniert fehlerhaft.
🔒	Die Komponente funktioniert fehlerhaft und wird durch eine Sicherheitsrichtlinie verwaltet.
●	Die Komponente ist deaktiviert.
🔒	Die Komponente ist deaktiviert und wird durch eine Sicherheitsrichtlinie verwaltet.
⏸	Die Komponente wurde angehalten.
🔑	Die Komponente wird von der aktuellen Lizenz nicht unterstützt.

Hinweis: Bei einigen Komponenten können Sie auch das 3-Punkte-Menü neben dem Komponentennamen verwenden, um einen Bericht zu öffnen oder die Komponenteneinstellungen zu konfigurieren.

Computerschutz deaktivieren und fortsetzen

Standardmäßig wird Kaspersky Endpoint Security automatisch beim Hochfahren des Betriebssystems gestartet und schützt den Computer während der gesamten Sitzung. Alle Schutzkomponenten („Schutz vor bedrohlichen Dateien“, „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“) sind aktiviert und laufen.

Sie können den Schutz auch komplett deaktivieren oder bestimmte Schutzkomponenten ausschalten.

Wichtig: Kaspersky warnt ausdrücklich davor, den Schutz oder die Schutzkomponenten zu deaktivieren, da dies zu einer Computerinfektion und zu Datenverlust führen kann.

Bei deaktiviertem Computerschutz gilt:

- Das Anwendungssymbol in der Menüleiste ist inaktiv.
- Der Indikator für den Schutzstatus im Hauptfenster der Anwendung ist rot.

Wenn eine oder mehrere Schutzkomponenten deaktiviert sind, ist der Indikator für den Schutzstatus rot oder gelb.

Hinweis: Das Deaktivieren oder Anhalten von Schutzkomponenten besitzt keinen Einfluss auf die Untersuchungsaufgaben und die Update-Aufgabe.

Um den Computerschutz vollständig zu deaktivieren oder anzuhalten, bestehen folgende Möglichkeiten:

- Aus dem Anwendungssymbol
- Aus dem Fenster mit Anwendungseinstellungen
- Aus dem Menü **Schutz**

Computerschutz über das Anwendungssymbol deaktivieren/fortsetzen

1. Klicken Sie in der Menüleiste auf das Anwendungssymbol und wählen Sie **Schutz deaktivieren/Schutz aktivieren**.

   Wenn Sie den Schutz deaktivieren, werden die Administrator-Anmeldedaten abgefragt.

2. Geben Sie in der Abfrage für die Administrator-Anmeldedaten den Benutzernamen und das Kennwort des Administrators ein und bestätigen Sie, dass Sie den Schutz deaktivieren möchten.

Computerschutz aus dem Fenster mit Anwendungseinstellungen deaktivieren/fortsetzen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren/aktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Allgemein** das Kontrollkästchen **Schutz aktivieren**.

Computerschutz aus der Menüleiste deaktivieren/fortsetzen

Klicken Sie in der Menüleiste auf **Schutz** > **Schutz deaktivieren/Schutz aktivieren**.

Wichtig: Wenn Sie den Computerschutz deaktivieren, wird er nach einem Neustart von Kaspersky Endpoint Security nicht mehr automatisch gestartet. Sie müssen den Computerschutz manuell wieder aktivieren.

Schutzkomponente deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **<Komponentenname>** das Kontrollkästchen **<Komponentenname>aktivieren**.

Wichtig: Wenn Sie eine Schutzkomponente deaktivieren, wird sie nach dem Neustart von Kaspersky Endpoint Security nicht mehr automatisch gestartet. Sie müssen die Schutzkomponente manuell wieder aktivieren.

Schutzkomponente aktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Basis** im Abschnitt **<Komponentenname>** das Kontrollkästchen **<Komponentenname> aktivieren**.

Der Computerschutz oder die Schutzkomponenten können auch im Schutz-Center aktiviert werden. Wenn der Computerschutz deaktiviert wird oder Schutzkomponenten ausgeschaltet werden, steigt das Infektionsrisiko für Ihren Computer erheblich. Deshalb informiert das Schutz-Center Sie darüber, wenn der Computerschutz deaktiviert ist.

Schutz-Center verwenden

Das *Schutz-Center* ist eine Funktion von Kaspersky Endpoint Security, die Ihnen dabei hilft, Probleme und Sicherheitsbedrohungen zu analysieren und zu beheben.

Schutz-Center öffnen

Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Schutz-Center**.

Im Schutz-Center finden Sie Informationen über aktive Bedrohungen, können den Status der Anwendungsdatenbanken anzeigen und erfahren, ob bestimmte Schutzkomponenten deaktiviert sind.

Hinweis: Wenn der Systemadministrator Ihres Unternehmens die „Web-Kontrolle“ aktiviert, um den Zugriff auf gefährliche Webressourcen zu blockieren, zeigt Kaspersky Endpoint Security im „Schutz-Center“ die Benachrichtigung **Die Web-Kontrolle ist aktiviert** an.

Kaspersky Endpoint Security schlägt für jedes Problem und jede Bedrohung entsprechende Aktionen vor, mit denen Sie das Problem oder die Bedrohung beseitigen können. Wenn Kaspersky Endpoint Security beispielsweise infizierte Dateien auf dem Computer findet, können Sie auf **Desinfizieren** klicken. Wenn die Anti-Malware-Datenbanken veraltet sind, können Sie auf **Aktualisieren** klicken. Sie können ein Problem oder eine Bedrohung entweder sofort oder später beseitigen.

Ein Problem beheben oder eine Bedrohung beseitigen

Klicken Sie auf die Schaltfläche mit dem Namen der empfohlenen Aktion, um das Problem zu beheben oder die Bedrohung zu beseitigen.

Die Anwendung führt die ausgewählte Aktion aus.

Wenn Sie das Schutz-Center schließen und noch nicht alle gefährlichen Bedrohungen neutralisiert haben, bleibt der Statusindikator für den Computerschutz im Hauptfenster der Anwendung rot, um Sie an diese Bedrohungen zu erinnern.

Untersuchungsaufgaben ausführen

Kaspersky Endpoint Security bietet die standardmäßige Aufgabe Vollständige Untersuchung. Bei dieser Aufgabe untersucht die Anwendung den Arbeitsspeicher des Computers, die Autostart-Objekte und alle internen Laufwerke auf Viren und andere Schadsoftware.

Vollständige Untersuchung des Computers ausführen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie auf **Vollständige Untersuchung**.

Eine vollständige Untersuchung des Computers wird gestartet.

Kaspersky Endpoint Security bietet die standardmäßige Aufgabe Schnelle Untersuchung. Bei dieser Aufgabe untersucht die Anwendung wichtige Computerbereiche (Arbeitsspeicher, Autostart-Objekte und Systemordner) auf Viren und Schadsoftware.

Schnelle Untersuchung des Computers ausführen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie auf **Schnelle Untersuchung**.

Eine schnelle Untersuchung des Computers wird gestartet.

Um ein einzelnes Objekt (internes Laufwerk, Ordner, Datei oder Wechseldatenträger) auf Viren und andere Schadsoftware zu untersuchen, können Sie die Aufgabe „Benutzerdefinierte Untersuchung“ verwenden.

Ausgewähltes Element untersuchen

Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie mit der rechten Maustaste auf den ausgewählten Eintrag und wählen Sie **Auf Malware untersuchen** aus.
- Ziehen Sie ein Element auf das Anwendungssymbol im Dock.
- Ziehen Sie einen Eintrag in das Fenster **Untersuchung**.

Die Ergebnisse der abgeschlossenen Untersuchungsaufgaben können im Fenster **Berichte** eingesehen werden.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Automatischen Start einer geplanten Untersuchungsaufgabe anpassen

Sie können einen Zeitplan für den Start der Aufgaben Schnelle Untersuchung und Vollständige Untersuchung erstellen. Kaspersky Endpoint Security untersucht den gesamten Computer oder die angegebenen Computerbereiche automatisch gemäß dem festgelegten Zeitplan.

Untersuchungsaufgabe aus dem Untersuchungsfenster planen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie auf **Untersuchungszeitplan**.

   Im folgenden Dialog können Sie den Zeitplan festlegen.

3. Aktivieren Sie das Kontrollkästchen **Vollständige Untersuchung** oder **Schnelle Untersuchung**.

4. Geben Sie die Frequenz und den Startzeitpunkt der Untersuchung an.

5. Klicken Sie auf **OK**.

Untersuchungsaufgabe im Konfigurationsfenster planen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Untersuchung** auf **Zeitplan**.

3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen für den Namen der Untersuchungsaufgabe, die Sie nach Zeitplan starten möchten.

4. Passen Sie die Frequenz und den Zeitpunkt der Untersuchung an.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern, die Sie im Zeitplan der Untersuchungsaufgabe vorgenommen haben.

Die Ergebnisse der Untersuchungsaufgabe können im Fenster **Berichte** angezeigt werden.

Anwendungsdatenbanken aktualisieren

Die grundlegende Update-Quelle für Kaspersky Endpoint Security sind die dedizierten Kaspersky-Update-Server. Kaspersky Endpoint Security kann auch Verteilungspunkte, lokale Ordner oder andere Webserver als *Update-Quelle* verwenden.

Hinweis: Um Updates von den Update-Servern herunterzuladen, ist eine Internetverbindung erforderlich.

In der Grundeinstellung überprüft Kaspersky Endpoint Security regelmäßig, ob auf den Kaspersky-Update-Servern neue Updates vorliegen. Wenn auf dem Server neue Updates vorliegen, werden diese von Kaspersky Endpoint Security im Hintergrund heruntergeladen und auf dem Computer installiert.

Ein Update von Kaspersky Endpoint Security starten

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Update**.

   Das Fenster **Update** wird geöffnet.

2. Klicken Sie auf **Aktualisieren**.

Die Anwendung überprüft, ob neue Updates verfügbar sind. Wenn Updates verfügbar sind, werden sie von der Anwendung heruntergeladen und auf Ihrem Computer installiert.

Sie können die Update-Aufgabe auch wie folgt starten:

- Klicken Sie auf das Anwendungssymbol und wählen Sie **Aktualisieren** aus.
- Wählen Sie in der Menüleiste den Punkt **Schutz** > **Aktualisieren** aus.

Sie können die Methode ändern, mit der Kaspersky Endpoint Security die Anwendungsdatenbanken aktualisiert. Standardmäßig werden Datenbanken von der Anwendung automatisch aktualisiert.

Automatischen Download der Datenbanken-Updates für Kaspersky Endpoint Security aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren/deaktivieren Sie auf der Registerkarte Update im Abschnitt **Datenbanken** das Kontrollkästchen **Updates automatisch herunterladen**.

Die Ergebnisse der abgeschlossenen Update-Aufgaben können im Fenster **Berichte** eingesehen werden.

Hinweis: Die Update-Funktion (einschließlich der Bereitstellung von Anti-Malware-Signatur-Updates und Codebase-Updates) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Vorgehen, wenn der Zugriff auf eine Datei blockiert ist

Das Programm Kaspersky Endpoint Security blockiert den Zugriff auf infizierte Dateien und Anwendungen. Eine infizierte Datei muss desinfiziert werden, bevor Sie darauf zugreifen können.

Gefundenes Objekt desinfizieren

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.

2. Klicken Sie im Abschnitt **Erkannte Objekte** auf ••• neben der erforderlichen Datei und wählen Sie **Desinfizieren** aus.

   Die Anwendung beginnt mit der Desinfektion des ausgewählten Objekts. Während der Desinfektion erscheint ein Dialog, in dem Sie eine Aktion für das Objekt wählen können.

Alle gefundenen Objekte desinfizieren

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.

2. Klicken Sie im Abschnitt **Erkannte Objekte** auf **Alle desinfizieren**.

   Die Anwendung beginnt mit der Desinfektion der erkannten Objekte. Während der Desinfektion erscheint ein Benachrichtigungsfenster, in dem Sie eine Aktion für das Objekt wählen können. Wenn Sie im Benachrichtigungsfenster eine Aktion auswählen und das Kontrollkästchen **Aktion auf alle anwenden** aktivieren, wird die gleiche Aktion auf alle Dateien dieses Typs angewendet.

Wenn Sie davon überzeugt sind, dass die Dateien, die vom „Schutz vor bedrohlichen Dateien“ blockiert werden, keine Gefahr darstellen, können Sie diese Dateien zur Vertrauenswürdigen Zone hinzufügen.

Datei wiederherstellen, die von der Anwendung gelöscht oder desinfiziert wurde

Es kann vorkommen, dass durch die Desinfektion die Integrität einer Datei verletzt wird. Wenn eine desinfizierte Datei wichtige Informationen enthalten hat, die aufgrund der Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, die ursprüngliche Datei aus der Backup-Kopie wiederherzustellen.

Eine Datei wiederherzustellen, die von der Anwendung bei der Desinfektion gelöscht oder verändert wurde

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.

2. Klicken Sie im Abschnitt **Backup** neben der Datei, die wiederhergestellt werden soll, auf •••.

   Ein Pop-up-Menü wird geöffnet.

3. Wählen Sie **Datei wiederherstellen**.

   Geben Sie im nächsten Fenster den Dateinamen, den Tag und den Zielordner für die wiederherzustellende Datei an. Standardmäßig sind der ursprüngliche Dateiname und Ordner angegeben.

4. Geben Sie den Dateinamen und den Zielordner für die wiederherzustellende Datei an.

5. Klicken Sie auf **Speichern**.

Die Anwendung stellt die Datei am angegebenen Ort unter dem gewünschten Namen wieder her.

Sie sollten die Datei sofort nach der Wiederherstellung auf Malware untersuchen. Möglicherweise gelingt es, die Datei mit den aktuellen Antiviren-Datenbanken zu desinfizieren, ohne dass sie beschädigt wird.

Wichtig: Es wird davon abgeraten, Backup-Kopien von Dateien wiederherzustellen, wenn dies nicht unbedingt erforderlich ist. Eine Wiederherstellung kann zu einer Computerinfektion führen.

Anwendungsbericht anzeigen

Auf der Registerkarte **Verarbeitete Objekte** können Sie einen Kaspersky Endpoint Security-Bericht mit einer Liste aller erkannten Objekte anzeigen. Systemereignisse werden auf der Registerkarte **Systemereignisse** angezeigt. Zusätzlich wird für jede der folgenden Programmkomponenten ein separater Detailbericht erstellt: Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Verhaltensanalyse und Untersuchungs- und Update-Aufgaben.

Fenster Berichte öffnen

Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

Was tun, wenn ein Benachrichtigungsfenster erscheint?

Anwendungsbenachrichtigungen in Form von Benachrichtigungsfenstern informieren Sie über Ereignisse, die in der Anwendung auftreten und die Ihre Aufmerksamkeit erfordern.

Wenn eine Benachrichtigung auf dem Bildschirm erscheint, wählen Sie eine der vorgegebenen Varianten aus. Als optimale Variante gilt die von Kaspersky standardmäßig festgelegte Aktion.

Erweiterte Konfiguration der Anwendung

Schutzbereich des Computers

Die Objekte, die von Kaspersky Endpoint Security erkannt werden, sind nach unterschiedlichen Merkmalen in Kategorien unterteilt. Die Anwendung sucht permanent nach Viren, Würmern, Trojanern und schädlichen Tools. Diese Programme können Ihrem Computer ernsthaft beschädigen. Um den Schutz für Ihren Computer zu verbessern, können Sie die Liste der zu erkennenden Objekte erweitern. Aktivieren Sie dazu die Untersuchung legaler Software, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können.

Die Objekte, vor denen Kaspersky Endpoint Security Schutz bietet, werden wie folgt unterteilt:

- **Viren, Würmer, Trojaner, schädliche Tools, Adware und Dialer**.

  Diese Kategorie umfasst:

  - Alle Typen von Schadsoftware
  - Software, die Sie stören kann, weil sie auf Ihrem Computer Werbung (z. B. Banner) anzeigt oder die Suchergebnisse in Ihrem Browser durch Websites mit Werbung ersetzt
  - Anwendungen, die heimlich Telefonverbindungen über ein Modem herstellen

  Der Schutz vor allen Schadsoftware-Typen entspricht der minimal erforderlichen Sicherheitsstufe. Objekte aus dieser Kategorie werden gemäß den Empfehlungen von Kaspersky immer von Kaspersky Endpoint Security überwacht.

- **Legale Software, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können**. Diese Kategorie umfasst legale Software, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können. Dazu zählen beispielsweise Tools zur Fernverwaltung.

Kategorien für zu erkennende Objekte auswählen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Zu erkennende Objekte** die Kontrollkästchen für jene Objektkategorien, die erkannt werden sollen.

   Hinweis: Kaspersky Endpoint Security schützt Ihren Computer immer vor Viren, Würmern, Trojanern, schädlichen Anwendungen, Adware und Dialern. Folglich kann das Kontrollkästchen für diese Kategorie nicht deaktiviert werden.

Abhängig davon, welche Kategorien für zu erkennende Objekte ausgewählt sind, werden die Anti-Malware-Datenbanken von Kaspersky Endpoint Security entweder vollständig oder nur teilweise verwendet, wenn der Schutz vor bedrohlichen Dateien, der Schutz vor Web-Bedrohungen und die Untersuchungsaufgaben ausgeführt werden.

Hinweis: Wenn Kaspersky Endpoint Security eine Anwendung als Schadsoftware einstuft, die Sie für sicher halten, können Sie diese Anwendung zur „Vertrauenswürdigen Zone“ hinzufügen.

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste mit Objekten, die von Kaspersky Endpoint Security nicht untersucht oder überwacht werden. Beispielsweise kann es erforderlich sein, Objekte in die vertrauenswürdige Zone aufzunehmen, wenn Kaspersky Endpoint Security den Zugriff auf eine Datei, eine Anwendung oder eine Website blockiert, obwohl Sie absolut sicher sind, dass das Objekt, die Anwendung oder die Webadresse unschädlich ist.

Wenn eine Anwendung zur Vertrauenswürdigen Zone hinzugefügt wird, werden die Datei- und Netzwerkaktivitäten dieser Anwendung (einschließlich verdächtiger Aktivitäten) nicht mehr überwacht. Die ausführbaren Dateien und die Prozesse von vertrauenswürdigen Anwendungen werden weiterhin von Kaspersky Endpoint Security untersucht.

Hinweis: Wenn ein Administrator die Richtlinie so konfiguriert, dass die Bearbeitung der „Vertrauenswürdigen Zone“ verboten ist, können die Benutzer nicht auf Einstellungen der „Vertrauenswürdigen Zone“ zugreifen.

Datei oder Ordner zur Liste der vertrauenswürdigen Dateien und Ordner hinzufügen oder aus dieser Liste löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Ausnahmen** auf **Vertrauenswürdige Zone**.

   Das Fenster mit den Einstellungen für die „Vertrauenswürdige Zone“ wird geöffnet.

3. Passen Sie auf der Registerkarte **Dateien und Ordner** die Liste der vertrauenswürdigen Dateien und Ordner an:

   - Um eine Datei oder einen Ordner zur Liste hinzuzufügen:

     a. Klicken Sie auf +.

     Im folgenden Dialog können Sie eine Datei oder einen Ordner auswählen.

     b. Wählen Sie aus, welche Datei oder welcher Ordner hinzugefügt werden soll.

     c. Klicken Sie auf **Öffnen**.

   - Um eine Datei oder einen Ordner aus der Liste zu löschen:

     a. Wählen Sie ein Objekt aus der Liste der vertrauenswürdigen Dateien und Ordner aus.

     b. Klicken Sie auf –.

4. Klicken Sie auf **OK**.

Vertrauenswürdige Webadresse zur Liste der vertrauenswürdigen Webadressen hinzufügen oder aus dieser Liste löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Ausnahmen** auf **Vertrauenswürdige Zone**.

   Das Fenster mit den Einstellungen für die „Vertrauenswürdige Zone“ wird geöffnet.

   Sie können dieses Fenster auch öffnen, indem Sie im Abschnitt **Vertrauenswürdige Zone** der Registerkarte **Allgemein** auf die Schaltfläche **Basis** klicken.

3. Passen Sie auf der Registerkarte **Webadressen** die Liste der vertrauenswürdigen Webadressen an:

   - Um eine Webadresse zur Liste hinzuzufügen:

     a. Klicken Sie auf +.

     b. Geben Sie die Webadresse ein, die Sie zur Liste hinzufügen möchten.

     c. Klicken Sie auf **OK**.

   - Um eine Webadresse aus der Liste zu löschen:

     a. Wählen Sie die zu löschende Webadresse aus.

     b. Klicken Sie auf –.

4. Klicken Sie auf **OK**.

Die Liste für vertrauenswürdige Webadressen ist standardmäßig leer.

Vertrauenswürdige Anwendungen zur Liste der vertrauenswürdigen Anwendungen hinzufügen oder aus dieser Liste löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Ausnahmen** auf **Vertrauenswürdige Zone**.

   Das Fenster mit den Einstellungen für die „Vertrauenswürdige Zone“ wird geöffnet.

   Sie können dieses Fenster auch öffnen, indem Sie im Abschnitt **Vertrauenswürdige Zone** der Registerkarte **Allgemein** auf die Schaltfläche **Basis** klicken.

3. Passen Sie auf der Registerkarte **Vertrauenswürdige Anwendungen** die Liste der vertrauenswürdigen Anwendungen an:

   - So fügen Sie eine Anwendung zur Liste hinzu:

     a. Klicken Sie auf +.

     Es öffnet sich ein Fenster, in dem Sie die Parameter der gewünschten Anwendung festlegen können.

     b. Geben Sie die folgenden Parameter für die Anwendung an, die Sie hinzufügen möchten:

     - **Pfad**
     - **Anforderung an die Codesignatur**

     Hinweis: Sie können die Werte dieser beiden Parameter entweder manuell eingeben oder auf die Schaltfläche **Auswählen** klicken und im angezeigten Fenster die Anwendung auswählen, die Sie hinzufügen möchten. In diesem Fall werden die Werte für diese Parameter automatisch eingefügt.

c. Wählen Sie im Abschnitt **Optionen** mindestens einen Aktivitätstyp aus, den Kaspersky Endpoint Security nicht überwachen soll:

- **Dateiaktivität nicht überwachen**
- **Netzwerkaktivität nicht überwachen**

d. Klicken Sie auf **OK**.

- So entfernen Sie eine Anwendung aus der Liste:

a. Wählen Sie die zu löschende Anwendung aus.

b. Klicken Sie auf –.

Die Liste für vertrauenswürdige Anwendungen ist standardmäßig leer.

Vertrauenswürdige Anwendung ändern

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Ausnahmen** auf **Vertrauenswürdige Zone**.

   Das Fenster mit den Einstellungen für die „Vertrauenswürdige Zone“ wird geöffnet.

   Sie können dieses Fenster auch öffnen, indem Sie im Abschnitt **Vertrauenswürdige Zone** der Registerkarte **Allgemein** auf die Schaltfläche **Basis** klicken.

3. Wählen Sie auf der Registerkarte **Vertrauenswürdige Anwendungen** eine Anwendung aus, das Sie bearbeiten möchten.

4. Klicken Sie auf **Bearbeiten**.

5. Passen Sie im folgenden Fenster die Parameter für die Anwendung an:

6. Klicken Sie auf **OK**.

Überwachung einer vertrauenswürdigen Webadresse aktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Ausnahmen** auf **Vertrauenswürdige Zone**.

   Das Fenster mit den Einstellungen für die „Vertrauenswürdige Zone“ wird geöffnet.

3. Deaktivieren Sie auf der Registerkarte **Webadressen** das Kontrollkästchen neben der Webadresse, die von Kaspersky Endpoint Security überwacht werden soll.

4. Klicken Sie auf **OK**.

Schutz vor bedrohlichen Dateien

Der „Schutz vor bedrohlichen Dateien“ schützt das Dateisystem des Computers vor Infektionen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet und befindet sich ständig im Arbeitsspeicher des Computers. Sie untersucht alle Dateien, die auf Ihrem Computer und auf allen verbundenen Laufwerken geöffnet, gespeichert und gestartet werden, auf Malware. Wenn Sie den „Schutz vor bedrohlichen Dateien“ deaktivieren, wird diese Komponente beim Hochfahren des Betriebssystems nicht gestartet. In diesem Fall müssen Sie den „Schutz vor bedrohlichen Dateien“ manuell wieder aktivieren.

„Schutz vor bedrohlichen Dateien“ aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** das Kontrollkästchen **Schutz vor bedrohlichen Dateien aktivieren**.

   Der „Schutz vor bedrohlichen Dateien“ kann auch im Schutz-Center aktiviert werden. Wenn der Computerschutz deaktiviert wird oder Schutzkomponenten ausgeschaltet werden, steigt das Infektionsrisiko für Ihren Computer erheblich. Deshalb informiert das Schutz-Center Sie darüber, wenn der Schutz deaktiviert ist.

Sie können einen Schutzbereich für den „Schutz vor bedrohlichen Dateien“ erstellen.

Datei oder Ordner zum Schutzbereich hinzufügen oder aus dem Schutzbereich löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** auf **Schutzbereich**.

   Es wird ein Fenster mit einer Liste der Objekte geöffnet, die vom „Schutz vor bedrohlichen Dateien“ untersucht werden. Standardmäßig untersucht der „Schutz vor bedrohlichen Dateien“ alle Objekte, die sich auf mit dem Computer verbundenen internen Laufwerken, Wechseldatenträgern und Netzlaufwerken befinden.

   > **Hinweis:** Sie können die Untersuchung des schreibgeschützten Systemvolume überspringen und dadurch die Untersuchungsdauer wesentlich reduzieren. Standardmäßig untersucht „Datei-Anti-Virus“ das schreibgeschützte Systemvolume nicht.

3. Fügen Sie im Abschnitt **Schutzbereich** Objekte zum Schutzbereich hinzu oder löschen Sie Objekte aus dem Schutzbereich:

   - Um eine Datei oder einen Ordner zum Schutzbereich hinzuzufügen:

     a. Klicken Sie auf +.

        Es wird ein Pop-up-Menü geöffnet, in dem Sie Objekte zum Schutzbereich hinzufügen können.

     b. Wählen Sie im Pop-up-Menü den Eintrag **Dateien und Ordner** aus.

        Im folgenden Dialog können Sie eine Datei oder einen Ordner auswählen.

c. Wählen Sie aus, welche Datei oder welcher Ordner zum Schutzbereich hinzugefügt werden soll.

d. Klicken Sie auf **Öffnen**.

- Um eine Datei oder einen Ordner aus dem Schutzbereich zu löschen:

  a. Wählen Sie in der Liste des Schutzbereichs ein Objekt aus.

  b. Ziehen Sie das ausgewählte Objekt aus dem Fenster heraus oder klicken Sie auf –.

4. Wenn Sie das schreibgeschützte Systemvolume untersuchen möchten, deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen **Schreibgeschütztes Systemvolume bei der Untersuchung überspringen**.

   Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

5. Klicken Sie auf **Speichern**.

Objekt aus der Liste der standardmäßigen Objekte zum Schutzbereich hinzufügen oder aus dem Schutzbereich löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** auf **Schutzbereich**.

   Es wird ein Fenster mit einer Liste der Objekte geöffnet, die vom „Schutz vor bedrohlichen Dateien“ untersucht werden. Standardmäßig untersucht der „Schutz vor bedrohlichen Dateien“ alle Objekte, die sich auf mit dem Computer verbundenen internen Laufwerken, Wechseldatenträgern und Netzlaufwerken befinden.

   Hinweis: Sie können die Untersuchung des schreibgeschützten Systemvolume überspringen und dadurch die Untersuchungsdauer wesentlich reduzieren. Standardmäßig untersucht „Datei-Anti-Virus“ das schreibgeschützte Systemvolume nicht.

3. Fügen Sie im Abschnitt **Schutzbereich** Objekte auf der Liste der standardmäßigen Objekte zum Schutzbereich hinzu oder löschen Sie Objekte aus dem Schutzbereich:

   - Objekt aus der Liste der standardmäßigen Objekte zum Schutzbereich hinzufügen:

     a. Klicken Sie auf +.

     Es wird ein Pop-up-Menü geöffnet, in dem Sie Objekte zum Schutzbereich hinzufügen können.

     b. Wählen Sie im Pop-up-Menü ein Objekt aus, das zum Schutzbereich hinzugefügt werden soll (z. B. **Alle internen Datenträger**).

   - Objekt aus der Liste der standardmäßigen Objekte aus dem Schutzbereich löschen:

     a. Wählen Sie in der Liste des Schutzbereichs ein Objekt aus.

     b. Ziehen Sie das ausgewählte Objekt aus dem Fenster heraus oder klicken Sie auf –.

4. Wenn Sie das schreibgeschützte Systemvolume untersuchen möchten, deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen **Schreibgeschütztes Systemvolume bei der Untersuchung überspringen**.

   Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

5. Klicken Sie auf **Speichern**.

Schutz für ein Objekt im Schutzbereich deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** auf **Schutzbereich**.

   Es wird ein Fenster mit einer Liste der Objekte geöffnet, die vom „Schutz vor bedrohlichen Dateien“ untersucht werden. Standardmäßig untersucht der „Schutz vor bedrohlichen Dateien“ alle Objekte, die sich auf mit dem Computer verbundenen internen Laufwerken, Wechseldatenträgern und Netzlaufwerken befinden.

   Hinweis: Sie können die Untersuchung des schreibgeschützten Systemvolume überspringen und dadurch die Untersuchungsdauer wesentlich reduzieren. Standardmäßig untersucht „Datei-Anti-Virus“ das schreibgeschützte Systemvolume nicht.

3. Deaktivieren Sie in der Liste des Schutzbereichs das Kontrollkästchen für das entsprechende Objekt.

4. Klicken Sie auf **Speichern**.

Untersuchung des schreibgeschützten Systemvolume aktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** auf **Schutzbereich**.

   Es wird ein Fenster mit einer Liste der Objekte geöffnet, die vom „Schutz vor bedrohlichen Dateien“ untersucht werden. Standardmäßig untersucht der „Schutz vor bedrohlichen Dateien“ alle Objekte, die sich auf mit dem Computer verbundenen internen Laufwerken, Wechseldatenträgern und Netzlaufwerken befinden.

   Hinweis: Sie können die Untersuchung des schreibgeschützten Systemvolume überspringen und dadurch die Untersuchungsdauer wesentlich reduzieren. Standardmäßig untersucht „Datei-Anti-Virus“ das schreibgeschützte Systemvolume nicht.

3. Deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen **Schreibgeschütztes Systemvolume bei der Untersuchung überspringen**.

   Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

4. Klicken Sie auf **Speichern**.

Wenn Sie oder eine Anwendung versuchen, auf eine Datei zuzugreifen, die zum Schutzbereich gehört, so überprüft der „Schutz vor bedrohlichen Dateien“, ob die Datei in den iSwift-Datenbanken verzeichnet ist, und entscheidet aufgrund dieser Informationen, ob die Datei untersucht werden muss.

Schädliche Objekte werden mithilfe der *Signaturanalyse* erkannt. Dabei wird auf Basis von Schadsoftware-Beschreibungen aus den Anti-Malware-Datenbanken nach Bedrohungen gesucht. Neben der Signaturanalyse setzt der „Schutz vor bedrohlichen Dateien“ auch eine heuristische Analyse und weitere Untersuchungstechnologien ein.

Wenn in einer Datei eine Bedrohung gefunden wird, identifiziert Kaspersky Endpoint Security den Typ der Schadsoftware (beispielsweise als *Virus* oder *Trojaner*). Anschließend wird eine Benachrichtigung über das erkannte Objekt angezeigt und die Anwendung führt mit dem Objekt die Aktion aus, die in den Einstellungen für den „Schutz vor bedrohlichen Dateien“ festgelegt ist.

Aktion auswählen, die der „Schutz vor bedrohlichen Dateien“ beim Fund einer infizierten Datei ausführen soll

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor bedrohlichen Dateien** aus, welche Aktion der „Schutz vor bedrohlichen Dateien“ ausführen soll, nachdem eine infizierte Datei gefunden wurde.

Bevor Kaspersky Endpoint Security versucht, eine infizierte Datei zu desinfizieren oder zu löschen, wird eine Backup-Kopie davon angelegt, um eine spätere Wiederherstellung oder Desinfektion zu ermöglichen.

Informationen über den „Schutz vor bedrohlichen Dateien“ und über alle erkannten Objekte werden in einem Bericht aufgezeichnet.

Hinweis: Wenn die Komponente „Schutz vor bedrohlichen Dateien“ mit einem Fehler beendet wurde, können Sie den Bericht überprüfen und versuchen, die Komponente neu zu starten. Sollte das Problem weiterhin bestehen, so können Sie sich an den Technischen Support von Kaspersky wenden.

Bericht über den „Schutz vor bedrohlichen Dateien“ anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Schutz vor bedrohlichen Dateien**.

Schutz vor Web-Bedrohungen

Wenn Sie das Internet verwenden, besteht für Ihren Computer das Risiko einer Infektion durch Malware und andere Sicherheitsbedrohungen. Sicherheitsbedrohungen können in Ihren Computer eindringen, während Sie kostenlose Programme herunterladen oder Websites besuchen, die von Hackern kompromittiert worden sind. Außerdem können Würmer Ihren Computer direkt beim Aufbau einer Internetverbindung angreifen, noch bevor eine Webseite geöffnet oder eine Datei heruntergeladen wird.

Kaspersky Endpoint Security schützt die Informationen, die Ihr Computer in Safari, Chrome oder Firefox über das HTTP- und HTTPS-Protokoll sendet und empfängt.

Hinweis: Kaspersky Endpoint Security überwacht den Web-Datenverkehr auf jenen Ports, die am häufigsten für die Datenübertragung mit dem HTTP- und HTTPS-Protokoll dienen. Verschlüsselte Verbindungen (HTTPS) werden nur dann von Kaspersky Endpoint Security untersucht, wenn das Kontrollkästchen **Sichere Verbindungen (HTTPS) untersuchen** im Abschnitt **Allgemein** aktiviert ist.

„Schutz vor Web-Bedrohungen“ aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor Web-Bedrohungen** das Kontrollkästchen **Schutz vor Web-Bedrohungen aktivieren**.

Der „Schutz vor Web-Bedrohungen“ kann auch im Schutz-Center aktiviert werden. Wenn der Computerschutz deaktiviert wird oder Schutzkomponenten ausgeschaltet werden, steigt das Infektionsrisiko für Ihren Computer erheblich. Deshalb informiert das Schutz-Center Sie darüber, wenn der Schutz deaktiviert ist.

Wichtig: Wenn Sie den „Schutz vor Web-Bedrohungen“ deaktivieren, wird er nach einem Neustart von Kaspersky Endpoint Security oder nach einem Neustart des Betriebssystems nicht mehr automatisch gestartet. In diesem Fall müssen Sie den „Schutz vor Web-Bedrohungen“ manuell wieder aktivieren.

Bei der Untersuchung des Web-Datenverkehrs verwendet der „Schutz vor Web-Bedrohungen“ die von Kaspersky empfohlenen Einstellungen. Zur Erkennung schädlicher Objekte werden Signaturanalyse, heuristische Analyse und Daten aus Kaspersky Security Network eingesetzt.

Wenn überprüft wird, ob Links auf Websites Phishing-Bedrohungen oder bösartige Webadressen sind, können *Phishing-Angriffe* verhindert werden. Für *Phishing-Angriffe* verwenden Kriminelle gewöhnlich E-Mails, die scheinbar von Kreditinstituten (z. B. Banken) stammen und Links zu betrügerischen Websites enthalten. In diesen E-Mails versuchen Kriminelle, den Benutzer zu überlisten, damit er eine Phishing-Website besucht und vertrauliche Daten (wie Bankkartennummer oder Benutzername und Kennwort für ein Online-Banking-Konto) eingibt. Ein Phishing-Angriff kann als eine Nachricht getarnt sein, die von Ihrer Bank stammt und einen Link zur offiziellen Bank-Website enthält. In Wirklichkeit führt der Link aber zu einer exakten Kopie der offiziellen Bank-Website, die von Betrügern erstellt wurde.

Der „Schutz vor Web-Bedrohungen“ überwacht Ihren Web-Datenverkehr auf Versuche zum Öffnen von Phishing-Websites und blockiert den Zugriff auf solche Websites. Um zu überprüfen, ob die Links auf Websites Phishing-Bedrohungen und bösartige Webadressen enthalten, verwendet Kaspersky Endpoint Security die Anwendungsdatenbanken, die heuristische Analyse und Daten aus Kaspersky Security Network.

Algorithmus für die Untersuchung des Web-Datenverkehrs

Jede Website oder Datei, auf die Sie oder eine Anwendung über das HTTP- oder HTTPS-Protokoll zugreifen, wird vom „Schutz vor Web-Bedrohungen“ abgefangen und auf schädlichen Code untersucht:

- Wenn eine Website oder eine Datei schädlichen Code enthält, kann Kaspersky Endpoint Security das Objekt blockieren und Sie darüber benachrichtigten, dass die angeforderte Datei oder Website infiziert ist.
- Wenn die Website oder Datei keinen schädlichen Code enthält, können Sie sofort darauf zugreifen.

Aktion auswählen, die der „Schutz vor Web-Bedrohungen“ beim Fund eines gefährlichen Objekts im Web-Datenverkehr ausführen soll

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor Web-Bedrohungen** aus, welche Aktion der „Schutz vor Web-Bedrohungen“ beim Fund eines gefährlichen Objekts im Web-Datenverkehr ausführen soll.

Informationen über den „Schutz vor Web-Bedrohungen“ sowie über alle gefährlichen Objekte, die im Web-Datenverkehr gefunden wurden, werden in einem Bericht aufgezeichnet.

Hinweis: Wenn der „Schutz vor Web-Bedrohungen“ mit einem Fehler beendet wurde, können Sie den Bericht für den „Schutz vor Web-Bedrohungen“ überprüfen und versuchen, die Komponente neu zu starten. Sollte das Problem weiterhin bestehen, so können Sie sich an den Technischen Support von Kaspersky wenden.

Bericht über den „Schutz vor Web-Bedrohungen“ anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Schutz vor Web-Bedrohungen**.

Schutz vor E-Mail-Bedrohungen

Die Komponente Schutz vor E-Mail-Bedrohungen untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Schadsoftware und andere bedrohliche Programme enthalten sind. Die Komponente verwendet die Anti-Malware-Datenbanken, den Cloud-Dienst Kaspersky Security Network und die heuristische Analyse, um den Computer zu schützen.

Die Anwendung unterstützt die folgenden E-Mail-Clients: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ for Gmail, Spike mail.

Der Schutz vor E-Mail-Bedrohungen ist standardmäßig aktiviert. Bei Bedarf können Sie den Schutz vor E-Mail-Bedrohungen deaktivieren.

Schutz vor E-Mail-Bedrohungen aktivieren/deaktivieren (über die Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Basisschutz** > **Schutz vor E-Mail-Bedrohungen**.

5. Aktivieren/deaktivieren Sie den Schalter **Schutz vor E-Mail-Bedrohungen**.

6. Wenn der Schutz vor E-Mail-Bedrohungen aktiviert ist, wählen Sie aus, welche Aktion die Anwendung beim Fund von Schadsoftware ausführen soll:

   - **Löschen**
   - **Blockieren**

7. Konfigurieren Sie bei Bedarf im Abschnitt **Erweiterte Einstellungen** das Zeitlimit für die Untersuchung von Archiven oder die maximale Größe eines zu untersuchenden Archivs.

8. Speichern Sie die Änderungen.

Schutz vor E-Mail-Bedrohungen aktivieren/deaktivieren (über die Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.

2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.

3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.

4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.

6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Basisschutz** > **Schutz vor E-Mail-Bedrohungen** aus.

7. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren**.

8. Wählen Sie im Abschnitt **Aktion beim Fund einer Bedrohung** aus, welche Aktion ausgeführt werden soll, wenn Kaspersky Endpoint Security eine Bedrohung erkennt.

9. Konfigurieren Sie bei Bedarf im Abschnitt **Schutz vor E-Mail-Bedrohungen: Einstellungen** das Zeitlimit für die Untersuchung von Archiven oder die maximale Größe eines zu untersuchenden Archivs.

10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

11. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.
    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Schutz vor E-Mail-Bedrohungen aktivieren/deaktivieren (über die Anwendung Kaspersky Endpoint Security)

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren oder deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor E-Mail-Bedrohungen** das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren**.

3. Wenn das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren** aktiviert ist, wählen Sie aus, welche Aktion ausgeführt werden soll, wenn Kaspersky Endpoint Security eine Bedrohung erkennt.

4. Konfigurieren Sie bei Bedarf das Zeitlimit für die Untersuchung von Archiven oder die maximale Größe eines zu untersuchenden Archivs.

Bericht für den Schutz vor E-Mail-Bedrohungen anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Schutz vor E-Mail-Bedrohungen**.

Schutz vor Netzwerkbedrohungen

Kaspersky Endpoint Security schützt Ihren Computer vor Netzwerkangriffen.

Bei einem *Netzwerkangriff* wird versucht, in das Betriebssystem eines Remote-Computers einzudringen. Mithilfe von Netzwerkangriffen versuchen Kriminelle, die Kontrolle über ein Betriebssystem zu übernehmen, das Betriebssystem zum Absturz zu bringen oder auf sensible Informationen zuzugreifen. Zu diesem Zweck führen Kriminelle entweder direkte Angriffe wie Port-Scanning oder Brute-Force-Angriffe aus oder sie verwenden Schadsoftware, die zuvor auf dem angegriffenen Computer installiert wurde.

Netzwerkangriffe lassen sich bedingt in folgende Kategorien unterteilen:

- *Port-Scanning*. Netzwerkangriffe dieser Art dienen gewöhnlich der Vorbereitung von gefährlicheren Angriffe. Ein Angreifer scannt die UDP-/TCP-Ports, die auf dem angegriffenen Computer von Netzwerkdiensten verwendetet werden, und stellt fest, ob der angegriffene Computer für gefährlichere Netzwerkattacken anfällig ist. Mithilfe von Port-Scans kann der Angreifer auch ermitteln, welches Betriebssystem auf dem angegriffenen Computer installiert ist, um dann relevante Netzwerkangriffe einzusetzen.

- *DoS-Angriffe* oder Netzwerkangriffe, die zur Dienstverweigerung führen. Solche Netzwerkangriffe destabilisieren das angegriffene Betriebssystem oder setzen es vollständig außer Gefecht.

  Die wichtigsten Arten von DoS-Angriffen sind:

  - Übertragung von speziellen Netzwerkpaketen, die der Zielcomputer nicht erwartet und die im angegriffenen Betriebssystem zu Störungen oder zum Absturz führen.

  - An einen Remote-Computer werden innerhalb eines kurzen Zeitraums sehr viele Netzwerkpakete geschickt. Der Zielcomputer setzt seine gesamten Ressourcen ein, um die vom Angreifer gesendeten Netzwerkpakete zu verarbeiten. Deshalb kann der Computer seine eigentlichen Funktionen nicht mehr ausführen.

- *Invasions-Netzwerkangriffe*. Das Ziel dieser Netzwerkangriffe ist es, das Betriebssystem des angegriffenen Computers zu „kapern“. Dies ist die gefährlichste Art von Netzwerkangriffen, da der Angreifer bei erfolgreichem Angriff das Betriebssystem vollständig kontrollieren kann.

  Diese Art von Netzwerkangriffen wird von Kriminellen verwendet, um vertrauliche Daten aus einem Remote-Computer zu stehlen (beispielsweise Bankkartennummern oder Kennwörter) oder um den Remote-Computer heimlich für eigene Zwecke zu nutzen (beispielsweise um von einem gekaperten Computer aus andere Computer anzugreifen).

„Schutz vor Netzwerkbedrohungen“ aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor Netzwerk- bedrohungen** das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**.

Der „Schutz vor Netzwerkbedrohungen“ kann auch im Schutz-Center aktiviert werden. Wenn der Computerschutz deaktiviert wird oder Schutzkomponenten ausgeschaltet werden, steigt das Infektionsrisiko für Ihren Computer erheblich. Deshalb informiert das Schutz-Center Sie darüber, wenn der Schutz deaktiviert ist.

Wichtig: Wenn Sie den „Schutz vor Netzwerkbedrohungen“ deaktivieren, wird er nach einem Neustart von Kaspersky Endpoint Security oder nach einem Neustart des Betriebssystems nicht mehr automatisch gestartet. In diesem Fall müssen Sie den „Schutz vor Netzwerkbedrohungen“ aktivieren manuell wieder aktivieren.

Wenn Kaspersky Endpoint Security eine gefährliche Netzwerkaktivität erkennt, wird die IP-Adresse des angreifenden Computers automatisch auf die Liste der blockierten Computer gesetzt. Eine Ausnahme gilt nur für angreifende Computer, die auf der Liste der vertrauenswürdigen Computer stehen.

Liste für blockierte Computer ändern

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor Netzwerk- bedrohungen** das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**.

3. Klicken Sie auf **Einstellungen**.

   Das folgende Fenster enthält eine Liste der vertrauenswürdigen Computer und eine Liste der blockierten Computer.

4. Öffnen Sie die Registerkarte **Blockierte Computer**.

5. Wenn Sie sicher sind, dass der blockierte Computer keine Bedrohung darstellt, wählen Sie in der Liste die IP-Adresse des Computers aus und klicken Sie auf **Freigeben**.

   Ein Bestätigungsdialog wird geöffnet.

6. Wählen Sie im Bestätigungsdialog eine der folgenden Varianten aus:

   - Wenn Sie den Computer freigeben möchten, klicken Sie auf **Freigeben**.

     Kaspersky Endpoint Security entsperrt die IP-Adresse.

   - Wenn Kaspersky Endpoint Security die markierte IP-Adresse in Zukunft nicht mehr blockieren soll, klicken Sie auf **Freigeben und zu Ausnahmen hinzufügen**.

     Kaspersky Endpoint Security entsperrt die IP-Adresse und fügt sie zur Liste der vertrauenswürdigen Computer hinzu.

7. Klicken Sie auf **Speichern**.

Sie können eine Liste mit vertrauenswürdigen Computern erstellen und ändern. Die IP-Adressen dieser Computer werden vom Programm Kaspersky Endpoint Security auch dann nicht automatisch blockiert, wenn eine gefährliche Netzwerkaktivität dieses Computers erkannt wurde.

Liste für vertrauenswürdige Computer ändern

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Schutz vor Netzwerk- bedrohungen** das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**.

3. Klicken Sie auf **Einstellungen**.

   Das folgende Fenster enthält eine Liste der vertrauenswürdigen Computer und eine Liste der blockierten Computer.

4. Öffnen Sie die Registerkarte **Vertrauenswürdige Computer**.

5. Passen Sie die Liste für vertrauenswürdige Computer an:

   - Um eine IP-Adresse zur Liste für vertrauenswürdige Computer hinzuzufügen:

     a. Klicken Sie auf +.

     b. Tagen Sie die IP-Adresse des vertrauenswürdigen Computers in das eingeblendete Feld ein.

   - Um eine IP-Adresse aus der Liste für vertrauenswürdige Computer zu löschen:

     a. Wählen Sie eine IP-Adresse aus der Liste aus.

     b. Klicken Sie auf –.

   - Um eine IP-Adresse in der Liste für vertrauenswürdige Computer zu ändern:

     a. Wählen Sie eine IP-Adresse aus der Liste aus.

     b. Klicken Sie auf **Bearbeiten**.

     c. Ändern Sie die IP-Adresse.

6. Klicken Sie auf **Speichern**.

Wenn ein Netzwerkangriff erkannt wurde, speichert Kaspersky Endpoint Security Informationen über den Angriff in einem Bericht.

Hinweis: Wenn die Komponente „Schutz vor Netzwerkbedrohungen“ mit einem Fehler beendet wurde, können Sie den Bericht überprüfen und versuchen, die Komponente neu zu starten. Sollte das Problem weiterhin bestehen, so können Sie sich an den Technischen Support von Kaspersky wenden.

Bericht über den „Schutz vor Netzwerkbedrohungen“ anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Schutz vor Netzwerkbedrohungen**.

Firewall

Die Firewall blockiert nicht autorisierte Verbindungen mit dem Computer, während das Internet oder ein lokales Netzwerk verwendet wird. Außerdem kontrolliert die Firewall auch die Netzwerkaktivität von Programmen auf dem Computer. Auf diese Weise können Sie Ihr lokales Unternehmensnetzwerk vor Identitätsdiebstahl und anderen Angriffen schützen. Die Komponente verwendet die Anti-Malware-Datenbanken, den Cloud-Dienst Kaspersky Security Network sowie vordefinierte Netzwerkregeln.

Prioritäten für Netzwerkregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel in der Liste steht, desto höher ist ihre Priorität. Ist die Netzwerkaktivität in mehreren Firewall-Regeln enthalten, wird die Netzwerkaktivität gemäß der Regel mit der höchsten Priorität geregelt.

Typen von Netzwerkverbindungen

Über die Firewall können Sie die Netzwerkaktivität abhängig vom Netzwerkverbindungstyp kontrollieren. Den Typ einer Netzwerkverbindung können Sie in den Einstellungen von Kaspersky Endpoint Security ändern.

Es gibt die folgenden Typen von Netzwerkverbindungen:

- **Öffentliches Netzwerk**. Das Netzwerk wird nicht durch Anti-Malware-Programme, Firewalls oder Filter geschützt (z. B. WLAN in einem Café). Verbindet der Benutzer seinen Computer mit einem solchen Netzwerk, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Dann können externe Benutzer auch nicht über freigegebene Ordner oder eine Remotedesktopverbindung auf die Daten dieses Computers zugreifen. Die Firewall weist dem Internet standardmäßig den Typ „Öffentliches Netzwerk“ zu. Der Netzwerktyp für das Internet kann nicht geändert werden.

- **Lokales Netzwerk**. Netzwerk für Benutzer, die auf diesem Computer eingeschränkten Zugriff auf Dateien und Drucker haben (z. B. für ein lokales Unternehmensnetzwerk oder ein Heimnetzwerk).

- **Vertrauenswürdiges Netzwerk**. Sicheres Netzwerk, in dem keine Angriffe auf den Computer und keine unbefugten Zugriffsversuche auf Daten zu befürchten sind. Innerhalb von Netzwerken mit diesem Status erlaubt die Firewall jede Netzwerkaktivität.

Komponente „Firewall“ verwalten (in der Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.

2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.

3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.

4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.

6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Basisschutz** > **Firewall** aus.

7. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Firewall aktivieren**.

8. Klicken Sie im Abschnitt **Firewall-Einstellungen** auf **Einstellungen**. Im folgenden Fenster können Sie Regeln hinzufügen, bearbeiten, löschen oder deren Priorität ändern.

9. Klicken Sie im Abschnitt **Verfügbare Netzwerke** auf Einstellungen. Im folgenden Fenster können Sie Netzwerke hinzufügen, bearbeiten, löschen oder den Netzwerktyp ändern.

10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

11. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Komponente „Firewall“ verwalten (in der Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Basisschutz** > **Firewall**.

5. Aktivieren/deaktivieren Sie den Schalter **Firewall**.

6. Klicken Sie im Abschnitt **Firewall-Einstellungen** auf **Regeln für Netzwerkpakete**. Im folgenden Fenster können Sie Regeln hinzufügen, bearbeiten, löschen oder deren Priorität ändern.

7. Klicken Sie im Abschnitt **Verfügbare Netzwerke** auf **Netzwerkeinstellungen**. Im folgenden Fenster können Sie Netzwerke hinzufügen, bearbeiten oder den Netzwerktyp ändern.

8. Speichern Sie die Änderungen.

Komponente „Firewall“ verwalten (in der Anwendung Kaspersky Endpoint Security)

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren oder deaktivieren Sie auf der Registerkarte **Basis** im Abschnitt **Firewall** das Kontrollkästchen **Firewall aktivieren**.

3. Klicken Sie bei Bedarf auf **Einstellungen** und passen Sie die Firewall-Einstellungen an:

   - Auf der Registerkarte **Regeln für Netzwerkpakete** können Sie Regeln hinzufügen, bearbeiten, löschen oder deren Priorität ändern.

   - Auf der Registerkarte **Verfügbare Netzwerke** können Sie Netzwerke hinzufügen, bearbeiten oder deren Typ ändern.

Wenn die Firewall aktiviert ist, kontrolliert Kaspersky Endpoint Security die Netzwerkaktivität und blockiert nicht autorisierte Netzwerkverbindungen mit Ihrem Computer.

Firewall-Bericht anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Firewall**.

Verhaltensanalyse

Die Komponente Verhaltensanalyse empfängt Daten über die Aktionen von auf Ihrem Computer installierten Programmen und stellt diese Daten anderen Schutzkomponenten zur Verfügung, um deren Leistung zu verbessern. Die Komponente Verhaltensanalyse verwendet Verhaltensstrom-Signaturen (Behavior Stream Signatures, BSS) von Programmen. Wenn die Aktivität eines Programms mit einer Verhaltensstrom-Signatur übereinstimmt, führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Endpoint Security, die auf Vorlagen für gefährliches Verhalten beruht, bietet einen proaktiven Computerschutz.

Die Verhaltensanalyse ist standardmäßig aktiviert und wird in dem Modus ausgeführt, den die Kaspersky-Experten empfehlen. Sie können die Verhaltenserkennung bei Bedarf deaktivieren.

Verhaltensanalyse über die Web Console aktivieren/deaktivieren

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zu **Erweiterter Schutz** > **Verhaltensanalyse**.

5. Aktivieren/deaktivieren Sie den Schalter **Verhaltensanalyse**.

6. Wenn die Verhaltensanalyse aktiviert ist, wählen Sie eine der folgenden Aktionen aus, die beim Erkennen von Malware-Aktivität ausgeführt werden soll:

   - **Blockieren**

     Wenn diese Option ausgewählt ist, beendet Kaspersky Endpoint Security die Anwendung, sobald eine schädliche Aktivität erkannt wird.

- **Löschen**

  Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security eine schädliche Aktivität erkennt, löscht Kaspersky Endpoint Security die ausführbare Schadsoftware-Datei und legt eine Backup-Kopie der Datei an.

- **Aktion erfragen**

  Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security eine schädliche Aktivität erkennt, zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster mit Informationen über das schädliche Objekt an und fragt den Benutzer, welche Aktion ausgeführt werden soll. Die verfügbaren Aktionen können je nach Objektstatus variieren.

7. Wenn die Verhaltensanalyse und der Schutz vor der externen Verschlüsselung freigegebener Ordner aktiviert sind, wählen Sie aus, welche der folgenden Aktionen beim Fund einer externen Verschlüsselung ausgeführt werden soll:

   - **Informieren**

     Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch erkennt, Dateien in freigegebenen Ordnern zu ändern, fügt es Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu, fügt einen Eintrag zu den Berichten der lokalen Programmberichten hinzu und sendet Informationen über die erkannte bösartige Aktivität an Kaspersky Security Center.

   - **Angreifendes Gerät blockieren für**

     Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch erkennt, Dateien in freigegebenen Ordnern zu ändern, so blockiert es den Zugriff auf Dateiänderungen (schreibgeschützt) für die Sitzung, die die bösartige Aktivität initiiert hat, und legt Backup-Kopien der geänderten Dateien an.

8. Speichern Sie die Änderungen.

Verhaltensanalyse über die Verwaltungskonsole aktivieren/deaktivieren

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Erweiterter Schutz** > **Verhaltensanalyse** aus
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**.
8. Wählen Sie bei Bedarf im Abschnitt **Aktion, wenn Schadsoftware-Aktivität erkannt wird** aus, welche Aktion ausgeführt werden soll, wenn Malware gefunden wird.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

10. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Kennwortschutz über die Anwendung Kaspersky Endpoint Security aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren oder deaktivieren Sie auf der Registerkarte **Erweitert** im Abschnitt **Verhaltensanalyse** das Kontrollkästchen **Verhaltensanalyse aktivieren**.

3. Wenn das Kontrollkästchen **Verhaltensanalyse aktivieren** aktiviert ist, wählen Sie eine der folgenden Aktionen aus, die beim Fund von Malware ausgeführt werden soll:

    - **Blockieren**

      Wenn diese Option ausgewählt ist, beendet Kaspersky Endpoint Security die Anwendung, sobald eine schädliche Aktivität erkannt wird.

    - **Löschen**

      Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security eine schädliche Aktivität erkennt, löscht Kaspersky Endpoint Security die ausführbare Schadsoftware-Datei und legt eine Backup-Kopie der Datei an.

    - **Aktion erfragen**

      Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security eine schädliche Aktivität erkennt, zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster mit Informationen über das schädliche Objekt an und fragt den Benutzer, welche Aktion ausgeführt werden soll. Die verfügbaren Aktionen können je nach Objektstatus variieren.

Wenn die Verhaltensanalyse aktiviert ist, verwendet Kaspersky Endpoint Security daher Verhaltensstrom-Signaturen, um die Aktivität von Programmen im Betriebssystem zu analysieren.

Wichtig: Es wird davor gewarnt, die Verhaltensanalyse zu deaktivieren, sofern dies nicht unbedingt erforderlich ist, da dadurch die Wirksamkeit der Schutzkomponenten verringert wird. Um Bedrohungen zu erkennen, können die Schutzkomponenten von der Komponente Verhaltensanalyse gesammelte Daten anfordern.

Virensuche

Der Schutz vor bedrohlichen Dateien und der Schutz vor Web-Bedrohungen gewährleisten den Echtzeitschutz des Computers. Es wird aber trotzdem empfohlen, den Computer regelmäßig auf Malware und andere Bedrohungen der Computersicherheit zu untersuchen. Die Untersuchung des Computers ist notwendig, um eine Ausbreitung von Schadsoftware zu verhindern, die von den Schutzkomponenten nicht erkannt wurde.

Kaspersky Endpoint Security bietet die folgenden integrierten Untersuchungsaufgaben:

- **Vollständige Untersuchung**.

  Arbeitsspeicher des Computers, Autostart-Objekte und alle internen Datenträger auf Malware untersuchen.

- **Schnelle Untersuchung**.

  Schadsoftware-Untersuchung, die nur wichtige Computerbereiche umfasst: Arbeitsspeicher, Autostart-Objekte und Systemordner.

- **Benutzerdefinierte Untersuchung**.

  Schadsoftware-Untersuchung eines bestimmten Objekts (Datei, Ordner, interner Datenträger oder Wechseldatenträger).

- **Untersuchung externer Datenträger**

  Eine Malware-Untersuchung für externe Datenträger, die gestartet wird, sobald ein externer Datenträger mit dem Computer verbunden wird.

Wenn die App eine Untersuchungsaufgabe ausführt, werden schädliche Objekte mithilfe der Signaturanalyse erkannt. Neben der Signaturanalyse setzt Kaspersky Endpoint Security auch eine heuristische Analyse und weitere Untersuchungstechnologien ein.

Das Fenster **Untersuchung** enthält Informationen über den Fortschritt aller laufenden Untersuchungsaufgaben (Prozentangabe und verbleibende Zeit) und einen Untersuchungsverlauf (die 100 letzten Untersuchungsaufgaben).

Aufgabe Vollständige Untersuchung und Schnelle Untersuchung starten

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie im Fenster **Untersuchung** auf **Vollständige Untersuchung** oder **Schnelle Untersuchung**.

Die Untersuchungsaufgabe wird gestartet.

Aufgabe Benutzerdefinierte Untersuchung starten

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Um die Aufgabe **Benutzerdefinierte Untersuchung** zu starten, führen Sie eine der folgenden Aktionen aus:

   - Ziehen Sie mit der Maus eine Datei oder einen Ordner in das Fenster.
   - Klicken Sie auf **Auswählen** und öffnen Sie eine Datei oder einen Ordner.

Die Untersuchungsaufgabe wird gestartet.

Untersuchungsaufgabe abbrechen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie im Fenster **Untersuchung** neben der Untersuchungsaufgabe auf die Schaltfläche „Abbrechen“ ( ).

   Ein Bestätigungsdialog wird geöffnet.

3. Klicken Sie im Bestätigungsdialog auf **Abbrechen**.

Die Untersuchungsaufgabe wird abgebrochen.

Sie können einen Zeitplan für die Aufgabe „Vollständige Untersuchung“ oder „Schnelle Untersuchung“ erstellen.

Untersuchungsaufgabe aus dem Untersuchungsfenster planen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.

2. Klicken Sie auf **Untersuchungszeitplan**.

   Im folgenden Dialog können Sie den Zeitplan festlegen.

3. Aktivieren Sie das Kontrollkästchen **Vollständige Untersuchung** oder **Schnelle Untersuchung**.

4. Geben Sie die Frequenz und den Startzeitpunkt der Untersuchung an.

5. Klicken Sie auf **OK**.

Untersuchungsaufgabe im Konfigurationsfenster planen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Untersuchung** auf **Zeitplan**.

3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen für den Namen der Untersuchungsaufgabe, die Sie nach Zeitplan starten möchten.

4. Passen Sie die Frequenz und den Zeitpunkt der Untersuchung an.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern, die Sie im Zeitplan der Untersuchungsaufgabe vorgenommen haben.

Wenn ein externer Datenträger mit dem Computer verbunden wird, kann Kaspersky Endpoint Security den Datenträger entweder automatisch untersuchen, fragen, ob eine Untersuchung erfolgen soll, oder nichts tun. Sie können in den Einstellungen für die „Untersuchung externer Datenträger“ eine der Optionen auswählen.

Wählen Sie die Aktion aus, die Kaspersky Endpoint Security ausführen soll, sobald ein externer Datenträger an den Computer angeschlossen wird

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** links in der Liste die Aufgabe **Untersuchung externer Datenträger** aus.

3. Wählen Sie im Abschnitt **Wenn ein externer Datenträger angeschlossen wird** die Aktion aus, die Kaspersky Endpoint Security ausführen soll, sobald ein externer Datenträger angeschlossen wird.

Die Aufgaben Vollständige Untersuchung und Schnelle Untersuchung enthalten bereits festgelegte Untersuchungsbereiche. Im Rahmen der Aufgabe „Vollständige Untersuchung“ untersucht das Programm Kaspersky Endpoint Security den Arbeitsspeicher des Computers, die Autostart-Objekte und alle internen Laufwerke. Im Rahmen der Aufgabe „Schnelle Untersuchung“ untersucht das Programm den Arbeitsspeicher des Computers, die Autostart-Objekte und die Systemordner. Sie können den Untersuchungsbereich für die Aufgabe Schnelle Untersuchung ändern.

Hinweis: Sie können die Untersuchung des schreibgeschützten Systemvolume überspringen und dadurch die Untersuchungsdauer wesentlich reduzieren. Standardmäßig untersucht Kaspersky Endpoint Security das schreibgeschützte Systemvolume nicht, wenn die Aufgabe „Schnelle Untersuchung“ ausgeführt wird. Dagegen wird es im Rahmen der Aufgabe „Vollständige Untersuchung“ untersucht.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Untersuchung des schreibgeschützten Systemvolume aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** in der Liste auf der linken Seite die Aufgabe **Vollständige Untersuchung** oder **Schnelle Untersuchung** aus.

3. Deaktivieren/aktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen **Schreibgeschütztes Systemvolume bei der Untersuchung überspringen**.

   Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

Datei oder Ordner zum Untersuchungsbereich der Aufgabe Schnelle Untersuchung hinzufügen oder aus dem Untersuchungsbereich löschen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** links in der Liste die Aufgabe **Schnelle Untersuchung** aus.

3. Klicken Sie im Abschnitt **Bereich** auf **Bearbeiten**.

   Das angezeigte Fenster enthält eine Liste mit den Objekten, die zum Untersuchungsbereich der Aufgabe „Schnelle Untersuchung“ gehören.

4. Passen Sie die Liste mit den Objekten des Untersuchungsbereichs an:

   - Um eine Datei oder einen Ordner zum Untersuchungsbereich der Aufgabe Schnelle Untersuchung hinzuzufügen:

     a. Klicken Sie auf +.

     Im eingeblendeten Pop-up-Menü können Sie Objekte auswählen, die zum Untersuchungsbereich hinzugefügt werden sollen.

b. Wählen Sie den Eintrag **Dateien und Ordner**.

Im folgenden Dialog können Sie eine Datei oder einen Ordner auswählen.

c. Wählen Sie aus, welche Datei oder welcher Ordner zum Untersuchungsbereich für die Schnelle Untersuchung hinzugefügt werden soll.

d. Klicken Sie auf **Öffnen**.

- Um eine Datei oder einen Ordner aus dem Untersuchungsbereich der Aufgabe Schnelle Untersuchung zu löschen:

a. Wählen Sie das zu löschende Objekt aus.

b. Ziehen Sie das ausgewählte Objekt aus dem Fenster heraus oder klicken Sie auf –.

5. Klicken Sie auf **Speichern**.

Objekt aus der Standardliste für die Schnelle Untersuchung zum Untersuchungsbereich der Aufgabe Schnelle Untersuchung hinzufügen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** links in der Liste die Aufgabe **Schnelle Untersuchung** aus.

3. Klicken Sie im Abschnitt **Bereich** auf **Bearbeiten**.

Ein Fenster mit einer Liste der Objekte im Untersuchungsbereich wird geöffnet.

4. Klicken Sie auf +.

Im eingeblendeten Pop-up-Menü können Sie Objekte auswählen, die zum Untersuchungsbereich hinzugefügt werden sollen.

5. Wählen Sie im Pop-up-Menü ein Objekt aus, das zum Untersuchungsbereich hinzugefügt werden soll (z. B. **Arbeitsspeicher**).

6. Klicken Sie auf **OK**.

Schutz für ein Objekt aus dem Untersuchungsbereich für die Aufgabe Schnelle Untersuchung deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** links in der Liste die Aufgabe **Schnelle Untersuchung** aus.

3. Klicken Sie im Abschnitt **Bereich** auf **Bearbeiten**.

Ein Fenster mit der Liste der Objekte im Untersuchungsbereich wird geöffnet.

4. Deaktivieren Sie in der Liste der Objekte im Untersuchungsbereich das Kontrollkästchen neben dem entsprechenden Objekt.

5. Klicken Sie auf **OK**.

Wenn in einer Datei eine Bedrohung gefunden wird, zeigt die Anwendung eine Benachrichtigung an und führt die angegebene Aktion mit dem Objekt aus. Sie können die Aktion ändern, die beim Fund eines Objekts ausgeführt werden soll.

Aktion auswählen, die Kaspersky Endpoint Security beim Fund von infizierten Dateien ausführen soll

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Wählen Sie auf der Registerkarte **Untersuchung** eine Aufgabe aus der Aufgabenliste aus.

3. Wählen Sie im Abschnitt **Aktion** aus, welche Aktion das Programm beim Fund von infizierten Dateien ausführen soll.

Bevor eine infizierte Datei desinfiziert oder gelöscht wird, legt Kaspersky Endpoint Security im Backup eine Kopie der Datei an. So können Sie die Originaldatei falls nötig wiederherstellen.

Informationen über die Ergebnisse der Untersuchungsaufgaben und über alle gefundenen Objekte werden in einem Bericht aufgezeichnet.

Hinweis: Wenn bei einer Untersuchungsaufgabe Fehler aufgetreten sind, starten Sie die Aufgabe neu. Falls der erneute Versuch, die Untersuchung zu starten, ebenfalls fehlschlägt, wenden Sie sich an den Technischen Support von Kaspersky.

Bericht für eine Untersuchungsaufgabe anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Untersuchung**.

Update-Aufgaben

Ein regelmäßiges Update der Anwendungsdatenbanken ist eine wichtige Voraussetzung für die Sicherheit Ihres Computers. Der Schutz vor bedrohlichen Dateien, der Schutz vor Web-Bedrohungen und die Untersuchungsaufgaben verwenden die Anwendungsdatenbanken, um auf Ihrem Computer Malware zu erkennen und zu neutralisieren. Die Anwendungsdatenbanken werden regelmäßig mit Einträgen über unterschiedliche Bedrohungsarten und Abwehrmethoden aktualisiert. Deshalb ist ein regelmäßiges Datenbanken-Update sehr wichtig.

Kaspersky Endpoint Security lädt die Anwendungsdatenbanken und neuen Anwendungsmodule von den Kaspersky-Update-Servern herunter und installiert sie auf Ihrem Computer. Kaspersky Endpoint Security kann auch Verteilungspunkte, lokale Ordner oder andere Webserver verwenden.

Hinweis: Für die Verbindung mit den Update-Servern und für den Update-Download ist eine Internetverbindung erforderlich. Falls für die Internetverbindung ein Proxy-Server verwendet wird, müssen eventuell die Netzwerkeinstellungen konfiguriert werden.

Updates für die Anwendungsdatenbanken können wie folgt heruntergeladen werden:

- **Automatisch**. Kaspersky Endpoint Security überprüft regelmäßig, ob auf den Kaspersky-Update-Servern neue Updates vorhanden sind. Wenn auf dem Update-Server ein neues Update vorliegt, wird dieses Update von Kaspersky Endpoint Security im Hintergrund heruntergeladen und auf Ihrem Computer installiert. Diese Option ist standardmäßig aktiviert.

- **Manuell**. Sie können jederzeit manuell überprüfen, ob Updates für Kaspersky Endpoint Security verfügbar sind.

Automatischen Download der Datenbanken-Updates für Kaspersky Endpoint Security aktivieren/deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren/deaktivieren Sie auf der Registerkarte Update im Abschnitt **Datenbanken** das Kontrollkästchen **Updates automatisch herunterladen**.

Datenbanken-Updates für Kaspersky Endpoint Security suchen

1. Klicken Sie in der Seitenleiste des App-Hauptfensters auf **Update**.

   Das Fenster **Update** wird geöffnet.

2. Klicken Sie auf **Aktualisieren**.

Die Anwendung beginnt mit dem Datenbanken-Update.

Sie können die Update-Aufgabe auch wie folgt starten:

- Klicken Sie auf das Anwendungssymbol und wählen Sie **Aktualisieren** aus.

- Wählen Sie in der Menüleiste den Punkt **Schutz** > **Aktualisieren** aus.

Bei einer Aktualisierung werden die Anwendungsdatenbanken und Module mit den momentan auf den Update-Servern vorhandenen Updates verglichen. Falls auf Ihrem Computer die neueste Version der Datenbanken installiert ist, wird im Fenster **Update** gemeldet, dass die Anwendungsdatenbanken aktuell sind. Wenn sich die Anwendungsversion und die Anwendungsdatenbanken von den momentan auf den Update-Servern verfügbaren unterscheiden, werden nur die fehlenden Komponenten des Updates auf Ihren Computer heruntergeladen und installiert. Inkrementelle Updates der Anwendungsdatenbanken sparen Zeit und reduzieren den Web-Datenverkehr.

Wenn die Internetverbindung über einen Proxy-Server erfolgt, können Sie die Verbindungseinstellungen für den Proxy-Server konfigurieren. Kaspersky Endpoint Security verwendet diese Einstellungen für die Aktualisierung der Anwendungsdatenbanken und für den Download von Updates der Module.

Verbindung mit dem Proxy-Server anpassen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Öffnen Sie die Registerkarte **Update**.

3. Aktivieren Sie im Abschnitt **Proxy** das Kontrollkästchen **Proxyserver verwenden** und klicken Sie auf **Einstellungen**.

   Im nächsten Fenster können Sie die Verbindungseinstellungen für den Proxy-Server anpassen.

4. Verbindung mit dem Proxy-Server anpassen.

5. Klicken Sie auf **Speichern**, um die geänderten Einstellungen für die Proxy-Server-Verbindung zu speichern.

Bevor die Anwendungsdatenbanken aktualisiert werden, erstellt Kaspersky Endpoint Security Backup-Kopien davon, damit bei Bedarf ein Update-Rollback zur vorherigen Datenbankversion erfolgen kann. Die Rollback-Option ist von Nutzen, wenn die neue Version der Anwendungsdatenbanken einen fehlerhaften Eintrag enthält, durch den Kaspersky Endpoint Security eine harmlose Anwendung blockiert.

Hinweis: Wenn die Datenbanken von Kaspersky Endpoint Security beschädigt sind, wird empfohlen, das Update zu starten, um die neueste Version der Anwendungsdatenbanken herunterzuladen und zu installieren.

Rollback des letzten Updates

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Öffnen Sie die Registerkarte **Update**.

3. Klicken Sie im Abschnitt **Rollback** auf **Update zurücksetzen**.

Kaspersky Endpoint Security bietet im Fenster **Berichte** einen ausführlichen Bericht über die Ergebnisse der Update-Aufgabe.

Bericht für die Update-Aufgabe

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

2. Das Fenster **Berichte** wird geöffnet.

3. Öffnen Sie die Registerkarte **Datenbanken-Update**.

Hinweis: Die Update-Funktion (einschließlich der Bereitstellung von Anti-Malware-Signatur-Updates und Codebase-Updates) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Lokale Aufgaben

Aufgabe zur Untersuchung externer Datenträger

Kaspersky Endpoint Security kann alle Dateien untersuchen, die Sie ausführen oder kopieren, selbst wenn sich die Datei auf einem externen Datenträger befindet. Um die Verbreitung von Malware zu verhindern, können Sie für externe Datenträger die automatische Untersuchung konfigurieren, sobald diese an das Gerät angeschlossen werden.

Die folgenden Einstellungen für die Untersuchung externer Datenträger können angepasst werden:

- **Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein externer Datenträger angeschlossen wird.**

  Untersuchen

  Wenn diese Option ausgewählt ist, startet Kaspersky Endpoint Security für den angeschlossenen externen Datenträger eine Aufgabe zur Untersuchung auf Malware.

  Diese Variante ist standardmäßig ausgewählt.

  Nichts tun

  Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security den angeschlossenen externen Datenträger nicht.

- **Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein schädliches Objekt erkannt wurde.**

  Desinfizieren – Löschen, wenn Desinfektion fehlschlägt

  Wenn diese Option ausgewählt ist, blockiert Kaspersky Endpoint Security den Zugriff auf das infizierte Objekt und versucht, es zu desinfizieren, ohne nach Bestätigung durch den Benutzer zu fragen.

  Wenn das Objekt desinfiziert werden konnte, wird es von Kaspersky Endpoint Security am ursprünglichen Ort unter dem ursprünglichen Namen gespeichert. Wenn die Desinfektion fehlschlägt, löscht Kaspersky Endpoint Security jene infizierten Objekte, die nicht desinfiziert werden konnten.

  Diese Variante ist standardmäßig ausgewählt.

  Aktion erfragen

  Wenn diese Option ausgewählt ist, zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster mit Informationen über das schädliche Objekt an und fordert den Benutzer auf, die Aktion auszuwählen, die Kaspersky Endpoint Security ausführen soll. Die verfügbaren Aktionen können je nach Objektstatus variieren.

Sie können die Untersuchung externer Datenträger in der Verwaltungskonsole, in der Web Console oder in der Anwendung von Kaspersky Endpoint Security konfigurieren.

So konfigurieren Sie die Untersuchung externer Datenträger in der Verwaltungskonsole (MMC)

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** die Option **Lokale Aufgaben** > **Untersuchung externer Datenträger** aus.
7. Passen Sie die Aufgabeneinstellungen an.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So konfigurieren Sie Ausführung der Untersuchung externer Datenträger in der Web Console und Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie die Option **Lokale Aufgaben** > **Untersuchung externer Datenträger** aus.
5. Passen Sie die Aufgabeneinstellungen an.
6. Klicken Sie auf OK, um die Änderungen zu speichern.

So konfigurieren Sie die Ausführung der Untersuchung externer Datenträger in der Benutzeroberfläche der Anwendung

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.
2. Wählen Sie auf der Registerkarte **Untersuchung** links in der Liste die Aufgabe **Untersuchung externer Datenträger** aus.
3. Wählen Sie im Abschnitt **Wenn ein externer Datenträger angeschlossen wird** die Aktion aus, die Kaspersky Endpoint Security ausführen soll, sobald ein externer Datenträger angeschlossen wird.

Backup

Bei der Desinfektion von infizierten Dateien gelingt es nicht immer, die Integrität der Dateien zu bewahren. Wenn eine desinfizierte Datei wichtige Informationen enthalten hat, die aufgrund der Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie die ursprüngliche Datei aus dem Backup wiederherstellen.

Eine *Backup-Kopie* ist die Kopie einer gefährlichen Datei. Die Kopie wird angelegt, wenn die Datei desinfiziert oder gelöscht wird. Sie wird im Backup gespeichert.

Das *Backup* ist ein spezieller Speicher für Backup-Kopien von Dateien, die bei der Desinfektion gelöscht oder verändert wurden. Die wichtigste Funktion des Backups besteht darin, jederzeit eine Wiederherstellung der ursprünglichen Datei zu ermöglichen. Die Backup-Kopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr für den Computer dar.

Inhalt des Backups anzeigen

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.
2. Öffnen Sie im Abschnitt **Backup** die Liste der Backup-Dateien.

Sie können die Backup-Kopien von Dateien aus dem Backup wiederherstellen oder löschen.

Backup-Kopie einer Datei aus dem Backup wiederherstellen

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.

2. Klicken Sie im Abschnitt **Backup** neben der Datei, die wiederhergestellt werden soll, auf ⋯.

   Ein Pop-up-Menü wird geöffnet.

3. Wählen Sie **Datei wiederherstellen**.

   Geben Sie im nächsten Fenster den Dateinamen, den Tag und den Zielordner für die wiederherzustellende Datei an. Standardmäßig sind der ursprüngliche Dateiname und Ordner angegeben.

4. Geben Sie den Dateinamen und den Zielordner für die wiederherzustellende Datei an.

5. Klicken Sie auf **Speichern**.

Die Anwendung stellt die Datei am angegebenen Ort unter dem gewünschten Namen wieder her.

Sie sollten die Datei sofort nach der Wiederherstellung auf Malware untersuchen. Möglicherweise gelingt es, die Datei mit den aktuellen Antiviren-Datenbanken zu desinfizieren, ohne dass sie beschädigt wird.

Wichtig: Es wird davon abgeraten, Backup-Kopien von Dateien wiederherzustellen, wenn dies nicht unbedingt erforderlich ist. Eine Wiederherstellung kann zu einer Computerinfektion führen.

Backup-Kopie einer Datei aus dem Backup löschen

1. Wählen Sie in der Menüleiste **Schutz** > **Erkannte Objekte** aus.

   Das Fenster **Erkannte Objekte** wird geöffnet.

2. Gehen Sie im Abschnitt **Backup** wie folgt vor:

   - Um alle Backup-Kopien für Dateien zu löschen, klicken Sie auf **Alle löschen**.
   - Um die ausgewählten Backup-Kopien zu löschen, klicken Sie daneben auf ⋯ und wählen Sie **Gesicherte Kopie löschen** aus.

Die Speicherdauer für Dateien im Backup beträgt standardmäßig 30 Tage. Nach Ablauf dieses Zeitraums werden die Dateien gelöscht. Sie können die maximale Speicherdauer für Dateien im Backup ändern oder diese Beschränkung vollständig aufheben.

Speicherdauer für Dateien im Backup anpassen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Bedrohungen** im Abschnitt **Backup** das Kontrollkästchen **Gesicherte Objekte löschen nach <Anzahl> Tagen** und legen Sie fest, nach welchem Zeitraum Dateien automatisch aus dem Backup gelöscht werden sollen.

Berichte

Auf der Registerkarte **Verarbeitete Objekte** können Sie einen Kaspersky Endpoint Security-Bericht mit einer Liste aller erkannten Objekte anzeigen. Systemereignisse werden auf der Registerkarte **Systemereignisse** angezeigt. Zusätzlich wird für jede der folgenden Programmkomponenten ein separater Detailbericht erstellt: Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Verhaltensanalyse und Untersuchungs- und Update-Aufgaben.

Fenster Berichte öffnen

Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

Berichte für Kaspersky Endpoint Security können im Textformat gespeichert werden. Diese Funktion kann nützlich sein, wenn bei Anwendungskomponenten oder Aufgaben Fehler auftreten, die Sie nicht selbst beheben können, und Sie die Hilfe des Technischen Supports von Kaspersky benötigen. In diesem Fall können Sie den Bericht im Textformat an den Technischen Support von Kaspersky senden, damit unsere Experten das Problem analysieren und schnellstmöglich lösen können.

Bericht über eine Komponente von Kaspersky Endpoint Security oder Aufgabenbericht in eine Textdatei exportieren

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Wählen Sie im linken Bereich die Registerkarte mit dem gewünschten Bericht aus.

3. Klicken Sie in der rechten oberen Ecke auf .

4. Geben Sie im folgenden Fenster den Dateinamen, die Tags und den Zielordner für den Bericht an.

5. Klicken Sie auf **Speichern**.

Standardmäßig werden informative Ereignisse von Kaspersky Endpoint Security nicht in Berichten protokolliert. Sie können festlegen, dass informative Ereignisse aufgezeichnet werden sollen.

Protokollierung von informativen Ereignissen erlauben

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Berichte** das Kontrollkästchen **Nicht-kritische Ereignisse protokollieren**, um Benachrichtigungen über informative Ereignisse von Kaspersky Endpoint Security zu erhalten.

Managed Detection and Response

Die Komponente Managed Detection and Response wurde in Kaspersky Endpoint Security mit Version 11.2 hinzugefügt. Diese Komponente interagiert mit einer Lösung, die als Kaspersky Managed Detection and Response bezeichnet wird. *Kaspersky Managed Detection and Response (MDR)* sucht und erkennt fortwährend Sicherheitsbedrohungen, die auf Ihr Unternehmen abzielen, und eliminiert sie. Ausführliche Informationen zur Funktionsweise der Lösung finden Sie in der *Hilfe zu Kaspersky Managed Detection and Response*.

Im Zusammenhang mit Kaspersky Managed Detection and Response können Sie die folgenden Funktionen ausführen:

- Managed Detection and Response mit einer BLOB-Konfigurationsdatei aktivieren.
- Befehle über Kaspersky Managed Detection and Response ausführen.
- Telemetriedaten zur Bedrohungserfassung an Kaspersky Managed Detection and Response senden.

Die Komponente „Managed Detection and Response“ stellt die folgenden zusätzlichen Anforderungen:

- macOS 12 oder höher
- Intel-basierter Mac, Apple Silicon
- Aktive Lizenz für Kaspersky Endpoint Security

Integration in Kaspersky Managed Detection and Response

Die Integration in Kaspersky Managed Detection and Response umfasst die folgenden Schritte:

1. **Konfiguration des Proxy-Servers von Kaspersky Security Network**

   Der Proxy-Server von Kaspersky Security Network vereinfacht den Datenaustausch zwischen Computern und der Cloud-Dienstinfrastruktur von Kaspersky Security Network über den Administrationsserver statt über einen direkten Austausch.

   Laden der Konfigurationsdatei für Kaspersky Security Network in den Eigenschaften des Administrationsservers. Die Konfigurationsdatei des Kaspersky Security Network befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv über die Kaspersky Managed Detection and Response Console abrufen. Details zur Konfiguration des Proxy-Server von Kaspersky Security Network finden Sie in der *Hilfe zu Kaspersky Security Center*.

   Dementsprechend verwendet Kaspersky Endpoint Security Private KSN, um die Reputation von Dateien, Anwendungen und Websites zu ermitteln. Der Betriebsstatus *„Infrastruktur: Kaspersky Private Security Network“* wird in den Richtlinieneinstellungen im Abschnitt „Kaspersky Security Network“ angezeigt.

   Die Nutzung von Private KSN mit Kaspersky Managed Detection and Response stellt sicher, dass Telemetriedaten an Server gesendet werden, die der DSGVO (Datenschutz-Grundverordnung) entsprechen. Wenn Private KSN nicht verwendet wird, können Telemetriedaten an Global KSN gesendet werden. Das verstößt aber möglicherweise gegen das in ihrem Land geltende Recht.

Wichtig: Sie müssen den erweiterten KSN-Modus aktivieren, damit „Managed Detection and Response“ wie vorgesehen funktioniert.

2 **Aktivieren von Managed Detection and Response**

Laden Sie die BLOB-Konfigurationsdatei in die Richtlinie von Kaspersky Endpoint Security (siehe Anleitung unten). Die BLOB-Datei enthält die Client-ID und Informationen zur Lizenz für Kaspersky Managed Detection and Response. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv über die Kaspersky Managed Detection and Response Console abrufen. Ausführliche Informationen über BLOB-Dateien finden Sie in der *Hilfe zu Kaspersky Managed Detection and Response*.

Managed Detection and Response in der Verwaltungskonsole (MMC) aktivieren

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften Detection and Response** > **Managed Detection and Response** aus.
7. Wählen Sie das Kontrollkästchen **Managed Detection and Response** aus.
8. Klicken Sie im Block der **MDR-Konfigurationsdatei** auf **Importieren**, und wählen Sie die von der Kaspersky Managed Detection and Response Console bereitgestellte BLOB-Datei aus. Die Datei hat die Erweiterung .P7.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Managed Detection and Response in der Web Console und Cloud Console aktivieren

1. Wählen Sie im Hauptfenster der Web Console **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.
3. Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
5. Wählen Sie **Detection and Response** > **Managed Detection and Response** aus.
6. Aktivieren Sie den Umschalter **Managed Detection and Response**.
7. Klicken Sie auf **Importieren**, und wählen Sie die BLOB-Datei aus, die von der Kaspersky Managed Detection and Response Console bereitgestellt wurde. Die Datei hat die Erweiterung .P7.
8. Speichern Sie die Änderungen.

Daraufhin verifiziert Kaspersky Endpoint Security die BLOB-Datei. Bei der Überprüfung der BLOB-Datei werden auch die digitale Signatur und der Lizenzzeitraum geprüft. Nachdem die BLOB-Datei erfolgreich überprüft wurde, lädt Kaspersky Endpoint Security die Datei und sendet sie bei der nächsten Synchronisierung mit Kaspersky Security Center an den Computer.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security unterstützt die Integration mit der Komponente Kaspersky Endpoint Detection and Response, die Teil der Lösung Kaspersky Anti Targeted Attack Platform ist. Diese Lösung wurde entwickelt, um komplexe Bedrohungen sofort zu erkennen. Dazu zählen beispielsweise gezielte Angriffe, hochentwickelte, hartnäckige Bedrohungen und Zero-Day-Angriffe. Ausführliche Informationen zur Funktionsweise der Lösung finden Sie in der *Hilfe zur Kaspersky Anti Targeted Attack Platform*.

Wenn die Integration mit Endpoint Detection and Response (KATA) konfiguriert ist, erhält der KATA-Server Informationen über Ereignisse, die bei der Ausführung von Kaspersky Endpoint Security auftreten, über die von der App erkannten Bedrohungen und über die Verarbeitung dieser Bedrohungen. Zur Reaktion auf erkannte Bedrohungen kann Kaspersky Endpoint Security dann Aufgaben ausführen, die in der Web-Oberfläche der Kaspersky Anti Targeted Attack Platform gestartet wurden.

Für Endpoint Detection and Response (KATA) gelten die folgenden zusätzlichen Anforderungen:

- Kaspersky Anti Targeted Attack Platform 6.0 oder höher.
- Kaspersky Security Center 14.2 oder höher.
- Die Integration mit Endpoint Detection and Response (KATA) kann in der Kaspersky Security Center Administration Console (MMC), Web Console oder Cloud Console konfiguriert werden.

Integration mit Kaspersky Endpoint Detection and Response (KATA)

Die Integration in Kaspersky Endpoint Detection and Response (KATA) umfasst die folgenden Schritte:

1. **Installation der Komponente „Endpoint Detection and Response“**

   Die Komponente Endpoint Detection and Response können Sie während der Installation von Kaspersky Endpoint Security auswählen.

2. **Aktivieren von Endpoint Detection and Response**

   Wenn die Komponente Endpoint Detection and Response von Ihrer aktuellen Lizenz nicht unterstützt wird, müssen Sie Kaspersky Endpoint Detection and Response separat aktivieren.

   Im Fenster **Lizenz** können Sie überprüfen, ob die Funktionalität von Endpoint Detection and Response von der aktuellen Lizenz unterstützt wird.

3. **Verbindung mit einem KATA-Server herstellen**

   Kaspersky Anti Targeted Attack Platform erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und einem KATA-Server. Um eine vertrauenswürdige Verbindung zu konfigurieren, müssen Sie ein TLS-Zertifikat verwenden. Sie können ein TLS-Zertifikat über die Web-Oberfläche der Kaspersky Anti Targeted Attack Platform herunterladen. Ausführliche Informationen zum Herunterladen eines Zertifikats finden Sie in der *Hilfe zur Kaspersky Anti Targeted Attack Platform*.

   Kaspersky Endpoint Security überprüft standardmäßig nur das TLS-Zertifikat des KATA-Servers. Um die Verbindung sicherer zu machen, können Sie die Zwei-Wege-Überprüfung aktivieren. Um die Zwei-Wege-Überprüfung zu aktivieren, müssen Sie einen kennwortgeschützten Krypto-Container verwenden. Ausführliche Informationen zum Herunterladen eines Krypto-Containers finden Sie in der *Hilfe zur Kaspersky Anti Targeted Attack Platform*.

Computer mit Kaspersky Endpoint Security über die Verwaltungskonsole mit einem KATA-Server verbinden

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Detection and Response** > **Endpoint Detection and Response (KATA)** aus.
7. Aktivieren Sie das Kontrollkästchen **Endpoint Detection and Response (KATA)**.
8. Klicken Sie auf **Einstellungen für die Serververbindung**.
9. Konfigurieren Sie im angezeigten Fenster **Einstellungen für die Serververbindung** die folgenden Einstellungen:
   - Klicken Sie auf **TLS-Zertifikat hinzufügen**, um ein TLS-Zertifikat auszuwählen, das zum Herstellen einer vertrauenswürdigen Verbindung mit einem KATA-Server verwendet werden soll.
   - Wenn Sie das Antwort-Timeout des KATA-Servers ändern möchten, geben Sie das Timeout im Feld **Timeout (s)** an. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, eine Verbindung zu einem anderen KATA-Server herzustellen.
   - Wenn Sie die Zwei-Wege-Überprüfung verwenden möchten, aktivieren Sie das Kontrollkästchen **Zwei-Wege-Überprüfung verwenden**. Klicken Sie auf **Krypto-Container laden**, um eine Krypto-Container-Datei auszuwählen, und geben Sie im Feld **Kennwort des Krypto-Containers** das Kennwort ein.
10. Klicken Sie auf **Speichern**.
11. Um einen KATA-Server hinzuzufügen, klicken Sie auf **Hinzufügen**.
12. Geben Sie im folgenden Fenster **KATA-Server** die Adresse und den Port des Servers an und klicken Sie auf **Speichern**.
13. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Computer mit Kaspersky Endpoint Security über die Web Console mit einem KATA-Server verbinden

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Detection and Response** > **Endpoint Detection and Response (KATA)** aus.
5. Aktivieren Sie den Schalter **Endpoint Detection and Response (KATA)**.

6. Klicken Sie auf **Einstellungen der Serververbindung**.

7. Konfigurieren Sie im angezeigten Dialog **Einstellungen der Serververbindung** die folgenden Einstellungen:

   - Klicken Sie auf **TLS-Zertifikat hinzufügen**, um ein TLS-Zertifikat auszuwählen, das zum Herstellen einer vertrauenswürdigen Verbindung mit einem KATA-Server verwendet werden soll.

   - Wenn Sie das Antwort-Timeout des KATA-Servers ändern möchten, geben Sie das Timeout im Feld **Timeout (s)** an. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, eine Verbindung zu einem anderen KATA-Server herzustellen.

   - Wenn Sie die Zwei-Wege-Überprüfung verwenden möchten, aktivieren Sie das Kontrollkästchen **Zwei-Wege-Überprüfung verwenden**. Klicken Sie auf **Krypto-Container laden**, um eine Krypto-Container-Datei auszuwählen, und geben Sie im Feld **Kennwort des Krypto-Containers** das Kennwort ein.

8. Klicken Sie auf **OK**.

9. Um einen KATA-Server hinzuzufügen, klicken Sie auf **Hinzufügen**.

10. Geben Sie im folgenden Dialog die Adresse und den Port des Servers an und klicken Sie auf **OK**.

11. Speichern Sie die Änderungen.

Daraufhin werden die Computer in der Web-Oberfläche der Kaspersky Anti Targeted Attack Platform angezeigt.

Endpoint Detection and Response Optimum

Beginnend mit Version 12.1 enthält Kaspersky Endpoint Security for Mac einen integrierten Agenten für die Lösung „Kaspersky Endpoint Detection and Response Optimum“ (im Weiteren auch „EDR Optimum“). Diese Lösung wurde entwickelt, um die IT-Infrastruktur von Unternehmen vor komplexen Cyberbedrohungen zu schützen. Die Funktionalität der Lösung kombiniert die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren. Auf diese Weise werden fortschrittliche Angriffe effektiv abgewehrt. Zu diesen gehören neuartige Exploits, Ransomware, dateilose Angriffe sowie Methoden, die legitime Systemtools ausnutzen. Weitere Informationen zu dieser Lösung finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

„Kaspersky Endpoint Detection and Response“ prüft und analysiert, wie sich eine Bedrohung entwickelt, und versorgt die *Sicherheitsabteilung* oder den *Administrator* mit Informationen über den möglichen Angriff, um eine rechtzeitige Reaktion zu ermöglichen. Kaspersky Endpoint Detection and Response (EDR) zeigt Alarm-Details in einem separaten Fenster an. Die *Alarmdetails* sind ein Tool zum Anzeigen aller gesammelten Informationen über eine erkannte Bedrohung. Zu den Alarmdetails gehört beispielsweise der Verlauf der auf dem Computer veränderten Dateien. Weitere Informationen zur Verwaltung der Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Hinweis: Die Komponente EDR Optimum können Sie in der Web Console konfigurieren.

Parameter	Beschreibung
Netzwerkisolation	Automatische Isolation des Computers vom Netzwerk als Reaktion auf erkannte Bedrohungen. Wenn die Netzwerkisolation aktiviert ist, trennt die Anwendung alle aktiven Verbindungen und blockiert alle neuen TCP/IP-Verbindungen auf dem Computer. Die Anwendung behält nur die folgenden Verbindungen bei: • Verbindungen, die als Ausnahmen für die Netzwerkisolation angegeben sind. • Verbindungen, die von Kaspersky Endpoint Security-Diensten initiiert werden. • Verbindungen, die vom Kaspersky Security Center-Administrationsagenten initiiert werden.
Isolation des Computers automatisch aufheben nach n Stunden	Die Netzwerkisolation kann automatisch nach einem bestimmten Zeitraum oder manuell deaktiviert werden. Standardmäßig deaktiviert Kaspersky Endpoint Security die Netzwerkisolation 8 Stunden nach Beginn der Isolation.
Ausnahmen für die Netzwerkisolation	Liste mit Regeln für die Ausnahmen von der Netzwerkisolation. Netzwerkverbindungen, die den Regeln entsprechen, werden auf Computern mit aktivierter Netzwerkisolation nicht blockiert. Um die Ausnahmen für die Netzwerkisolation zu konfigurieren, können Sie eine Liste mit Standardnetzwerkprofilen verwenden. Zu den Ausnahmen gehören standardmäßig Netzwerkprofile mit Regeln, die sicherstellen, dass Geräte mit den Rollen DNS/DHCP-Server und DNS/DHCP-Client unterbrechungsfrei funktionieren. Sie können die Einstellungen der Standardnetzwerkprofile auch ändern oder manuell Ausnahmen definieren. **Wichtig:** Die in den Richtlinieneigenschaften angegebenen Ausnahmen werden nur angewendet, wenn die Netzwerkisolation als Reaktion auf eine erkannte Bedrohung automatisch aktiviert wird. In den Computereigenschaften angegebene Ausnahmen werden nur angewendet, wenn die Netzwerkisolation manuell in den Computereigenschaften in der Kaspersky Security Center-Konsole oder in den Alarm-Details aktiviert wurde.
Ausführungsprävention	Mit der Ausführungsprävention kann das Starten von ausführbaren Dateien und Skripten sowie das Öffnen von Dateien im Office-Format verwaltet werden. Auf diese Weise können Sie beispielsweise die Ausführung von Anwendungen verhindern, die Sie als unsicher einstufen. Dies kann die Ausbreitung einer Bedrohung begrenzen. Die Ausführungsprävention unterstützt eine Reihe von Skriptinterpretern. Um die Komponente „Ausführungsprävention“ verwenden zu können, müssen Sie dieser Regeln für die Ausführungsprävention hinzufügen. Die Regel für die Ausführungsprävention ist eine Zusammenstellung von Kriterien, die von der Anwendung berücksichtigt werden, wenn sie auf die Ausführung eines Objekts reagiert, beispielsweise wenn das Starten eines Objekts blockiert wird. Die Anwendung identifiziert Dateien anhand ihres Pfads oder ihrer Prüfsummen, die mithilfe der MD5- und SHA256-Hash-Algorithmen berechnet wurden.
Aktion beim Ausführen oder Öffnen eines verbotenen Objekts	**Blockieren und protokollieren**. In diesem Modus blockiert die Anwendung den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Zusätzlich veröffentlicht die Anwendung im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über Versuche, Objekte zu starten oder Dokumente zu öffnen. **Nur Ereignisse protokollieren**. In diesem Modus veröffentlicht Kaspersky Endpoint Security im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Allerdings wird das Starten oder Öffnen des Objekts nicht blockiert. Diese Variante ist standardmäßig ausgewählt.
Cloud Sandbox	Cloud Sandbox ist eine Technologie, mit der Sie komplexe Bedrohungen auf einem Computer erkennen können. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox“ weiter. „Cloud Sandbox“ führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivität zu erkennen, und entscheidet dann über ihre Reputation. Daten über diese Dateien werden an Kaspersky Security Network gesendet. Wenn „Cloud Sandbox“ eine schädliche Datei gefunden hat, führt Kaspersky Endpoint Security die passende Aktion aus, um diese Bedrohung auf allen Computern, auf denen die Bedrohung vorliegt, zu beseitigen. **Hinweis:** Cloud Sandbox ist dauerhaft aktiviert und steht allen Benutzern von Kaspersky Security Network unabhängig von deren verwendeten Lizenztyp zur Verfügung.

Integration mit Endpoint Detection and Response Optimum

Für die Integration mit Kaspersky Endpoint Detection and Response müssen Sie die Komponente „Endpoint Detection and Response“ Optimum (EDR Optimum) hinzufügen und Kaspersky Endpoint Security konfigurieren.

Hinweis: EDR Optimum und Endpoint Detection and Response (KATA) sind nicht miteinander kompatibel.

Damit „Endpoint Detection and Response“ funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Security Center 13.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die Funktion „Endpoint Detection and Response“ nicht aktiviert werden.
- Das Verwaltungs-Plug-in für Kaspersky Endpoint Detection and Response ist installiert. Dies ist ein separates Plug-in für die Arbeit mit Agents unter den Betriebssystemen Windows, Mac und Linux. Wenn Sie mit Endpoint Detection and Response Optimum arbeiten, benötigen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security, um Aufgaben zur Bedrohungsreaktion zu erstellen, sowie das EDR-Verwaltungs-Plug-in, um Alarm-Details anzusehen.
- Die Komponente „EDR Optimum“ unterstützt als Teil von Kaspersky Endpoint Security die Interaktion mit der Lösung „Kaspersky Endpoint Detection and Response Optimum 3.0“. Die Interaktion mit älteren Versionen von Kaspersky Endpoint Detection and Response Optimum wird nicht unterstützt.
- EDR Optimum kann über die Web Console verwaltet werden.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die Komponente „Endpoint Detection and Response“ ist aktiviert.

Integration mit Kaspersky Endpoint Detection and Response Optimum

Die Integration mit Kaspersky Endpoint Detection and Response Optimum umfasst die folgenden Schritte:

1. **Installation der Komponente „Endpoint Detection and Response Optimum“**

   Die Komponente Endpoint Detection and Response können Sie während der Installation von Kaspersky Endpoint Security auswählen.

2. **Aktivieren von Endpoint Detection and Response**

   Wenn die Komponente Endpoint Detection and Response von Ihrer aktuellen Lizenz nicht unterstützt wird, müssen Sie Kaspersky Endpoint Detection and Response separat aktivieren.

   Im Fenster **Lizenz** können Sie überprüfen, ob die Funktionalität von Endpoint Detection and Response von der aktuellen Lizenz unterstützt wird.

3. **Aktivieren der Komponente „Endpoint Detection and Response“**

   Sie können die Komponente in den Richtlinieneinstellungen von Kaspersky Endpoint Security for Mac aktivieren oder deaktivieren.

   So aktivieren oder deaktivieren Sie die Komponente Endpoint Detection and Response über die Web Console

   1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.

5. Aktivieren Sie den Schalter **Endpoint Detection and Response**.

6. Speichern Sie die Änderungen.

Nach Kompromittierungsindikatoren suchen

Ein **Kompromittierungsindikator (IOC)** ist eine Sammlung von Informationen über ein Objekt oder eine Aktivität, die auf einen unbefugten Zugriff auf den Computer (eine Datenkompromittierung) hinweisen. Beispielsweise können viele erfolglose Anmeldeversuche am System einen Kompromittierungsindikator darstellen. Mit der Aufgabe **IOC-Untersuchung** können Kompromittierungsindikatoren auf dem Computer gefunden und Maßnahmen zur Reaktion auf Bedrohungen ergriffen werden.

Kaspersky Endpoint Security sucht mithilfe von IOC-Dateien nach Kompromittierungsindikatoren. IOC-Dateien sind Dateien, die Sammlung von Indikatoren enthalten, mit denen die Anwendung nach Übereinstimmungen sucht, um sie einem Fund anzurechnen. IOC-Dateien müssen den Anforderungen für IOC-Dateien entsprechen.

Ausführungsmodus Aufgabe zur IOC-Untersuchung

Mit „Kaspersky Endpoint Detection and Response“ können Sie standardmäßige IOC-Untersuchungsaufgaben erstellen, um kompromittierte Daten zu erkennen. Eine standardmäßige Aufgabe zur IOC-Untersuchung ist eine Gruppenaufgabe oder lokale Aufgabe, die manuell in der Web Console erstellt und konfiguriert wird. Die Aufgaben verwenden während ihrer Ausführung IOC-Dateien, die vom vorher vom Benutzer vorbereitet wurden. Wenn Sie einen Kompromittierungsindikator manuell hinzufügen möchten, lesen Sie bitte die Anforderungen an IOC-Dateien.

Erstellen einer Aufgabe zur IOC-Untersuchung

Sie können IOC-Untersuchungsaufgaben manuell erstellen:

- In den Alarmdetails (nur für EDR Optimum).

  Die *Alarmdetails* sind ein Tool zum Anzeigen aller gesammelten Informationen über eine erkannte Bedrohung. Zu den Alarmdetails gehört beispielsweise der Verlauf der auf dem Computer veränderten Dateien. Weitere Informationen zur Verwaltung der Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

- Unter Verwendung des Assistenten für die Aufgabe.

So erstellen Sie eine Aufgabe zur IOC-Untersuchung:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **IOC-Untersuchung** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen werden soll** den Aufgabenbereich aus.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus.

5. Laden Sie im Abschnitt **IOC-Untersuchungseinstellungen** die IOC-Dateien, mit denen nach Kompromittierungsindikatoren gesucht werden soll. Sie können eine IOC-Datei hinzufügen oder eine IOC-Datei aus einer Datei erstellen, die Datei-Hashs oder IP-Adressen enthält.

   Nachdem die IOC-Dateien geladen wurden, können Sie die Liste der Indikatoren aus den IOC-Dateien ansehen und bearbeiten.

   > **Hinweis:** Das Hinzufügen oder Entfernen von IOC-Dateien nach dem Ausführen der Aufgabe wird nicht empfohlen. Dies kann dazu führen, dass die Ergebnisse der IOC-Untersuchung für frühere Ausführungen der Aufgabe falsch angezeigt werden. Um Kompromittierungsindikatoren anhand neuer IOC-Dateien zu suchen, wird es empfohlen, neue Aufgaben hinzuzufügen.

6. Konfiguration der Aktionen Erkennung eines IOC:

   - **Computer vom Netzwerk isolieren**. Wenn diese Option ausgewählt ist, isoliert Kaspersky Endpoint Security den Computer vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. Die Isolationsdauer können Sie in den Einstellungen der Komponente „Endpoint Detection and Response“ anpassen.

   - **Kopie in die Quarantäne verschieben und Objekt löschen**. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne.

   - **Untersuchung wichtiger Bereiche ausführen**. Wenn diese Option ausgewählt ist, führt Kaspersky Endpoint Security die Aufgabe „Schnelle Untersuchung“ aus. Standardmäßig untersucht Kaspersky Endpoint Security den Arbeitsspeicher, die Autostart-Objekte und die Systemordner.

7. Gehen Sie zum Abschnitt **Erweitert**.

8. Wählen Sie die Datentypen (IOC-Dokumente) aus, die im Rahmen der Aufgabe analysiert werden sollen.

   > **Hinweis:** Kaspersky Endpoint Security wählt die Datentypen (IOC-Dokumente) für die Aufgabe zur IOC-Untersuchung automatisch aus, entsprechend dem Inhalt der geladenen IOC-Dateien. Es wird nicht empfohlen, Datentypen abzuwählen.

   Für die folgenden Datentypen können Sie zusätzliche Untersuchungsbereiche konfigurieren:

   - **Prozesse – ProcessItem**

   - **Dateien – FileItem**

- **Netzwerkports – PortItem**
- **Benutzerkonten – UserItem**
- **ARP-Tabellen – ArpEntryItem**
- **Hosts – SystemInfoItem**
- **URLs – UrlHistoryItem**
- **Routes – RouteEntryItem**

9. Klicken Sie auf **OK**.
10. Geben Sie die Anmeldedaten des Benutzers ein, mit dessen Rechten die Aufgabe ausgeführt werden soll. Klicken Sie auf **Weiter**.

    Hinweis: Standardmäßig startet Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (root).

11. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

    Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

12. Klicken Sie auf die neue Aufgabe.

    Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

13. Wählen Sie die Registerkarte **Zeitplan**.
14. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

15. Klicken Sie auf **Speichern**.
16. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

17. Klicken Sie auf Sie Schaltfläche **Starten**.

    Daraufhin durchsucht Kaspersky Endpoint Security den Computer nach Kompromittierungsindikatoren. Sie können die Aufgabenergebnisse in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** anzeigen. Informationen über gefundene Kompromittierungsindikatoren können Sie in den Aufgabeneigenschaften unter **Anwendungseinstellungen** > **IOC-Untersuchungsergebnisse** einsehen.

Hinweis: Die Ergebnisse der IOC-Untersuchung werden 30 Tage lang gespeichert. Nach diesem Zeitraum löscht Kaspersky Endpoint Security automatisch die ältesten Einträge.

Datei in Quarantäne verschieben

Als Reaktion auf Bedrohungen kann Kaspersky Endpoint Detection and Response Aufgaben vom Typ *Datei in Quarantäne verschieben* erstellen. Dies ist notwendig, um die Folgen von Bedrohung zu minimieren. Die *Quarantäne* ist ein spezieller lokaler Speicherbereich auf dem Computer. Der Benutzer kann Dateien in die Quarantäne verschieben, die er als Gefahr für die Computersicherheit einstuft. Dateien, die sich in Quarantäne befinden, werden verschlüsselt gespeichert und stellen keine Gefahr für die Sicherheit des Geräts dar. Kaspersky Endpoint Security verwendet das Backup zum Speichern der Dateien. Weitere Informationen zur Verwaltung der Quarantäne im Rahmen von EDR-Lösungen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Auf diese Arten können Sie Aufgaben des Typs *Datei in Quarantäne verschieben* erstellen:

- In den Alarmdetails (nur für EDR Optimum).

  Die *Alarmdetails* sind ein Tool zum Anzeigen aller gesammelten Informationen über eine erkannte Bedrohung. Zu den Alarmdetails gehört beispielsweise der Verlauf der auf dem Computer veränderten Dateien. Weitere Informationen zur Verwaltung der Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

- Unter Verwendung des Assistenten für die Aufgabe.

  Sie müssen entweder den Pfad oder den Hash (SHA256 oder MD5) der Datei eingeben oder alternativ sowohl den Pfad als auch den Hash der Datei eingeben.

Die Aufgaben vom Typ *Datei in Quarantäne verschieben* besitzen folgende Einschränkungen:

- Die Dateigröße darf maximal 100 MB betragen.
- Sie können die Aufgabe für EDR Optimum in der Web Console konfigurieren.
- Die Kapazität des Backups wird durch den freien Speicherplatz auf der Festplatte begrenzt.

So erstellen Sie eine Aufgabe des Typs Datei in Quarantäne verschieben:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Datei in Quarantäne verschieben** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

d. Wählen Sie einen der folgenden Optionen aus:

- **Aufgabe einer Administrationsgruppe zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die zu einer Administrationsgruppe gehören. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe zum Senden einer Nachricht an Benutzer auszuführen, wenn die Nachricht spezifisch für die Geräte aus einer bestimmten Administrationsgruppe ist.

  Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Eigenschaftenfenster der Aufgabe nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

- **Geräteadressen manuell angeben oder Adressen aus einer Liste importieren**

  Sie können die NetBIOS-Namen, DNS-Namen, IP-Adressen und IP-Subnetze der Geräten angeben, denen Sie die Aufgabe zuweisen möchten.

  Sie können diese Option verwenden, um eine Aufgabe für ein bestimmtes Subnetz auszuführen. Sie können beispielsweise eine bestimmte Anwendung auf den Geräten der Buchhaltung installieren oder ausschließlich die Geräte eines mutmaßlich infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Version des Betriebssystems auszuführen.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Geräteauswahl an.

   Die verfügbaren Einstellungen hängen von der Option ab, die im vorherigen Schritt festgelegt wurde.

6. Klicken Sie in der Liste der Dateien auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Dateien wird gestartet.

7. Wählen Sie in der Dropdown-Liste **Bitte geben Sie die Datei an, die in Quarantäne verschoben werden soll** eine der Optionen aus und füllen Sie die erforderlichen Felder aus. Um die Datei hinzuzufügen, können Sie entweder nur den vollständigen Dateipfad oder den Datei-Hash zusammen mit dem Dateipfad angeben.

8. Wenn Sie möchten, dass die Aufgabe für kritische Systemobjekte gilt, aktivieren Sie das Kontrollkästchen **Auf kritische Systemobjekte anwenden**.

9. Geben Sie die Anmeldedaten des Benutzers ein, mit dessen Rechten die Aufgabe ausgeführt werden soll. Klicken Sie auf **Weiter**.

   Hinweis: Standardmäßig startet Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (root).

10. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

    Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

11. Klicken Sie auf die neue Aufgabe.

    Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

12. Wählen Sie die Registerkarte **Zeitplan**.

13. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

14. Klicken Sie auf **Speichern**.

15. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

16. Klicken Sie auf Sie Schaltfläche **Starten**.

Daraufhin verschiebt Kaspersky Endpoint Security die Datei in die Quarantäne.

Eine Aufgabe des Typs *Datei in Quarantäne verschieben* kann mit der Fehlermeldung *Zugriff verweigert* abgeschlossen werden, wenn Sie versuchen, eine ausführbare Datei, die gerade gestartet ist, in die Quarantäne zu verschieben. Erstellen Sie für diese Datei eine Aufgabe des Typs Prozess beenden und versuchen Sie es erneut.

Eine Aufgabe des Typs *Datei in Quarantäne verschieben* kann mit der Fehlermeldung *Ungenügender Speicherplatz der Quarantäne* abgeschlossen werden, wenn Sie versuchen, eine zu große Datei in die Quarantäne zu verschieben. Geben Sie zusätzlichen Speicherplatz frei und versuchen Sie es erneut.

Datei abrufen

Sie können Dateien von den Computern der Benutzer abrufen. Sie können beispielsweise den Abruf einer Ereignisprotokolldatei konfigurieren, die von der Anwendung eines Drittanbieters erstellt wurde. Um die Datei abzurufen, müssen Sie eine spezielle Aufgabe erstellen. Als Ergebnis der Aufgabenausführung wird die Datei im Backup gespeichert. Sie können diese Datei mithilfe der Web Console aus dem Backup auf Ihren Computer herunterladen. Auf dem Computer des Benutzers verbleibt die Datei in ihrem ursprünglichen Ordner.

Wichtig: Die Dateigröße darf maximal 100 MB betragen. Die Kapazität des Backups wird durch den freien Speicherplatz auf der Festplatte begrenzt.

So erstellen Sie eine Aufgabe zum Abrufen einer Datei:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Datei abrufen** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie einen der folgenden Optionen aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die zu einer Administrationsgruppe gehören. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe zum Senden einer Nachricht an Benutzer auszuführen, wenn die Nachricht spezifisch für die Geräte aus einer bestimmten Administrationsgruppe ist.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Eigenschaftenfenster der Aufgabe nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

   - **Geräteadressen manuell angeben oder Adressen aus einer Liste importieren**

     Sie können die NetBIOS-Namen, DNS-Namen, IP-Adressen und IP-Subnetze der Geräten angeben, denen Sie die Aufgabe zuweisen möchten.

     Sie können diese Option verwenden, um eine Aufgabe für ein bestimmtes Subnetz auszuführen. Sie können beispielsweise eine bestimmte Anwendung auf den Geräten der Buchhaltung installieren oder ausschließlich die Geräte eines mutmaßlich infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Version des Betriebssystems auszuführen.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus. Klicken Sie im Fenster **Datei anfordern** auf **Hinzufügen**.

   Der Dialog **Datei anfordern** wird geöffnet.

5. Wählen Sie in der Dropdown-Liste **Benötigte Datei angeben** eine der Optionen aus und füllen Sie die erforderlichen Felder aus.

   Um die Datei hinzuzufügen, können Sie entweder nur den vollständigen Dateipfad oder den Datei-Hash zusammen mit dem Dateipfad angeben.

6. Klicken Sie auf **OK**.

   Die Einstellungen der hinzuzufügenden Datei werden in der Dateiliste angezeigt.

7. Klicken Sie auf **Weiter**.

8. Geben Sie die Anmeldedaten des Benutzers ein, mit dessen Rechten die Aufgabe ausgeführt werden soll. Klicken Sie auf **Weiter**.

   Hinweis: Standardmäßig startet Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (root).

9. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

10. Klicken Sie auf die neue Aufgabe.

    Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

11. Wählen Sie die Registerkarte **Zeitplan**.

12. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

13. Klicken Sie auf **Speichern**.

14. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf Sie Schaltfläche **Starten**.

Infolgedessen erstellt Kaspersky Endpoint Security eine Kopie der Datei und verschiebt diese Kopie in das Backup. Sie können die Datei aus dem Backup in Web Console herunterladen.

Datei löschen

Mit der Aufgabe *Datei löschen* können Sie Dateien aus der Ferne löschen. Sie können beispielsweise eine Datei aus remote löschen, wenn Sie auf Bedrohungen reagieren.

So erstellen Sie eine Aufgabe zum Löschen einer Datei:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Datei löschen** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie einen der folgenden Optionen aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die zu einer Administrationsgruppe gehören. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe zum Senden einer Nachricht an Benutzer auszuführen, wenn die Nachricht spezifisch für die Geräte aus einer bestimmten Administrationsgruppe ist.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Eigenschaftenfenster der Aufgabe nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

   - **Geräteadressen manuell angeben oder Adressen aus einer Liste importieren**

     Sie können die NetBIOS-Namen, DNS-Namen, IP-Adressen und IP-Subnetze der Geräten angeben, denen Sie die Aufgabe zuweisen möchten.

     Sie können diese Option verwenden, um eine Aufgabe für ein bestimmtes Subnetz auszuführen. Sie können beispielsweise eine bestimmte Anwendung auf den Geräten der Buchhaltung installieren oder ausschließlich die Geräte eines mutmaßlich infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Version des Betriebssystems auszuführen.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus.

5. Wählen Sie in der Dropdown-Liste **Zu löschende Datei angeben** eine der Optionen und füllen Sie die erforderlichen Felder aus. Um die Datei hinzuzufügen, können Sie entweder nur den vollständigen Dateipfad oder den Datei-Hash zusammen mit dem Dateipfad angeben.

6. Wenn Sie möchten, dass die Aufgabe für kritische Systemobjekte gilt, aktivieren Sie das Kontrollkästchen **Auf kritische Systemobjekte anwenden**.

7. Geben Sie die Anmeldedaten des Benutzers ein, mit dessen Rechten die Aufgabe ausgeführt werden soll. Klicken Sie auf **Weiter**.

   Hinweis: Standardmäßig startet Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (root).

8. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

9. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

10. Wählen Sie die Registerkarte **Zeitplan**.

11. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

12. Klicken Sie auf **Speichern**.

13. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

14. Klicken Sie auf Sie Schaltfläche **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security die Datei vom entsprechenden Computer. Wenn die Datei durch einem anderen Prozess gesperrt wurde, wird die Aufgabe als *Abgeschlossen* angezeigt, die Datei selbst wird jedoch erst nach einem Neustart des Computers gelöscht. Stellen Sie nach einem Neustart des Computers sicher, dass die Datei gelöscht wurde.

Eine Aufgabe des Typs *Datei löschen* kann mit der Fehlermeldung *Zugriff verweigert* abgeschlossen werden, wenn Sie versuchen, eine ausführbare Datei, die gerade gestartet ist, zu löschen. Erstellen Sie für diese Datei eine Aufgabe des Typs Prozess beenden und versuchen Sie es erneut.

Prozess starten

Mithilfe der Aufgabe *Prozess starten* können Sie Dateien remote starten.

Wichtig: Sie können die Aufgabe für EDR Optimum in der Web Console konfigurieren.

So erstellen Sie eine Aufgabe des Typs Prozesses starten:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Prozess starten** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie einen der folgenden Optionen aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die zu einer Administrationsgruppe gehören. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe zum Senden einer Nachricht an Benutzer auszuführen, wenn die Nachricht spezifisch für die Geräte aus einer bestimmten Administrationsgruppe ist.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Eigenschaftenfenster der Aufgabe nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

   - **Geräteadressen manuell angeben oder Adressen aus einer Liste importieren**

     Sie können die NetBIOS-Namen, DNS-Namen, IP-Adressen und IP-Subnetze der Geräten angeben, denen Sie die Aufgabe zuweisen möchten.

     Sie können diese Option verwenden, um eine Aufgabe für ein bestimmtes Subnetz auszuführen. Sie können beispielsweise eine bestimmte Anwendung auf den Geräten der Buchhaltung installieren oder ausschließlich die Geräte eines mutmaßlich infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Version des Betriebssystems auszuführen.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Geräteauswahl an.

   Die verfügbaren Einstellungen hängen von der Option ab, die im vorherigen Schritt festgelegt wurde.

6. Passen Sie die Aufgabeneinstellungen an:

   a. Geben Sie im Feld **Ausführbarer Befehl** den Befehl ein, der auf dem lokalen Gerät ausgeführt werden soll.

   b. Geben Sie bei Bedarf im Feld **Befehlszeilenargumente (optional)** die Befehlszeilenargumente an.

   c. Geben Sie bei Bedarf im Feld **Pfad zum Arbeitsverzeichnis (optional)** den Pfad der ausführbaren Datei an.

7. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

8. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

9. Wählen Sie die Registerkarte **Zeitplan**.

10. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

11. Klicken Sie auf **Speichern**.

12. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

13. Klicken Sie auf Sie Schaltfläche **Starten**.

    Daraufhin führt Kaspersky Endpoint Security den Befehl im Hintergrund aus und startet den Prozess. Sie können die Aufgabenergebnisse in den Aufgabeneigenschaften im Abschnitt **Ausführungsergebnisse** anzeigen.

Prozess beenden

Mit der Aufgabe *Prozess beenden* können Sie Prozesse remote beenden. Sie können beispielsweise remote ein Tool zum Messen der Internet-Geschwindigkeit beenden, das zuvor mithilfe der Aufgabe Prozess starten gestartet wurde.

Wenn Sie die Ausführung einer Datei verbieten möchten, können Sie dazu die Komponente Ausführungsprävention konfigurieren. Sie können die Ausführung von ausführbaren Dateien, Skripten und Dateien im Office-Format verbieten.

Für die Aufgabe *Prozess beenden* gelten die folgenden Einschränkungen:

- Sie können die Aufgabe nur für EDR Optimum in der Web Console konfigurieren.

So erstellen Sie eine Aufgabe des Typs Prozesses beenden:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Aufgaben** aus.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet.

3. Passen Sie die Aufgabeneinstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt Kaspersky Endpoint Security for Mac (12.2) aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Prozess beenden** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

d. Wählen Sie einen der folgenden Optionen aus:

- **Aufgabe einer Administrationsgruppe zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die zu einer Administrationsgruppe gehören. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe zum Senden einer Nachricht an Benutzer auszuführen, wenn die Nachricht spezifisch für die Geräte aus einer bestimmten Administrationsgruppe ist.

  Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Eigenschaftenfenster der Aufgabe nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

- **Geräteadressen manuell angeben oder Adressen aus einer Liste importieren**

  Sie können die NetBIOS-Namen, DNS-Namen, IP-Adressen und IP-Subnetze der Geräten angeben, denen Sie die Aufgabe zuweisen möchten.

  Sie können diese Option verwenden, um eine Aufgabe für ein bestimmtes Subnetz auszuführen. Sie können beispielsweise eine bestimmte Anwendung auf den Geräten der Buchhaltung installieren oder ausschließlich die Geräte eines mutmaßlich infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Version des Betriebssystems auszuführen.

4. Wählen Sie die Geräte entsprechend des ausgewählten Gültigkeitsbereichs der Aufgabe aus.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Geräteauswahl an.

   Die verfügbaren Einstellungen hängen von der Option ab, die im vorherigen Schritt festgelegt wurde.

6. Wählen Sie bei diesem Schritt des Assistenten in der Dropdown-Liste **Bitte geben Sie die Datei an, deren Prozesse beendet werden sollen** eine der Optionen aus und füllen Sie die erforderlichen Felder aus. Um die Datei anzugeben, können Sie entweder nur den vollständigen Dateipfad oder den Datei-Hash zusammen mit dem Dateipfad angeben.

   Hinweis: Wenn Sie diese Aufgabe für ein lokales Gerät erstellen, können Sie den Prozess nach PID angeben.

7. Wenn Sie möchten, dass die Aufgabe für kritische Systemobjekte gilt, aktivieren Sie das Kontrollkästchen **Auf kritische Systemobjekte anwenden**.

8. Geben Sie die Anmeldedaten des Benutzers ein, mit dessen Rechten die Aufgabe ausgeführt werden soll. Klicken Sie auf **Weiter**.

   Hinweis: Standardmäßig startet Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (root).

9. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Abschließen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie bei Bedarf die Aufgabenparameter überprüfen und ändern oder einen Startzeitplan für die Aufgabe festlegen.

10. Klicken Sie auf die neue Aufgabe.

    Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

11. Wählen Sie die Registerkarte **Zeitplan**.

12. Passen Sie den Startzeitplan für die Aufgabe an.

    Hinweis: Stellen Sie sicher, dass der Computer zum Zeitpunkt der geplanten Aufgabenausführung eingeschaltet ist.

13. Klicken Sie auf **Speichern**.

14. Um die Aufgabe unabhängig vom festgelegten Zeitplan sofort zu starten, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf Sie Schaltfläche **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security den Prozess vom entsprechenden Computer. Wenn beispielsweise das Programm *Game* ausgeführt wird und Sie den Prozess *Game* beenden, wird das Programm geschlossen, ohne Daten zu speichern. Sie können die Aufgabenergebnisse in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** anzeigen.

Ausführungsprävention

Mit der Ausführungsprävention kann das Starten von ausführbaren Dateien und Skripten sowie das Öffnen von Dateien im Office-Format verwaltet werden. Auf diese Weise können Sie beispielsweise die Ausführung von Anwendungen verhindern, die Sie als unsicher einstufen. Dies kann die Ausbreitung einer Bedrohung begrenzen. Die Ausführungsprävention unterstützt eine Reihe von Skriptinterpretern.

Präventionsregel für die Ausführung

Die Ausführungsprävention verwaltet den Benutzerzugriff auf Dateien mithilfe von Präventionsregeln für die Ausführung. Die Regel für die Ausführungsprävention ist eine Zusammenstellung von Kriterien, die von der Anwendung berücksichtigt werden, wenn sie auf die Ausführung eines Objekts reagiert, beispielsweise wenn das Starten eines Objekts blockiert wird. Die Anwendung identifiziert Dateien anhand von Pfaden oder Prüfsummen, die auf MD5- und SHA256-Hash-Algorithmen beruhen.

Sie können Präventionsregeln für die Ausführung erstellen:

- In den Alarmdetails (nur für EDR Optimum).

  Die *Alarmdetails* sind ein Tool zum Anzeigen aller gesammelten Informationen über eine erkannte Bedrohung. Zu den Alarmdetails gehört beispielsweise der Verlauf der auf dem Computer veränderten Dateien. Weitere Informationen zur Verwaltung der Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

- Unter Verwendung einer Gruppenrichtlinie oder lokaler Anwendungseinstellungen. Sie müssen entweder den Pfad oder den Hash (SHA256 oder MD5) der Datei eingeben oder alternativ sowohl den Pfad als auch den Hash der Datei eingeben.

Sie können die Ausführungsprävention auch lokal über die Befehlszeile verwalten.

Hinweis: Der Start von systemkritischen Objekten (SCO) kann nicht blockiert werden. SCOs sind Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security for Mac erforderlich sind.

Modi der Präventionsregeln für die Ausführung

Die Komponente „Ausführungsprävention“ kann in zwei Modi ausgeführt werden:

- **Nur Statistik**

  In diesem Modus veröffentlicht Kaspersky Endpoint Security im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Allerdings wird das Starten oder Öffnen des Objekts nicht blockiert. Standardmäßig ist dieser Modus ausgewählt.

- **Aktiv**

  In diesem Modus blockiert die Anwendung den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Zusätzlich veröffentlicht die Anwendung im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über Versuche, Objekte zu starten oder Dokumente zu öffnen.

Ausführungsprävention verwalten

Wichtig: Sie können die Einstellungen der Komponente nur in der Web Console konfigurieren.

So verhindern Sie eine Ausführung:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.

5. Aktivieren Sie den Schalter **Ausführungsprävention**.

6. Wählen Sie im Block **Aktion beim Ausführen oder Öffnen eines verbotenen Objekts** den Ausführungsmodus der Komponente aus:

   - **Blockieren und protokollieren**. In diesem Modus blockiert die Anwendung den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Zusätzlich veröffentlicht die Anwendung im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über Versuche, Objekte zu starten oder Dokumente zu öffnen.

   - **Nur Ereignisse protokollieren**. In diesem Modus veröffentlicht Kaspersky Endpoint Security im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Allerdings wird das Starten oder Öffnen des Objekts nicht blockiert. Standardmäßig ist dieser Modus ausgewählt.

7. Eine Liste mit Präventionsregeln für die Ausführung erstellen:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie im neuen Dialogfeld den Namen der Präventionsregel für die Ausführung ein (z. B. „Anwendung A“).

   c. Wählen Sie in der Dropdown-Liste **Typ** die Art des Objekts aus, das Sie blockieren möchten: **Anwendung**, **Skript** oder **Dokument**.

      Falls Sie einen falschen Objekttyp auswählen, blockiert Kaspersky Endpoint Security die Datei oder das Skript nicht.

   d. Um die Datei hinzuzufügen, können Sie den Datei-Hash (SHA256 oder MD5), den vollständigen Dateipfad oder sowohl den Hash als auch den Pfad eingeben.

   Hinweis: Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie den Dateipfad wie folgt ein: /Volumes/Freigegebener_Ordner/Dateiname. Falls der Dateipfad einen Netzlaufwerksbuchstaben enthält, wird Kaspersky Endpoint Security die Datei oder das Skript nicht blockieren.

   a. Klicken Sie auf **OK**.

8. Speichern Sie die Änderungen.

Dadurch blockiert Kaspersky Endpoint Security die Ausführung von ausführbaren Dateien und Skripten sowie das Öffnen von Dateien im Office-Format. Eine Skriptdatei kann jedoch beispielsweise in einem Texteditor geöffnet werden, selbst wenn die Ausführung des Skripts verhindert ist. Wenn die Ausführung eines Objekts blockiert wird und die Benachrichtigungen in den Anwendungseinstellungen aktiviert sind, zeigt Kaspersky Endpoint Security eine Standardbenachrichtigung an.

Netzwerkisolation eines Computers

Die Netzwerkisolation eines Computers ermöglicht die automatische Isolierung eines Computers vom Netzwerk, wenn ein Kompromittierungsindikator (IOC) erkannt wird. Dies geschieht automatisch (automatischer Modus). Sie können die Netzwerkisolation auch manuell aktivieren, etwa während Sie eine erkannte Bedrohung untersuchen (manueller Modus).

Wenn die Netzwerkisolation aktiviert ist, trennt die Anwendung alle aktiven Verbindungen und blockiert alle neuen TCP/IP-Netzwerkverbindungen auf dem Computer, mit Ausnahme der folgenden:

- Verbindungen, die als Ausnahmen für die Netzwerkisolation angegeben sind.
- Verbindungen, die von Kaspersky Endpoint Security-Diensten initiiert werden.
- Verbindungen, die vom Kaspersky Security Center-Administrationsagenten initiiert werden.

Wichtig: Sie können die Einstellungen der Komponente nur in der Web Console konfigurieren.

Modus für die automatische Netzwerkisolation

Sie können die Netzwerkisolation so konfigurieren, dass sie als Reaktion auf eine IOC-Erkennung automatisch aktiviert wird. Sie können den automatischen Modus der Netzwerkisolation mithilfe einer Gruppenrichtlinie konfigurieren.

So können Sie die Netzwerkisolation so konfigurieren, dass sie als Reaktion auf eine IOC-Erkennung automatisch aktiviert wird

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Aufgaben** aus.
2. Die Liste mit Aufgaben wird geöffnet.
3. Klicken Sie auf die Aufgabe **IOC-Untersuchung** von Kaspersky Endpoint Security.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Erstellen Sie bei Bedarf die Aufgabe IOC-Untersuchung.
4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
5. Aktivieren Sie im Block **Aktion, wenn IOC erkannt wird** die Option **Warnen und Antwortaktionen ausführen, wenn ein IOC gefunden wurde** und aktivieren Sie anschließend das Kontrollkästchen **Computer vom Netzwerk isolieren (8 Stunden)**.
6. Speichern Sie die Änderungen.
7. Wenn ein IOC erkannt wird, isoliert die Anwendung den Computer vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern.

Sie können die Netzwerkisolation so konfigurieren, dass sie nach Ablauf eines bestimmten Zeitraums automatisch deaktiviert wird. Standardmäßig deaktiviert die Anwendung die Netzwerkisolation 8 Stunden nach deren Aktivierung. Sie können die Netzwerkisolation auch manuell deaktivieren (siehe Anleitung unten). Nach dem Deaktivieren der Netzwerkisolation kann der Computer das Netzwerk wieder uneingeschränkt verwenden.

So konfigurieren Sie den Zeitraum zum Deaktivieren der Netzwerkisolation eines Computers im automatischen Modus

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.
5. Klicken Sie im Block **Netzwerkisolation** auf **Einstellungen für das Aufheben der Netzwerkisolation von Computern konfigurieren**.
6. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Isolation des Computers automatisch aufheben nach** und geben Sie den Zeitraum für das automatische Deaktivieren der Netzwerkisolation ein.
7. Speichern Sie die Änderungen.

Modus für die manuelle Netzwerkisolation

Sie können die Netzwerkisolation manuell ein- und ausschalten. Den manuellen Modus zur Netzwerkisolation können Sie über die Computereigenschaften in der Kaspersky Security Center-Konsole anpassen.

Sie können die Netzwerkisolation aktivieren:

- In den Alarmdetails (nur für EDR Optimum).

  Die *Alarmdetails* sind ein Tool zum Anzeigen aller gesammelten Informationen über eine erkannte Bedrohung. Zu den Alarmdetails gehört beispielsweise der Verlauf der auf dem Computer veränderten Dateien. Weitere Informationen zur Verwaltung der Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

- Unter Verwendung der lokaler Anwendungseinstellungen.

So aktivieren Sie die Netzwerkisolation eines Computers manuell

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Verwaltete Geräte** aus.
2. Wählen Sie den Computer aus, für den Sie die lokalen Anwendungseinstellungen konfigurieren möchten.

   Die Computereigenschaften werden angezeigt.
3. Wechseln Sie zum Abschnitt **Anwendungen**.
4. Klicken Sie auf **Kaspersky Endpoint Security for Mac**.

   Die lokalen Anwendungseinstellungen werden angezeigt.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.
7. Klicken Sie im Block **Netzwerkisolation** auf **Computer vom Netzwerk isolieren**.

Sie können die Netzwerkisolation so konfigurieren, dass sie nach Ablauf eines bestimmten Zeitraums automatisch deaktiviert wird. Standardmäßig deaktiviert die Anwendung die Netzwerkisolation 8 Stunden nach deren Aktivierung. Nach dem Deaktivieren der Netzwerkisolation kann der Computer das Netzwerk wieder uneingeschränkt verwenden.

So konfigurieren Sie den Zeitraum zum Deaktivieren der Netzwerkisolation eines Computers im manuellen Modus

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Verwaltete Geräte** aus.
2. Wählen Sie den Computer aus, für den Sie die lokalen Anwendungseinstellungen konfigurieren möchten.
   Die Computereigenschaften werden angezeigt.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
   Die Liste der auf dem Computer verfügbaren Aufgaben wird angezeigt.
4. Wählen Sie die Aufgabe **Netzwerkisolation** aus.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Legen Sie im angezeigten Fenster den Zeitraum für die Deaktivierung der Netzwerkisolation fest.
7. Speichern Sie die Änderungen.

So deaktivieren Sie die Netzwerkisolation eines Computers manuell

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Verwaltete Geräte** aus.
2. Wählen Sie den Computer aus, für den Sie die lokalen Anwendungseinstellungen konfigurieren möchten.
3. Die Computereigenschaften werden angezeigt.
4. Wechseln Sie zum Abschnitt **Anwendungen**.
5. Klicken Sie auf Kaspersky Endpoint Security for Mac.
6. Die lokalen Anwendungseinstellungen werden angezeigt.
7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
8. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.
9. Klicken Sie im Block **Netzwerkisolation** auf **Netzwerkisolation des Computers aufheben**.

Sie können die Netzwerkisolation auch lokal über die Befehlszeile deaktivieren.

Ausnahmen für die Netzwerkisolation

Sie können Ausnahmen für die Netzwerkisolation angeben. Netzwerkverbindungen, die den Regeln entsprechen, werden auf dem Computer mit aktivierter Netzwerkisolation nicht blockiert.

Um die Ausnahmen für die Netzwerkisolation zu konfigurieren, können Sie eine Liste mit Standardnetzwerkprofilen verwenden. Zu den Ausnahmen gehören standardmäßig Netzwerkprofile mit Regeln, die sicherstellen, dass Geräte mit den Rollen DNS/DHCP-Server und DNS/DHCP-Client unterbrechungsfrei funktionieren. Sie können die Einstellungen der Standardnetzwerkprofile auch ändern oder manuell Ausnahmen definieren (siehe Anleitung unten).

Wichtig: Die in den Richtlinieneigenschaften angegebenen Ausnahmen werden nur angewendet, wenn die Netzwerkisolation als Reaktion auf eine erkannte Bedrohung automatisch aktiviert wird. Die in den Computereigenschaften angegeben Ausnahmen werden nur angewendet, wenn die Netzwerkisolation in den Computereigenschaften der Konsole von Kaspersky Security Center manuell aktiviert wird.

Hinweis: Eine aktive Richtlinie verhindert nicht die Anwendung von Ausnahmen der für die Netzwerkisolation, die in den Computereigenschaften konfiguriert sind. Diese Parameter besitzen unterschiedliche Verwendungsszenarien.

So fügen Sie der Netzwerkisolation eine Ausnahme im automatischen Modus hinzu

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
3. Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
5. Wechseln Sie zu **Erkennung und Reaktion** > **Endpoint Detection and Response**.
6. Klicken Sie im Block **Ausnahmen der Netzwerkisolation** auf **Ausnahmen**.
7. Dadurch wird ein neues Fenster geöffnet. Klicken Sie in diesem Fenster auf **Aus Profil hinzufügen** und wählen Sie Standardnetzwerkprofile aus, um die Ausnahmen zu konfigurieren.
8. Die Ausnahmen der Netzwerkisolation aus dem Profil werden zur Liste mit den Ausnahmen der Netzwerkisolation hinzugefügt. Sie können die Eigenschaften von Netzwerkverbindungen anzeigen. Bei Bedarf können Sie die Einstellungen der Netzwerkverbindung ändern.
9. Bei Bedarf können Sie eine Ausnahme für die Netzwerkisolation manuell hinzufügen. Klicken Sie dazu im Fenster mit der Liste der Ausnahmen auf **Hinzufügen** und bearbeiten Sie die Einstellungen der Netzwerkverbindung manuell.
10. Speichern Sie die Änderungen.

So fügen Sie der Netzwerkisolation eine Ausnahme im manuellen Modus hinzu

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Verwaltete Geräte** aus.
2. Wählen Sie den Computer aus, für den Sie die lokalen Anwendungseinstellungen konfigurieren möchten.
3. Die Computereigenschaften werden angezeigt.
4. Wählen Sie die Registerkarte **Aufgaben** aus.
5. Die Liste der auf dem Computer verfügbaren Aufgaben wird angezeigt.

6. Wählen Sie die Aufgabe **Netzwerkisolation aus**.
7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
8. Klicken Sie im folgenden Fenster auf **Ausnahmen**.
9. Klicken Sie im nächsten Fenster auf **Aus Profil hinzufügen** und wählen Sie Standardnetzwerkprofile aus, um die Ausnahmen zu konfigurieren.
10. Die Ausnahmen der Netzwerkisolation aus dem Profil werden zur Liste mit den Ausnahmen der Netzwerkisolation hinzugefügt. Sie können die Eigenschaften von Netzwerkverbindungen anzeigen. Bei Bedarf können Sie die Einstellungen der Netzwerkverbindung ändern.
11. Bei Bedarf können Sie eine Ausnahme für die Netzwerkisolation manuell hinzufügen. Klicken Sie dazu im Fenster mit der Liste der Ausnahmen auf **Hinzufügen** und bearbeiten Sie die Einstellungen der Netzwerkverbindung manuell.
12. Speichern Sie die Änderungen.

Sie können die Liste mit den Ausnahmen der Netzwerkisolation auch lokal über die Befehlszeile anzeigen. In diesem Fall muss der Computer isoliert werden.

Cloud Sandbox

Mit der Technologie *Cloud Sandbox* können Sie komplexe Bedrohungen auf einem Computer erkennen. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox“ weiter. „Cloud Sandbox“ führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivität zu erkennen, und entscheidet dann über ihre Reputation. Daten über diese Dateien werden an Kaspersky Security Network gesendet. Wenn Cloud Sandbox eine bösartige Datei erkennt, führt Kaspersky Endpoint Security die entsprechende Aktion aus, um die Bedrohung auf allen Computern zu entfernen, auf denen diese Datei gefunden wurde.

Wichtig: Damit Cloud Sandbox ordnungsgemäß funktioniert, müssen Sie die Verwendung von Kaspersky Security Network aktivieren.

Hinweis: Wenn Sie Kaspersky Private Security Network verwenden, steht die Cloud Sandbox nicht zur Verfügung.

So aktivieren Sie Cloud Sandbox:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zu **Detection and Response** > **Endpoint Detection and Response**.

5. Aktivieren Sie den Umschalter **Cloud Sandbox**.

6. Speichern Sie die Änderungen.

Sobald eine Bedrohung auftritt, aktiviert Kaspersky Endpoint Security im Programmhauptfenster im Abschnitt **Bedrohungserkennung** den Zähler für Bedrohungen, die mit Cloud Sandbox erkannt wurden. Kaspersky Endpoint Security geht außerdem im Bedrohungsbericht der Konsole von Kaspersky Security Center auf die Technologie zur Bedrohungserkennung von Cloud Sandbox ein

FileVault-Volume-Verschlüsselung

Hinweis: Die Funktion FileVault-Volume-Verschlüsselung ist in Kaspersky Security Center 10 SP3 oder höher verfügbar. Weitere Informationen erhalten Sie vom Technischen Support von Kaspersky.

Kaspersky Endpoint Security erlaubt es, die FileVault-Verschlüsselung per Fernzugriff zu verwalten. Die Verschlüsselung verhindert, dass unbefugte Benutzer auf sensible Daten zugreifen, die sich auf dem Startvolume des Computers befinden.

Wenn ein Administrator die FileVault-Verschlüsselung auf einem Computer aus Kaspersky Security Center startet, fordert Kaspersky Endpoint Security den Benutzer dieses Computers zur Eingabe seiner Anmeldedaten auf. Die Festplattenverschlüsselung wird erst gestartet, nachdem der Benutzer die Anmeldeinformationen angegeben hat, der Computer neu gestartet wurde und 30 Minuten vergangen sind, seit die Richtlinieneinstellungen auf dem Computer empfangen wurden. Das Mindestintervall zwischen den Aufforderungen zur Eingabe von Anmeldeinformationen beträgt ebenfalls 30 Minuten.

Um zu verhindern, dass der Benutzer das Startvolume seines Macs entschlüsselt, wenn die FileVault-Verschlüsselung aktiviert ist, muss der Administrator mithilfe von JAMF ein MDM-Profil bereitstellen, das die Entschlüsselung des Laufwerks untersagt. Zur Entschlüsselung des Startvolume eines Mac mit einem MDM-Profil, das die Entschlüsselung verbietet, muss der Administrator zuerst das Profil entfernen.

Hinweis: Wenn die Verwaltung für FileVault-Volume-Verschlüsselung in Kaspersky Security Center nicht aktiviert ist, können Benutzer mit Administratorrechten ihre Mac-Startvolumes in den Systemeinstellungen verschlüsseln und entschlüsseln. Weitere Informationen über FileVault finden Sie in der Apple-Dokumentation.

Befinden sich auf dem Computer mehrere Benutzerkonten, so wird das Volume durch die FileVault-Verschlüsselung für alle anderen Benutzer mit Ausnahme des Benutzers, der seine Anmeldedaten eingegeben hat, gesperrt.

Anderen Benutzern die Entsperrung des Volumes ermöglichen

1. Wählen Sie **Apple-Menü** > **Systemeinstellungen** > **Datenschutz & Sicherheit**.

2. Klicken Sie auf **FileVault**.

   Das Fenster **FileVault** wird geöffnet.

3. Klicken Sie auf **Benutzer aktivieren**.

4. Wählen Sie im folgenden Fenster einen Benutzer aus, den Sie zum Entsperren des Computers autorisieren möchten.

5. Geben Sie das Kennwort für das Computerkonto des Benutzers ein und klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter**.

Der Benutzer kann jetzt auf das verschlüsselte Volume zugreifen.

Hinweis: Für die Freigabe von Benutzern zum Entsperren des Volumes sind Administratorrechte erforderlich.

Wenn ein Administrator Kaspersky Endpoint Security über die Kaspersky Security Center-Verwaltungskonsole, „Web Console“ oder „Cloud Console“ verwaltet, und ein Benutzer dieses Computers seine Anmeldedaten vergisst oder verliert und nicht mehr auf ein verschlüsseltes Laufwerk zugreifen kann, kann der Administrator einen Wiederherstellungsschlüssel anfordern.

Anfordern eines Wiederherstellungsschlüssels mithilfe der Kaspersky Security Center Verwaltungskonsole

Anfordern eines Wiederherstellungsschlüssels mithilfe von Kaspersky Security Center Web Console und „Cloud Console“

Kennwortschutz

Kaspersky Endpoint Security ermöglicht es, unerwünschte Aktionen auf Benutzergeräten durch das Festlegen eines Administratorkennworts einzuschränken.

Wenn der Kennwortschutz aktiviert ist, erfordert Kaspersky Endpoint Security für die folgenden Aktionen die Eingabe eines Kennworts:

- Konfigurieren der von Anwendungseinstellungen
- Verlassen der Anwendung
- Entfernen des Lizenzschlüssels
- Deinstallieren der Anwendung

  Hinweis: Der Kennwortschutz betrifft die Deinstallation von Kaspersky Endpoint Security nur dann, wenn sie über das Deinstallationsprogramm durchgeführt wird.

- Wiederherstellen von Dateien in Quarantäne aus dem Backup
- Anzeigen von Berichten

Das Deaktivieren des Kennwortschutzes führt nicht zur Deaktivierung der Richtlinieneinstellungen. Wenn das Ändern einer Richtlinieneinstellung verboten ist, kann sie auch dann nicht bearbeitet werden, wenn kein Kennwortschutz aktiv ist.

Aktivieren des Kennwortschutzes über die Verwaltungskonsole

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.

3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** die Option **Weitere Einstellungen > Interaktion mit dem Benutzer** aus.
7. Aktivieren Sie im Abschnitt **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren**.
8. Konfigurieren Sie im angezeigten Fenster **Einstellungen des Kennwortschutzes** die folgenden Einstellungen:
   - Geben Sie das Kennwort im Feld **Kennwort** und zusätzlich im Feld **Kennwort bestätigen** ein.
   - Aktivieren Sie im Abschnitt **Kennwort erforderlich für** die erforderlichen Kontrollkästchen, um die entsprechenden Aktionen auf dem Gerät des Benutzers zu schützen.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.
10. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:
    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.
    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Ändern der Einstellungen des Kennwortschutzes über die Verwaltungskonsole

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** die Option **Weitere Einstellungen > Interaktion mit dem Benutzer** aus.
7. Klicken Sie im Abschnitt **Kennwortschutz** auf die Schaltfläche **Einstellungen**.
8. Passen Sie im neuen Fenster **Einstellungen des Kennwortschutzes** die Einstellungen an, die Sie ändern möchten.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Aktivieren des Kennwortschutzes über die Web Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.
3. Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
5. Wählen Sie **Weitere Einstellungen** > **Benutzerinteraktion** aus.
6. Aktivieren Sie den Umschalter **Kennwortschutz**.
7. Konfigurieren Sie im angezeigten Dialog **Einstellungen des Kennwortschutzes** die folgenden Einstellungen:
   - Geben Sie das Kennwort im Feld **Kennwort** und zusätzlich im Feld **Kennwort bestätigen** ein. Aus Sicherheitsgründen werden die Zeichen des Kennworts standardmäßig verborgen. Um das Kennwort anzuzeigen, klicken Sie auf **Anzeigen**.
   - Aktivieren Sie im Abschnitt **Kennwort erforderlich für** die erforderlichen Kontrollkästchen, um die entsprechenden Aktionen auf dem Gerät des Benutzers zu schützen.
8. Klicken Sie auf **OK**, um den Dialog **Einstellungen des Kennwortschutzes** zu schließen.
9. Klicken Sie auf **OK**, um den Abschnitt **Interaktion mit dem Benutzer** zu schließen.
10. Klicken Sie auf **Speichern**, um die Änderungen für die Richtlinie zu speichern.

Ändern des Kennwortschutzes über die Web Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security for Mac.
3. Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
5. Wählen Sie **Weitere Einstellungen** > **Benutzerinteraktion** aus.
6. Klicken Sie im Abschnitt **Kennwortschutz** auf die Schaltfläche **Einstellungen**.
7. Passen Sie im neuen Dialog **Einstellungen des Kennwortschutzes** die Einstellungen an, die Sie ändern möchten.
8. Klicken Sie auf **OK**, um den Dialog **Einstellungen des Kennwortschutzes** zu schließen.
9. Klicken Sie auf **OK**, um den Abschnitt **Interaktion mit dem Benutzer** zu schließen.
10. Klicken Sie auf **Speichern**, um die Änderungen für die Richtlinie zu speichern.

Aktivieren des Kennwortschutzes in der Anwendung von Kaspersky Endpoint Security

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.
   Das Fenster mit Anwendungseinstellungen wird geöffnet.
2. Aktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren**.

3. Konfigurieren Sie im angezeigten Fenster die folgenden Einstellungen:

   - Geben Sie das Kennwort im Feld **Kennwort** und zusätzlich im Feld **Kennwort bestätigen** ein.
   - Aktivieren Sie im Abschnitt **Kennwort erforderlich für** die erforderlichen Kontrollkästchen, um die entsprechenden Aktionen auf dem Gerät des Benutzers zu schützen.

4. Klicken Sie auf **OK**.

> **Hinweis:** Wenn Sie für die Aktion **Programmeinstellungen ändern** den Kennwortschutz aktiviert haben, müssen Sie das Kennwort zweimal eingeben, um die Einstellungen des Kennwortschutzes zu ändern.

Ändern des Kennwortschutzes in der Anwendung von Kaspersky Endpoint Security

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Kennwortschutz** auf **Einstellungen**.
3. Passen Sie im neuen Fenster die Einstellungen an, die Sie ändern möchten.
4. Klicken Sie auf **OK**.

Exploit-Prävention

Die Komponente Exploit-Prävention erkennt Programmcode, der Schwachstellen auf dem Computer ausnutzt, um Administratorrechte zu erhalten oder bösartige Aktivitäten auszuführen. Exploits können beispielsweise einen Angriff mit Überlauf der Zwischenablage verwenden. Dazu sendet der Exploit große Datenvolumen an ein verwundbares Programm. Bei der Verarbeitung dieser Daten führt das verwundbare Programm schädlichen Code aus. Aufgrund dieses Angriffs kann der Exploit eine nicht autorisierte Installation von Schadsoftware starten. Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer ausgeführt wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei oder informiert den Benutzer.

Die Exploit-Prävention ist standardmäßig aktiviert. Bei Bedarf können Sie die Exploit-Prävention deaktivieren.

Exploit-Prävention aktivieren/deaktivieren (über die Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Erweiterter Schutz** > **Exploit-Prävention**.
5. Aktivieren/deaktivieren Sie den Schalter **Exploit-Prävention**.

6. Wenn die Exploit-Prävention aktiviert ist, wählen Sie eine der folgenden Aktionen aus, die beim Erkennen eines Exploits ausgeführt werden soll:

   - **Blockieren**

     Wenn diese Option ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Protokolleintrag, der Informationen über diesen Exploit enthält.

   - **Informieren**

     Wenn diese Option ausgewählt ist, protokolliert Kaspersky Endpoint Security beim Fund eines Exploits Informationen über den Exploit und fügt Informationen über den Exploit zur Liste der aktiven Bedrohungen hinzu.

7. Speichern Sie die Änderungen.

Exploit-Prävention aktivieren/deaktivieren (über die Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Erweiterter Schutz** > **Exploit-Prävention** aus.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Exploit-Prävention**.
8. Wählen Sie im Abschnitt **Wenn ein Exploit erkannt wird** aus, welche Aktion ausgeführt werden soll, wenn Kaspersky Endpoint Security einen Exploit erkennt.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.
10. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.
    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Exploit-Prävention aktivieren/deaktivieren (über die Anwendung Kaspersky Endpoint Security)

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren oder deaktivieren Sie auf der Registerkarte **Erweitert** im Abschnitt „Exploit-Prävention“ das Kontrollkästchen **Exploit-Prävention aktivieren**.

3. Wenn das Kontrollkästchen **Verhaltensanalyse aktivieren** aktiviert ist, wählen Sie eine der folgenden Aktionen aus, die beim Fund von Malware ausgeführt werden soll:

   - **Gefährliche Malware-Aktivitäten automatisch blockieren**

     Wenn diese Option ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Protokolleintrag, der Informationen über diesen Exploit enthält.

   - **Informieren**

     Wenn diese Option ausgewählt ist, protokolliert Kaspersky Endpoint Security beim Fund eines Exploits Informationen über den Exploit und fügt Informationen über den Exploit zur Liste der aktiven Bedrohungen hinzu.

Bericht für die Exploit-Prävention anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffnen Sie die Registerkarte **Exploit-Prävention**.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- **Dateiaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - Löschen ausführbarer Dateien, die von Malware erstellt wurden (auf allen Datenträgern außer Netzlaufwerken).
  - Löschen ausführbarer Dateien, die von Programmen erstellt wurden, die durch Malware infiltriert sind.
  - Wiederherstellen von Dateien, die durch Malware verändert oder gelöscht wurden.

- **Systemaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - Beenden von Prozessen, die von Malware initiiert wurden.
  - Beenden von Prozessen, in die ein bösartiges Programm eingedrungen ist.
  - Fortsetzen von Prozessen, die durch Malware angehalten wurden.

- **Netzwerkaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - Blockieren von schädlicher Netzwerkaktivität.

Ein Rollback von schädlichen Aktionen kann von der Komponente „Schutz vor bedrohlichen Dateien“ oder „Verhaltensanalyse“ sowie während einer Malware-Untersuchung gestartet werden.

Das Rollback von schädlichen Vorgängen betrifft einen streng definierten Datensatz. Das Rollback hat keine negativen Auswirkungen auf das Betriebssystem oder die Integrität der Computerdaten.

Rollback von schädlichen Aktionen aktivieren/deaktivieren (in der Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Erweiterter Schutz** > **Rollback von schädlichen Aktionen** aus.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.
9. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:
   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.
   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Rollback von schädlichen Aktionen aktivieren/deaktivieren (in der Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Erweiterter Schutz** > **Rollback von schädlichen Aktionen**.
5. Aktivieren oder deaktivieren Sie den Schalter **Rollback von schädlichen Aktionen**.
6. Speichern Sie die Änderungen.

Rollback von schädlichen Aktionen aktivieren/deaktivieren (in der Programmoberfläche)

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.
2. Aktivieren oder deaktivieren Sie auf der Registerkarte **Erweitert** im Abschnitt Rollback von schädlichen Aktionen das Kontrollkästchen **Rollback von schädlichen Aktionen aktivieren**.

Wenn Rollback von schädlichen Aktionen aktiviert ist, rollt Kaspersky Endpoint Security die von bösartigen Programmen im Betriebssystem ausgeführten Aktionen zurück.

Web-Kontrolle

Die Web-Kontrolle steuert den Zugriff von Benutzern auf Webressourcen. Dies trägt dazu bei, den Datenverkehr zu reduzieren und die unsachgemäße Nutzung der Arbeitszeit einzuschränken. Wird versucht, eine durch die Web-Kontrolle eingeschränkte Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff oder zeigt eine Warnung an.

Sie können den Zugriff auf bestimmte Websites oder ausgewählte Website-Kategorien blockieren.

Hinweis: Die Anwendung Kaspersky Endpoint Security kann nur den Zugriff auf Websites blockieren, die HTTPS für ihre Verbindungen verwenden. Verschlüsselte Verbindungen (HTTPS) werden nur dann von der Anwendung untersucht, wenn das Kontrollkästchen **Sichere Verbindungen (HTTPS) untersuchen** im Abschnitt **Allgemein** auf der Registerkarte **Basis** aktiviert ist.

Neue Regel hinzufügen (in der Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Sicherheitskontrolle** > **Web-Kontrolle** aus.
7. Aktivieren Sie das Kontrollkästchen **Web-Kontrolle aktivieren**.
8. Klicken Sie auf **Hinzufügen**.
9. Geben Sie im folgenden Fenster einen Namen für die Regel ein.
10. Wenn Sie möchten, dass die Regel aktiv ist, aktivieren Sie das Kontrollkästchen **Aktive Regel**.
11. Führen Sie eine der folgenden Aktionen aus:
    - Wenn die Regel für bestimmte Webadressen gelten soll, wählen Sie die Option **Webadresse oder eine Gruppe von Webadressen durch Maske** aus.
    - Wenn die Regel für bestimmte Website-Kategorien gelten soll, wählen Sie die Option **Website-Kategorien** aus.
12. Klicken Sie auf **Angeben**.
13. Geben Sie im folgenden Fenster den Bereich für die Regel an.

14. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Kaspersky Endpoint Security den Zugriff blockieren soll, wählen Sie die Option **Blockieren** aus.
    - Wenn Kaspersky Endpoint Security den Zugriff erlauben soll, wählen Sie die Option **Erlauben** aus.
    - Wenn Kaspersky Endpoint Security eine Warnung anzeigen soll, wählen Sie die Option **Warnung anzeigen** aus.

15. Klicken Sie auf **OK**, um die Änderungen zu speichern.

16. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.
    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Neue Regel hinzufügen (in der Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** > **Web-Kontrolle**.
5. Aktivieren Sie den Schalter **Web-Kontrolle**.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie im folgenden Fenster einen Namen für die Regel ein.
8. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Sie möchten, dass die Regel aktiv ist, wählen Sie die Option **Aktiv** aus.
    - Wenn Sie möchten, dass die Regel inaktiv ist, wählen Sie die Option **Inaktiv** aus.

9. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Kaspersky Endpoint Security den Zugriff erlauben soll, wählen Sie die Option **Erlauben** aus.
    - Wenn Kaspersky Endpoint Security den Zugriff blockieren soll, wählen Sie die Option **Blockieren** aus.
    - Wenn Kaspersky Endpoint Security eine Warnung anzeigen soll, wählen Sie die Option **Warnung anzeigen** aus.

10. Führen Sie eine der folgenden Aktionen aus:

    - Wenn die Regel für bestimmte Website-Kategorien gelten soll, wählen Sie die Option **Kategorien** aus, klicken Sie auf **Kategorien auswählen** und geben Sie die Kategorien an.

    - Wenn die Regel für bestimmte Webadressen gelten soll, wählen Sie die Option **Individuelle Adressen** aus und fügen Sie die Webadressen darunter in der Tabelle hinzu.

11. Speichern Sie die Änderungen.

Hinweis: Die Einstellungen der Web-Kontrolle können nicht in Kaspersky Endpoint Security verwaltet werden.

Gerätekontrolle

Die Gerätekontrolle verwaltet den Benutzerzugriff auf Geräte, die auf dem Computer installiert oder mit dem Computer verbunden sind. Auf diese Weise können Sie den Computer vor Infektionen schützen, wenn solche Geräte angeschlossen werden, und den Verlust oder das Abfließen von Daten verhindern.

Ebenen für den Zugriff auf Geräte

Die Gerätekontrolle kontrolliert den Zugriff auf den folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger und CD/DVD-Laufwerke.

  Sie können den Gerätezugriff wie folgt konfigurieren:

  - Erlauben.

  - Blockieren.

  - Verbieten mit Ausnahmen (nur WLAN).

- **Vertrauenswürdige Geräte.** Vertrauenswürdige Geräte sind Geräte, auf die Benutzer, die in den Einstellungen für vertrauenswürdige Geräte angegeben sind, immer vollständigen Zugriff haben.

  Vertrauenswürdige Geräte können anhand der folgenden Daten hinzugefügt werden:

  - **Geräte nach ID**. Jedes Gerät hat eine eindeutige ID (Hardware-ID oder HWID). Die ID können Sie in den Geräteeigenschaften mithilfe von Betriebssystem-Tools anzeigen. Beispiel für eine Geräte-ID: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. Die Angabe von Geräte-IDs ist praktisch, wenn Sie mehrere bestimmte Geräte hinzufügen möchten.

  - **Geräte nach Modell**. Jedes Gerät besitzt eine Hersteller-ID (VID) und eine Produkt-ID (PID). Die IDs können Sie in den Geräteeigenschaften mithilfe von Betriebssystem-Tools anzeigen. Muster für die Eingabe der VID und PID: VID_1234&PID_5678. Die Angabe von Geräten nach Modell ist praktisch, wenn Sie in Ihrem Unternehmen Geräte eines bestimmten Modells verwenden. Auf diese Weise können Sie alle Geräte dieses Modells hinzufügen.

- **Geräte nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs verwenden, können Sie Masken verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht für eine beliebige Zeichenfolge. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.

- **Geräte nach Modellmaske**. Wenn Sie mehrere Geräte mit ähnlichen VIDs oder PIDs verwenden (z. B. Geräte desselben Herstellers), können Sie Masken verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht für eine beliebige Zeichenfolge. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Zum Beispiel: `VID_05AC&PID_*`.

Komponente „Gerätekontrolle“ verwalten (in der Verwaltungskonsole)

1. Starten Sie die Verwaltungskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Wählen Sie im Fenster **Eigenschaften** den Punkt **Sicherheitskontrolle** > **Gerätekontrolle** aus.
7. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
8. Konfigurieren Sie auf der Registerkarte **Gerätetypen** die Zugriffsregeln für Gerätetypen und WLAN-Netzwerke.
9. Konfigurieren Sie auf der Registerkarte **Vertrauenswürdige Geräte** die Zugriffsregeln für bestimmte Geräte oder Gerätegruppen.
10. Klicken Sie auf **OK**, um die Änderungen zu speichern.
11. Führen Sie eine der folgenden Aktionen aus, um die Änderungen der Richtlinie zu übernehmen:

    - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

    - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Komponente „Gerätekontrolle“ verwalten (in der Web Console)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Assets (Geräte)** > **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** > **Gerätekontrolle**.
5. Aktivieren Sie den Schalter **Gerätekontrolle**.

6. Konfigurieren Sie auf der Registerkarte **Einstellungen der Gerätekontrolle** die Zugriffsregeln für Geräte, Gerätetypen und WLAN-Netzwerke.

7. Speichern Sie die Änderungen.

Hinweis: Die Einstellungen der Gerätekontrolle können nicht in Kaspersky Endpoint Security verwaltet werden.

Wenn die Gerätekontrolle aktiviert ist, leitet das Programm Informationen über angeschlossene Geräte an das Kaspersky Security Center weiter. Eine Liste der verbundenen Geräte können Sie in Kaspersky Security Center unter **Erweitert** → **Datenverwaltungen** → **Hardware-Ordner** einsehen.

Bericht der Gerätekontrolle anzeigen

1. Wählen Sie in der Menüleiste den Punkt **Schutz** > **Berichte** aus.

   Das Fenster **Berichte** wird geöffnet.

2. Öffne die Registerkarte **Gerätekontrolle**.

An Kaspersky Security Network teilnehmen

Wenn Sie an Kaspersky Security Network teilnehmen, werden statistische Daten zum Programm Kaspersky Endpoint Security automatisch an Kaspersky gesendet, um Ihren Mac besser zu schützen.

Hinweis: Ohne Ihre ausdrückliche Zustimmung empfängt, verarbeitet oder speichert Kaspersky keine personenbezogenen Daten.

Die Teilnahme an Kaspersky Security Network ist freiwillig. Sie entscheiden im Verlauf der Programminstallation über die Teilnahme. Sie können diese Entscheidung jederzeit ändern.

Kaspersky Security Network aktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Klicken Sie auf der Registerkarte **Erweitert** im Abschnitt **KSN** auf **KSN-Erklärung anzeigen**, um die Erklärung zu Kaspersky Security Network zu öffnen.

3. Wenn Sie möchten, dass Kaspersky Endpoint Security von Kaspersky Security Network Informationen über die Reputation von Dateien, Webressourcen und Anwendungen erhält, und wenn Sie alle Bedingungen der Erklärung akzeptieren, aktivieren Sie das Kontrollkästchen **An Kaspersky Security Network teilnehmen**.

4. Klicken Sie im folgenden Fenster auf **Bestätigen**.

   Die Kontrollkästchen **An Kaspersky Security Network teilnehmen** und **Erweiterten KSN-Modus aktivieren** werden aktiviert.

Hinweis: Kaspersky Endpoint Security verwendet standardmäßig den „Erweiterten KSN-Modus“. Im *Erweiterten KSN-Modus* sendet Kaspersky Endpoint Security zusätzliche Daten an Kaspersky. Wenn Sie diese Daten nicht bereitstellen möchten, deaktivieren Sie das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**.

Daten, die an Kaspersky bereitgestellt werden, wenn Kaspersky Security Network verwendet wird

Wenn das Kontrollkästchen **An Kaspersky Security Network teilnehmen** aktiviert ist und das Kontrollkästchen **Erweiterten KSN-Modus aktivieren** deaktiviert ist, stellt Kaspersky Endpoint Security die folgenden Daten an Kaspersky bereit:

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Vollversion der installierten Software;
  Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; einmalige Geräte-ID Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

Wenn die Kontrollkästchen **An Kaspersky Security Network teilnehmen** und **Erweiterten KSN-Modus aktivieren** aktiviert sind, stellt Kaspersky Endpoint Security die folgenden Daten an Kaspersky bereit:

- Informationen über die Version des Betriebssystems (OS) und die auf dem Computer installierten Service Packs, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems, Parameter des Funktionsmodus des Betriebssystems; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Windows Service Packs; Datum und Uhrzeit des Betriebssystemstarts; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Verhaltensanalyse-Subsystem; Anzahl der verzögerten Aktionsereignisse des Betriebssystems des aktuellen Typs; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Subsystem für den proaktiven Schutz; Anzahl der verarbeiteten Aktionsereignisse des Betriebssystems; Anzahl der verarbeiteten synchronen Aktionsereignisse des Betriebssystems; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems des aktuellen Typs; Verarbeitungsverzögerungszeit des Ereignisses über die Betriebssystemaktion im Subsystem für die persistente Ereignisspeicherung; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems; Anzahl der wartenden synchronen Aktionsereignisse des Betriebssystems; Datum und Uhrzeit des empfangenen Ereignisses über eine Aktion im Betriebssystem.

- Informationen über den fehlgeschlagenen letzten Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.

- Informationen über die installierte Anwendung des Rechtsinhabers und den Status des Antiviren-Schutzes: ID der Software-Installation (PCID) Version des Software-Datenbankeintrags; eindeutige ID der Instanz der Anwendungsinstallation auf dem Computer, Anwendungstyp, Anwendungstyp-ID, die Vollversion der installierten Anwendung, ID der Version der Anwendungseinstellungen, ID des Computertyps, eindeutige ID des Computers, auf dem die Anwendung installiert ist, eindeutige Benutzer-ID beim Dienst des Rechteinhabers, lokale Sprache und Betriebszustand, Version der installierten Softwarekomponenten und ihr Betriebszustand, Version des verwendeten Protokolls zur Verbindungsherstellung zum Dienst des Rechteinhabers; Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Anzahl der Update-Anwendungs-Zyklen für die Antiviren-Datenbanken; Zeitpunkt (Datum und Uhrzeit), an dem die Antiviren-Datenbanken zuletzt aktualisiert und angewendet wurden; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version der Software-Komponente; ID des Software-Updates; Typ der installierten Software; Startdatum und -uhrzeit vom Aktivitätsmonitor; Installationsdatum und -uhrzeit der Software; Wahrscheinlichkeit der Übermittlung von Statistiken durch den Aktivitätsmonitor; Code des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Datenbank-Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; maximal zulässige Zeit für die Verarbeitung eines Ereignisses durch den Aktivitätsmonitor; Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Gesamtzahl der Ereignisse, die länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert haben.

- Informationen über alle verarbeiteten Objekte und Vorgänge: Verdikt der Software für das verarbeitete Objekt; Verzeichniscode; Größe des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Anzahl der erkannten Software im Kontext des „Aktivitätsmonitors“; Zeitpunkt (Datum und Uhrzeit), zu dem der „Aktivitätsmonitor“ die Software erkannt hat; Erkennungscharakteristiken; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Grund, aus dem der „Aktivitätsmonitor“ die Software erkannt hat; Prüfsumme (MD5) des verarbeiteten Objekts; Ergebnis der Modul-Integritätsprüfung; Name des verarbeiteten Objekts; Typ des ausgelösten Eintrags der Antiviren-Datenbanken der Software; Speicherpfad des verarbeiteten Objekts; Name des untersuchten Objekts; Datum und Uhrzeit der Untersuchung; URL-Adresse und Referenzadresse, von denen es heruntergeladen wurde; Größe und Pfade der untersuchten Dateien; Zeichen des Archivs; Datum und Uhrzeit der Dateierstellung; Name, Größe und Prüfsummen (MD5, SHA2-256) des Packers (falls die Datei gepackt wurde); Entropie der Datei; Typ der Datei; Code des Dateityps; Zeichen, ID und Format der ausführbaren Datei; Prüfsumme des Objekts (MD5, SHA2-256); Typ und Wert der zusätzlichen Prüfsumme des Objekts; Daten über die digitale Signatur des Objekts (Zertifikat): Daten über den Herausgeber des Zertifikats, Anzahl der Starts des Objekts seit der letzten Übermittlung von Statistiken, ID der Überprüfungsaufgabe der Anwendung, Mittel zum Erhalt von Informationen über den Ruf des Objekts, Wert des Zielfilters, technische Parameter der anwendbaren Erkennungstechnologien; Speicherpfad des verarbeiteten Objekts; Verzeichniscode.

- Für ausführbare Dateien: Entropie der Dateiabschnitte, Kennzeichen der Reputations-Überprüfung oder Kennzeichen der Dateisignatur, Name, Typ, ID-Typ, Prüfsumme (MD5) und Größe der Anwendung, die vom zu validierenden Objekt geladen wurde, Anwendungspfad und Vorlagenpfade, Attribut, das das Vorhandensein in der Autostart-Liste angibt, Datum des Eintrags, Liste mit Attributen, Name des Packers, Informationen über die digitale Signatur der Anwendung: Herausgeberzertifikat, Name der hochgeladenen Datei im MIME-Format, Datum und Uhrzeit der Dateierstellung.

- Informationen über die gestarteten Anwendungen und deren Module: Prüfsummen (MD5, SHA2-256) von ausgeführten Dateien, Größe, Attribute, Erstellungsdatum, Name des Packers (falls die Datei gepackt wurde), Dateinamen, Informationen über die im System ausgeführten Prozesse (Prozess-ID (PID), Prozessname, Informationen über das Benutzerkonto, aus dem der Prozess gestartet wurde, Anwendung und Befehl, mit dem der Prozess gestartet wurde, vollständiger Pfad der Dateien des Prozesses sowie auszuführende Befehlszeile, Beschreibung der Anwendung, zu dem der Prozess gehört (Name der Anwendung und Informationen über den Herausgeber) sowie die verwendeten digitalen Zertifikate und Informationen, die zur Überprüfung ihrer Authentizität dienen, oder Informationen über das Fehlen einer digitalen Signatur einer Datei) und Informationen über die in die Prozesse geladenen Module: deren Namen, Größen, Typen, Erstellungsdaten, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfade, Header-Informationen der PE-Datei, Namen der Packer (falls die Datei gepackt wurde), Informationen über die Verfügbarkeit und Gültigkeit dieser Statistiken, ID des Modus zur Erstellung von zu sendenden Statistiken.

- Falls Bedrohungen oder Schwachstellen erkannt werden, werden zusätzlich zu den Informationen über das erkannte Objekt auch die folgenden Informationen bereitgestellt: ID, Version und Typ des Eintrags in der Antiviren-Datenbank, Name der Bedrohung, basierend auf der Klassifikation von Kaspersky, Datum und Uhrzeit der letzten Aktualisierung der Antiviren-Datenbank, Name der ausführbaren Datei, Prüfsumme (MD5) der Anwendungsdatei, welche die Webadresse, unter der die Bedrohung erkannt wurde, angefordert hat, IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, ID der Schwachstelle und ihre Gefahrenstufe, URL und Referenz der Webseite, auf der die Schwachstelle gefunden wurde.

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt.

- Informationen über einen Netzwerkangriff: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.

- Informationen zu Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, aus der der Prozess gestartet wurde, der den Port geöffnet hat, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Verbindungsports, Verbindungsstatus, Zeitstempel für das Öffnen des Ports.

- URL- und IP-Adresse der Webseite, auf der schädliche oder verdächtige Inhalte erkannt wurden, Name, Größe und Prüfsumme der Datei, die die URL anforderte, Kennung, Priorität und Grad der Regel, die für die Entscheidung verwendet wurde, Ziel des Angriffs.

- Informationen über Updates der installierten App- und Antiviren-Datenbanken: Bearbeitungsstand der Update-Aufgabe, Art des Fehlers, der möglicherweise während des Update-Vorgangs aufgetreten ist, Anzahl der fehlgeschlagenen Updates, ID der Anwendungskomponente, die die Updates ausführt.

- Informationen über die Nutzung von Kaspersky Security Network (KSN): KSN-ID, Anwendungs-ID, vollständige Version der Anwendung, anonymisierte IP-Adresse des Benutzergerätes, Indikatoren für die Qualität der Ausführung von KSN-Anfragen, Indikatoren für die Qualität der Verarbeitung von KSN-Paketen, Indikatoren für die Anzahl der KSN-Anfragen und Informationen über die Arten von KSN-Anfragen, Datum und Uhrzeit für den Beginn des Sendevorgangs von Statistiken, Datum und Uhrzeit für das Ende des Sendevorgangs von Statistiken, Informationen über die Aktualisierung der KSN-Konfiguration: ID der aktiven Konfiguration, ID der empfangenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen zu Systemprotokoll-Ereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.

- Informationen zur Bestimmung der Reputation von Dateien und URL-Adressen: URL-Adresse, unter der die Reputation angefordert wird, und Referrer, Protokolltyp der Verbindung, interne ID des Anwendungstyps, Nummer des verwendeten Ports, Benutzer-ID, Prüfsumme der untersuchten Datei (MD5), Typ der erkannten Bedrohung, Informationen über den Datensatz, der zum Erkennen der Bedrohung verwendet wurde (ID des Datensatzes für die Antiviren-Datenbanken, Zeitstempel und Typ des Datensatzes); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

- Daten zur geografischen Verteilung der Anwendung: Datum der Anwendungsinstallation und -aktivierung, ID des Partners, der die Lizenz für die Anwendungsaktivierung bereitstellt, Anwendungs-ID, Lokalisierungs-ID der Anwendungssprache, Lizenz-Seriennummer für die Anwendungsaktivierung, Merkmal für die KSN-Teilnahme.

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Informationen über die auf dem Computer installierte Hardware: Typ, Name, Modellname, Firmware-Version, Parameter der integrierten und angeschlossenen Geräte.

- Informationen über das Gerät: Geräte-ID.

- Informationen zum Betrieb der Komponente Web-Kontrolle:
  Komponentenversion, Kategorisierungsgrund, zusätzliche Informationen zum Kategorisierungsgrund, kategorisierte URL, Host-IP-Adresse des blockierten/kategorisierten Objekts.

Hinweis: Abhängig von den Einstellungen von Kaspersky Security Center können Sie anstatt Kaspersky Security Network an Kaspersky Private Security Network teilnehmen. Kaspersky Endpoint Security benachrichtigt Sie, wenn von Kaspersky Private Security Network zu Kaspersky Security Network gewechselt wird, und fordert Sie auf, die Bedingungen der Erklärung zu Kaspersky Security Network zu akzeptieren. Ausführliche Informationen zur Teilnahme an Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center.

Infrastruktur von Kaspersky Security Network

Kaspersky Endpoint Security unterstützt folgende Infrastrukturlösungen für Kaspersky Security Network:

- *Global KSN* ist die von den meisten Kaspersky-Anwendungen verwendete Lösung. KSN-Teilnehmer erhalten von Kaspersky Security Network Informationen und senden Informationen zu auf dem Benutzercomputer erkannten Objekten an Kaspersky, wo diese zusätzlich von Kaspersky-Analytikern untersucht und in die Reputations- und Statistikdatenbanken von Kaspersky Security Network übernommen werden.

- *Private KSN* ist eine Lösung, die Benutzern von Hostcomputern für Kaspersky Endpoint Security oder anderen Kaspersky-Anwendungen gestattet, auf die Reputationsdatenbanken von Kaspersky Security Network sowie weitere Statistiken zuzugreifen, ohne Daten von ihren eigenen Computern an Kaspersky Security Network zu senden. Private KSN ist für Unternehmenskunden vorgesehen, denen die Teilnahme an Kaspersky Security Network aus beliebigen der folgenden Gründe nicht möglich ist:

  - Die lokalen Workstations sind nicht mit dem Internet verbunden.

- Die Übertragung von Daten aus dem Land ihres Standorts oder aus dem Unternehmens-LAN ist rechtlich oder durch Unternehmenssicherheitsrichtlinien untersagt.

Standardmäßig verwendet Kaspersky Security Center Global KSN. Sie können die Verwendung von Private KSN in der Kaspersky Security Center-Verwaltungskonsole (MMC) und der Kaspersky Security Center Web Console konfigurieren. Es ist nicht möglich, über die Kaspersky Security Center Cloud Console die Verwendung von Private KSN zu konfigurieren.

KSN-Proxy

Computer, die über den Administrationsserver von Kaspersky Security Center verwaltet werden, können über den KSN-Proxydienst mit Kaspersky Security Network interagieren.

Der KSN-Proxydienst bietet folgende Möglichkeiten:

- Der Computer des Benutzers kann auch ohne direkten Internetzugang eine Anfrage bei KSN einreichen und Informationen an KSN weiterleiten.
- Der KSN-Proxydienst erfasst verarbeitete Daten im Cache, was die Belastung des Netzwerkkanals zur externen Kommunikation reduziert und vom Benutzercomputer angeforderte Informationen schneller an diesen übermittelt.

Details zum KSN-Proxy-Dienst finden Sie in der Hilfe zu Kaspersky Security Center.

Hinweis: Die Update-Funktion (einschließlich der Bereitstellung von Anti-Malware-Signatur-Updates und Codebase-Updates) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Integrität der Anwendungskomponenten überprüfen

Kaspersky Endpoint Security enthält verschiedene Binärmodule in Form von dynamisch verknüpften Bibliotheken, ausführbaren Dateien, Konfigurationsdateien und Schnittstellendateien. Angreifer können ein oder mehrere ausführbare Module oder Dateien der Anwendung durch andere Dateien ersetzen, die bösartigen Code enthalten. Um dies zu verhindern, kann Kaspersky Endpoint Security die Integrität der Anwendungskomponenten überprüfen. Die Anwendung überprüft Module und Dateien auf nicht autorisierte Änderungen oder Beschädigungen. Wenn ein Modul oder Datei der Anwendung eine falsche Prüfsumme aufweist, wird sie als beschädigt betrachtet.

Die Integrität der Anwendungskomponenten wird mithilfe der Utility integrity_checker überprüft, die sich im Verzeichnis /Library/Application Support/Kaspersky Lab/KAV/Binaries befindet. Dieses Dienstprogramm überprüft die Integrität der Manifest-Datei, die eine Liste der Anwendungsdateien enthält, deren Integrität für den ordnungsgemäßen Betrieb der Anwendungskomponente entscheidend ist.

Die Manifest-Datei „integrity_check.xml“ ist durch eine kryptografische Signatur von Kaspersky geschützt und befindet sich im selben Verzeichnis wie das Dienstprogramm integrity_checker (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Hinweis: Für die Ausführung des Tools „integrity_checker“ sind Berechtigungen des Root-Benutzerkontos erforderlich.

Die Integritätsprüfung kann mithilfe des Dienstprogramms, das zusammen mit der Anwendung installiert wird, oder mithilfe des Dienstprogramms auf einer zertifizierten CD ausgeführt werden.

Führen Sie den folgenden Befehl aus, um die Integrität der Anwendungskomponenten zu überprüfen:

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

Standardmäßig verwendet das Tool die Datei „integrity_check.xml“, die sich im Verzeichnis /Library/Application Support/Kaspersky Lab/KAV/Binaries befindet.

Um die Hilfe für die Einstellungen des Tools anzuzeigen, führen Sie den folgenden Befehl aus:

```
--help
```

Die Überprüfungsergebnisse werden neben dem Namen der jeweiligen Manifest-Datei im folgenden Format angezeigt:

- `SUCCEEDED` — Die Integrität der Dateien wurde bestätigt (Rückgabecode `0`)
- `FAILED` — Die Integrität der Dateien wurde nicht bestätigt (Rückgabecode ist nicht `0`)

Anwendung über die Kaspersky Security Center Verwaltungskonsole verwalten

Kaspersky Security Center dient der zentralisierten Verwaltung des Schutzsystems eines Unternehmensnetzwerks. Ausführliche Informationen zu Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Sie können Kaspersky Endpoint Security auch über die grafische Benutzeroberfläche der Anwendung, Kaspersky Security Center Web Console und Cloud Console und über die Befehlszeile verwalten.

Kaspersky Endpoint Security im Unternehmensnetzwerk verteilen

1. Verteilen Sie den *Administrationsserver* im Netzwerk.

   Der Administrationsserver ist eine Komponente von Kaspersky Security Center, mit der Informationen über alle im Unternehmensnetzwerk installierten Kaspersky-Anwendungen zentral gespeichert und verwaltet werden.

2. Installieren Sie die *Verwaltungskonsole* am Arbeitsplatz des Administrators für Kaspersky Security Center.

   Die Verwaltungskonsole ist eine Komponente von Kaspersky Security Center, die eine Benutzeroberfläche für die Verwaltungsdienste des Administrationsservers und des *Administrationsagenten* bietet. Der Administrationsagent koordiniert die Interaktion zwischen Administrationsserver und Kaspersky Endpoint Security, die auf Computern innerhalb desselben Unternehmensnetzwerks installiert sind.

3. Installieren Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security am Arbeitsplatz des Administrators für Kaspersky Security Center.

   Das *Verwaltungs-Plug-in* ist eine spezielle Komponente, die eine Schnittstelle bietet, um Kaspersky-Anwendungen über die Verwaltungskonsole zu verwalten. Für jede Anwendung ist ein spezielles Verwaltungs-Plug-in verfügbar. Das Verwaltungs-Plug-in gehört zum Lieferumfang der Kaspersky-Anwendungen, die mit Kaspersky Security Center verwaltet werden können.

4. Verwenden Sie eine der folgenden Methoden, um den Administrationsagenten auf entfernten Mac-Computern zu installieren:

   - Lokal
   - „Apple Remote Desktop“ per Fernzugriff verwenden
   - Per Fernzugriff über Kaspersky Security Center
   - Per Fernzugriff über das SSH-Protokoll

   Hinweis: Um Kaspersky Endpoint Security for Mac 12.2 über Kaspersky Security Center zu verwalten, müssen Sie auf Remote-Computern den Administrationsagenten Version 15 installieren.

5. Verwenden Sie eine der folgenden Methoden, um Kaspersky Endpoint Security auf entfernten Mac-Computern zu installieren:

   - Lokal
   - „Apple Remote Desktop“ per Fernzugriff verwenden
   - Per Fernzugriff über das SSH-Protokoll
   - Per Fernzugriff über Kaspersky Security Center

   Wichtig: Falls Kaspersky Internet Security for Mac oder Anti-Malware-Software von Drittherstellern auf den Remote-Computern installiert ist, müssen Sie diese vor der Installation von Kaspersky Endpoint Security deinstallieren.

Details zur Bereitstellung des Administrationsservers und zur Installation der Verwaltungskonsole finden Sie in der Hilfe zu Kaspersky Security Center.

Kaspersky Endpoint Security Version 11.1 oder höher auf Version 12.2 aktualisieren

Hinweis: Um Kaspersky Endpoint Security for Mac 12.2 über Kaspersky Security Center zu verwalten, müssen Sie auf Remote-Computern den Administrationsagenten Version 15 installieren.

Wenn Kaspersky Endpoint Security über Kaspersky Security Center verwaltet wird, gibt es folgende Möglichkeiten zum Upgrade von Version 11.1 oder höher auf Version 12.2:

- Simultanes Update auf den Remote-Computern: Kaspersky Endpoint Security wird auf Version 12.2 aktualisiert und der Administrationsagent auf Version 15.
- Zuerst wird der Administrationsagent auf Version 15 aktualisiert und anschließend Kaspersky Endpoint Security auf Version 12.2.

Wenn Sie die Anwendung auf eine neuere Version aktualisieren, beachten Sie Folgendes:

- Um Kaspersky Endpoint Security auf Version 12.2 upzugraden, ist macOS 12 oder höher erforderlich.
- Sie müssen das Archiv KES_11.3_profile.zip von der Website des Technischen Supports herunterladen, um das neue Konfigurationsprofil zu übernehmen.

- Nach dem Upgrade von Kaspersky Endpoint Security auf Version 12.2 werden in den Netzwerkeinstellungen möglicherweise zwei Einträge für „Kaspersky Filter“ und „Kaspersky Monitor“ angezeigt.
- Wenn Sie Kaspersky Endpoint Security Version 11.0.1 oder älter verwenden, müssen Sie die App deinstallieren und macOS auf Version 12 oder höher aktualisieren, um die App auf Version 12.2 zu aktualisieren. Anschließend können Sie Kaspersky Endpoint Security Version 12.2 installieren.

Hinweis: Die Update-Funktion (einschließlich der Bereitstellung von Anti-Malware-Signatur-Updates und Codebase-Updates) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Installation von Kaspersky Endpoint Security per Fernzugriff vorbereiten

Dieser Abschnitt enthält Angaben zur Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security am Arbeitsplatz des Kaspersky Endpoint Security-Administrators und zur Installation des Administrationsagenten auf dem Remote-Computer.

Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security und des Administrationsagenten ist eine Voraussetzung für die Installation von Kaspersky Endpoint Security über Kaspersky Security Center.

Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security bietet eine Oberfläche, mit der sich Kaspersky Endpoint Security über die Verwaltungskonsole verwalten lässt.

Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren

1. Entpacken Sie am Arbeitsplatz des Kaspersky Security Center-Administrators das Archiv mit den Dateien des Installationspakets für Kaspersky Endpoint Security.
2. Öffnen Sie den Ordner mit den Dateien des Installationspakets für Kaspersky Endpoint Security.
3. Doppelklicken Sie auf klcfginst.exe.

   Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security startet.

Wichtig: Bevor das Verwaltungs-Plug-in für Kaspersky Endpoint Security installiert wird, muss die Verwaltungskonsole am Arbeitsplatz des Administrators für Kaspersky Security Center geschlossen werden.

Administrationsagenten lokal installieren

Der Administrationsagent koordiniert die Interaktion zwischen Administrationsserver und Kaspersky Endpoint Security, die auf Computern innerhalb desselben Unternehmensnetzwerks installiert sind.

Administrationsagenten lokal installieren

1. Öffnen Sie auf dem Remote-Computer den Ordner mit dem Lieferumfang des Administrationsagenten.
2. Öffnen Sie das Installationspaket für den Administrationsagenten (dmg-Datei).

   Ein Fenster mit dem Inhalt des Installationspakets wird geöffnet.
3. Doppelklicken Sie im Fenster mit dem Installationspaket auf **Kaspersky Administrationsagent**.
4. Bestätigen Sie, dass Sie den Administrationsagenten installieren möchten, indem Sie auf **Fortfahren** klicken.
5. Klicken Sie im Fenster **Einführung** auf **Fortfahren**.
6. Im Fenster **Lizenz** können Sie den Endbenutzer-Lizenzvertrag für den Administrationsagenten lesen, der zwischen Ihnen und der AO Kaspersky Lab abgeschlossen wird. Gehen Sie anschließend folgendermaßen vor:

   - Um alle Bedingungen des Vertrags zu akzeptieren und mit der Installation fortzufahren, klicken Sie auf **Fortfahren**.
   - Um den Vertragstext auszudrucken, klicken Sie auf **Drucken**.
   - Um den Vertragstext in einer Textdatei zu speichern, klicken Sie auf **Speichern**.
7. Führen Sie im Bestätigungsfenster eine der folgenden Aktionen aus:

   - Um mit der Installation des Administrationsagenten fortzufahren, klicken Sie auf **Akzeptieren**.
   - Um ins Fenster mit dem Text des Lizenzvertrags zurückzukehren, klicken Sie auf **Lizenz lesen**.
   - Um die Installation abzubrechen, klicken Sie auf **Ablehnen**.
8. Gehen Sie im Fenster **Einstellungen** wie folgt vor:

   a. Geben Sie im Feld **Server** die IP-Adresse oder den DNS-Namen des Servers an, auf dem Kaspersky Security Center installiert ist.

   b. Geben Sie im Feld **Port** die Portnummer für eine unverschlüsselte Verbindung zum Server an.

   c. Geben Sie im Feld **SSL-Port** die Portnummer für eine SSL-Verbindung zum Server an.

   d. Damit der Administrationsagent sofort nach der Installation gestartet wird, aktivieren Sie das Kontrollkästchen **Nach der Installation ausführen**.

   Wenn Sie für die Verbindung zum Server kein SSL verwenden möchten, deaktivieren das Kontrollkästchen **SSL verwenden**. Klicken Sie auf **Fortfahren**, um die Installation fortzusetzen.

9. Im Fenster **Installationstyp** finden Sie Informationen über den Datenträger, auf dem der Administrationsagent installiert werden soll.

   Um den Administrationsagenten mit den Standardeinstellungen zu installieren, klicken Sie auf **Installieren** und geben Sie zur Bestätigung das Administratorkennwort ein.

   Warten Sie, bis der Installer des Administrationsagenten die Installation der Anwendungskomponenten abgeschlossen hat.

10. Klicken Sie auf **Schließen**, um den Installer zu schließen.

Installieren des Administrationsagenten mithilfe von „Apple Remote Desktop“

1. Wählen Sie auf einem Remote-Computer **Apple-Menü** > **Systemeinstellungen** > **Allgemein** > **Freigaben**.
2. Aktivieren Sie das Kontrollkästchen **Entfernte Verwaltung**.
3. Installieren Sie „Apple Remote Desktop“ auf einem anderen Mac, den Sie als Server verwenden möchten. Weitere Informationen über „Apple Remote Desktop“ finden Sie bei Apple Support.
4. Öffnen Sie „Apple Remote Desktop“.
5. Klicken Sie im Fenster **Remote Desktop** links auf **Scanner** und wählen Sie die Geräte aus, auf denen Sie den Administrationsagenten installieren möchten.
6. Klicken Sie auf **Kopieren**.
7. Klicken Sie auf + und wählen Sie die folgenden Installationsdateien für den Administrationsagenten aus: dmg-Datei, kud-Datei und sh-Datei.
8. Wählen Sie im Pop-up-Menü **Objekte ablegen in** den Punkt **oberster Ordner des Volumes** aus.
9. Klicken Sie auf **Kopieren**.
10. Nachdem die Dateien erfolgreich kopiert wurden, klicken Sie auf **Unix**.
11. Geben Sie den folgenden Befehl ein:

    ```
    cd /;
    ./install.sh --accept_eula -r <Adresse des Administrationsservers>
    ```

    dabei steht `<Adresse des Administrationsservers>` für den DNS-Namen oder die IP-Adresse des Administrationsservers von Kaspersky Security Center.

    Hinweis: Wenn Sie diesen Befehl eingeben, akzeptieren Sie den Endbenutzer-Lizenzvertrag.

12. Wählen Sie **User** aus, um den Befehl auszuführen, und geben Sie „root“ in das Feld ein.
13. Klicken Sie auf **Senden**.

Auf den ausgewählten Geräten beginnt die Installation des Administrationsagenten.

Installation des Administrationsagenten unter Verwendung von Kaspersky Security Center

Kaspersky Security Center installiert den Administrationsagenten auf einem Client-Computer mithilfe einer SSH-Verbindung.

Bevor Sie den Administrationsagenten auf einem Client-Computer installieren, vergewissern Sie sich, ob folgende Bedingungen erfüllt sind:

- Der Administrationsserver für Kaspersky Security Center wurde im Unternehmensnetzwerk verteilt.
- Die Verwaltungskonsole wurde am Arbeitsplatz des Administrator für Kaspersky Security Center installiert.
- Auf den Remote-Computern ist Anmeldung per Fernzugriff aktiviert.
- Auf einem Remote-Computer ist ein spezielles Administratorkonto vorhanden, das für die Installation per Fernzugriff verwendet wird. Für die Installation können Sie ein Domänenkonto verwenden.
- Für das spezielle Konto ist das sudo-Kennwort deaktiviert.

Ein Installationspaket für den Administrationsagenten erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie in der Baumstruktur den Ordner **Erweitert**, danach den Unterordner **Remote-Installation** und dann den Unterordner **Installationspakete** aus.
4. Klicken Sie im Arbeitsbereich auf **Installationspaket erstellen**.
5. Klicken Sie im Fenster **Typ des Installationspakets auswählen** auf **Installationspaket für eine Kaspersky-Anwendung erstellen**.
6. Geben Sie im Fenster **Name des Installationspakets festlegen** im Feld **Name** einen Namen für das neue Installationspaket ein und klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster **Programmpaket für die Installation auswählen** auf **Durchsuchen**.

   Im folgenden Fenster können Sie eine Datei zum Erstellen des Installationspakets auswählen.
8. Öffnen Sie den Ordner mit dem Installationspaket für den Administrationsagenten und wählen Sie die Datei klnagent.kud aus.

   Im Fenster **Programmpaket für die Installation auswählen** werden Name und Version der Anwendung genannt, die mit der hinzugefügten Datei per Fernzugriff installiert werden kann.
9. Klicken Sie auf **Weiter**.

   Ein Installationspaket für Kaspersky Endpoint Security wird mit den angegebenen Einstellungen erstellt.
10. Klicken Sie im letzten Fenster des Assistenten auf **Fertig**, um den Assistenten für neue Pakete zu beenden.

Aufgabe für die Remote-Installation des Administrationsagenten auf einem Client-Computer erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie den Ordner **Aufgaben** aus.
4. Um den Assistenten für neue Aufgaben zu starten, klicken Sie im Arbeitsbereich auf **Neue Aufgabe**.
5. Folgen Sie den nachfolgenden Anweisungen des Assistenten für neue Aufgaben, um eine Aufgabe für die Remote-Installation von Kaspersky Endpoint Security auf einem Client-Computer zu erstellen.

Um zum nächsten Schritt des Assistenten zu gehen, klicken Sie auf **Weiter**. Um zum vorherigen Schritt des Assistenten zurückzukehren, klicken Sie auf ←. Um den Assistenten bei einem beliebigen Schritt abzubrechen, klicken Sie auf **Abbrechen**.

Hinweis: Das Aussehen der Schaltflächen kann je nach Windows-Version unterschiedlich sein.

Schritt 1. Aufgabentyp auswählen

1. Maximieren Sie im Fenster **Aufgabentyp auswählen** den Knoten **Kaspersky Security Center Administrationsserver**.
2. Wählen Sie die Aufgabe **Remote-Installation eines Programms** aus.

Schritt 2. Installationspaket auswählen

Führen Sie im Fenster **Installationspaket auswählen** eine der folgenden Aktionen aus:

- Falls bereits ein Installationspaket für den Administrationsagenten mit den erforderlichen Einstellungen erstellt wurde, wählen Sie das Paket oben im Fenster **Installationspaket auswählen** in der Liste der Installationspakete aus.
- Wenn das erforderliche Installationspaket noch nicht erstellt wurde, klicken Sie auf **Neu**, um den Assistenten für neue Pakete zu starten.

Schritt 3. Installationseinstellungen anpassen

Gehen Sie im Fenster **Einstellungen** wie folgt vor:

1. Aktivieren Sie das Kontrollkästchen **Durch Ressourcen des Betriebssystems über den Administrationsserver**.
2. Deaktivieren Sie alle anderen Kontrollkästchen.

Schritt 4. Administrationsgruppe auswählen, der nach der Installation Computer hinzugefügt werden sollen

Wählen Sie im Fenster **In die Liste mit verwalteten Geräten verschieben** eine Gruppe aus, in welche Computer falls nötig nach der Installation verschoben werden.

Schritt 5. Festlegen einer Methode zur Auswahl der Client-Computer, für die diese Aufgabe erstellt wird

Wählen Sie im Fenster **Geräte auswählen, denen die Aufgabe zugewiesen wird** das Verfahren aus, mit dem Client-Computer festgelegt werden sollen:

- Um die Client-Computer aus den Computern auszuwählen, die vom Administrationsserver im Netzwerk gefunden wurden, wählen Sie die Option **Geräte auswählen, die vom Administrationsserver erkannt wurden** aus.
- Um die IP-Adressen der Computer manuell anzugeben oder die IP-Adressen der Computer aus einer Datei zu importieren, wählen Sie die Variante **Geräteadressen manuell festlegen oder Adressen aus Liste importieren** aus.
- Um eine Aufgabe zu erstellen, mit der Geräte nach einem vordefinierten Kriterium ausgewählt werden, wählen Sie die Variante **Aufgabe einer Geräteauswahl zuordnen** aus.
- Um Computer aus einer bestimmten Administrationsgruppe auszuwählen, wählen Sie die Variante **Aufgabe einer Administrationsgruppe zuweisen** aus.

Schritt 6. Client-Computer auswählen

Im folgenden Fenster (**Geräte auswählen**, **Geräteauswahl** oder **Administrationsgruppe auswählen**, je nachdem, welche Variante Sie im vorherigen Schritt ausgewählt haben) können Sie die Client-Computer auswählen, die IP-Adressen der Computer angeben, die Computerauswahl angeben oder die Administrationsgruppe auswählen, auf die die Aufgabe angewendet werden soll.

Schritt 7. Benutzerkonto für den Aufgabenstart auswählen

1. Aktivieren Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** das Kontrollkästchen **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**.
2. Klicken Sie auf **Hinzufügen** > **Benutzerkonto**.

   Das Fenster **Konto** wird geöffnet.
3. Geben Sie den Benutzernamen und das Kennwort des dedizierten Administratorkontos eines Remote-Computers ein.
4. Klicken Sie auf **OK**.

Schritt 8. Startzeitplan für die Aufgabe anpassen

1. Wählen Sie im Fenster **Aufgabenzeitplan anpassen** in der Dropdown-Liste **Start nach Zeitplan** einen Startmodus aus.
2. Konfigurieren Sie erforderlichenfalls den automatischen Start einer geplanten Aufgabe (indem Sie Datum und Uhrzeit des Aufgabenstarts festlegen).
3. Damit Aufgaben gestartet werden, die von der Anwendung nicht nach Zeitplan ausgeführt werden konnten (weil der Computer zum betreffenden Zeitpunkt beispielsweise ausgeschaltet war), aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

   Kaspersky Endpoint Security startet die Aufgabe, sobald der Aufgabenstart möglich ist.

Schritt 9. Aufgabenname festlegen

Geben Sie im Fenster **Aufgabenname festlegen** im Feld **Name** den Namen der zu erstellenden Aufgabe ein.

Schritt 10. Erstellen der Aufgabe abschließen

Gehen Sie im Fenster **Erstellung der Aufgabe abschließen** wie folgt vor:

1. Damit die Aufgabe gestartet wird, sobald der Assistent abgeschlossen wird, aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**.
2. Klicken Sie auf **Fertigstellen**, um den Assistenten abzuschließen.

Administrationsagenten mit dem SSH-Protokoll installieren

Die Verwendung des SSH-Protokolls ist eine der Methoden, um den Administrationsagenten auf einem Remote-Computer zu installieren.

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt werden:

- Der Administrationsserver für Kaspersky Security Center wurde im Unternehmensnetzwerk verteilt.
- Die Verwaltungskonsole wurde am Arbeitsplatz des Administrator für Kaspersky Security Center installiert.
- Es wurde ein Installationspaket für den Administrationsagenten erstellt und in einem gemeinsam genutzten Ordner des Administrationsservers abgelegt.
- Auf dem Remote-Computer wird Anmeldung per Fernzugriff aktiviert.
- Die für die Installation des Administrationsagenten verwendeten Anmeldedaten sind in sudoers-Dateien enthalten.

Ausführliche Informationen über Installationspakete finden Sie in der Hilfe zu Kaspersky Security Center.

Administrationsagenten mit dem SSH-Protokoll installieren

1. Starten Sie am Administrator-Arbeitsplatz den SSH-Client.
2. Stellen Sie eine Verbindung mit dem entfernten Remote-Computer her.
3. Verbinden Sie den gemeinsam genutzten Ordner des Administrationsservers als Netzlaufwerk mit dem Remote-Computer. Geben Sie dazu im SSH-Client den folgenden Befehl ein:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<Administratorkonto>:<Kennwort>@<IP-Adresse des
   Administrationsservers>/KLSHARE /Volumes/KLSHARE
   ```

   Beschreibungen der Parameter:

   - `<Administratorkonto>` – Name des Administratorkontos auf dem Administrationsserver.
   - `<Kennwort>` – Kennwort des Administratorkontos auf dem Administrationsserver.
   - `<IP-Adresse des Administrationsservers>` – IP-Adresse des Host-Servers für Kaspersky Security Center.
4. Starten Sie das Installationsskript. Geben Sie dazu im SSH-Client den folgenden Befehl ein:

   ```
   cd /Volumes/KLSHARE/<klnagent_package_folder>
   ```

   wobei `<klnagent_package_folder>` der Ordner ist, in dem sich das Installationspaket für den Administrationsagenten befindet.

```
sudo ./install.sh --accept_eula [-r <Server>] [-p <Portnummer>] [-s use_ssl 0|1] [-
l <SSL-Portnummer>] [-x use_proxy 0|1] [-a <Proxy>] [-n <Proxy-Benutzername>] [-w
<Proxy-Kennwort>]
```

Beschreibungen der Parameter:

- `<Server>` – IP-Adresse oder DNS-Name des Servers, auf dem Kaspersky Security Center installiert ist.
- `<Portnummer>` – Nummer des Ports, über den die nicht gesicherte Verbindung mit dem Administrationsserver erfolgt. Standardmäßig wird Port 14000 verwendet.
- `use_ssl 0|1` – Dieser Parameter legt fest, ob die Verbindung zwischen dem Administrationsagenten und dem Administrationsserver verschlüsselt wird. Der Wert „0“ steht für eine unverschlüsselte Verbindung. Der Wert „1“ steht für eine Verbindung über das SSL-Protokoll (Standardwert).
- `<SSL-Portnummer>` – Nummer des Ports, über den die nicht gesicherte Verbindung mithilfe des SSL-Protokolls mit dem Administrationsserver erfolgt. Standardmäßig wird Port 13000 verwendet.
- `use_proxy 0|1` – Dieser Parameter legt fest, ob ein Proxy-Server für die Verbindung zum Internet verwendet wird. Der Wert „0“ bedeutet, dass kein Proxy-Server verwendet wird. Der Wert „1“ steht für eine Verbindung über Proxy-Server (Standardwert).
- `<Proxy>` – IP-Adresse oder DNS-Name des Proxy-Servers.
- `<Proxy-Benutzername>` – Benutzerkonto für die Verbindung mit dem Proxy-Server.
- `<Proxy-Kennwort>` – Kennwort für die Verbindung mit dem Proxy-Server.

Wichtig: Für diesen Befehl sind Administratorrechte erforderlich.

5. Trennen Sie das Netzlaufwerk auf dem Remote-Computer. Geben Sie dazu im SSH-Client den folgenden Befehl ein:
   ```
   umount /Volumes/KLSHARE
   ```
6. Testen Sie, ob der Administrationsagent auf dem Remote-Computer einwandfrei funktioniert. Geben Sie dazu im SSH-Client den folgenden Befehl ein:
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```
   Wenn der Test erfolgreich war, funktioniert der Administrationsagent wie vorgesehen.

Administrationsagenten lokal deinstallieren

1. Öffnen Sie auf dem Remote-Computer den Ordner mit dem Lieferumfang des Administrationsagenten.
2. Öffnen Sie das Installationspaket für den Administrationsagenten (dmg-Datei).
   Ein Fenster mit dem Inhalt des Installationspakets wird geöffnet.
3. Doppelklicken Sie im Fenster mit dem Installationspaket auf **Uninstaller für den Administrationsagenten**.
4. Klicken Sie im Fenster **Einführung** auf **Fortfahren**.
5. Klicken Sie im Fenster **Informationen** auf **Entfernen**.

6. Die Administrator-Anmeldedaten werden abgefragt. Geben Sie den Benutzernamen und das Kennwort des Administrators ein und bestätigen Sie, dass Sie den Administrationsagenten deinstallieren möchten.

   Die Deinstallieren des Administrationsagenten beginnt.

7. Lesen Sie die Informationen über die Deinstallation und klicken Sie auf **Fertig**, um den Uninstaller zu beenden.

Der Administrationsagent wurde von dem Remote-Computer entfernt.

Administrationsagent über die Befehlszeile verwalten

Dieser Abschnitt enthält Informationen darüber, wie der Administrationsagent über die Befehlszeile auf dem Client-Computer gesteuert werden kann.

Sie können den Administrationsagenten beenden und mithilfe der Befehlszeile auf einem Client-Computer neu starten.

Außerdem können Sie mithilfe des Tools klmover den Remote-Computer manuell mit dem Administrationsserver verbinden und mithilfe des Tools klnagchk die Verbindung des Remote-Computers mit dem Administrationsserver testen.

Sie können den Administrationsagenten deinstallieren.

Administrationsagent auf einem Remote-Computer starten/beenden

Sie können mithilfe der Befehlszeile den Administrationsagenten auf einem Client-Computer beenden und neu starten.

Administrationsagent beenden

Geben Sie auf dem Remote-Computer in der Befehlszeile den Befehl unload ein, um das Tool launchctl zu starten.

Syntax des Befehls:

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Administrationsagent starten

Geben Sie auf dem Remote-Computer in der Befehlszeile den Befehl load ein, um das Tool launchctl zu starten.

Syntax des Befehls:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Wichtig: Es sind Administratorrechte erforderlich, um den Administrationsagenten zu beenden und zu starten.

Testen Sie die Verbindung zwischen Client-Computer und Administrationsserver manuell. Tool Klnagchk

Testen Sie die Verbindung eines Remote-Computers zum Administrationsserver.

Führen Sie auf dem Remote-Computer über die Befehlszeile das Tool klnagchk aus.

Das Tool klnagchk ist im Lieferumfang für den Administrationsagenten enthalten.

Das Tool klnagchk befindet sich nach der Installation des Administrationsagenten im Ordner /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Abhängig von den Parametern, die Sie angeben, führt das Tool klnagchk beim Ausführen über die Befehlszeile die folgenden Aktionen aus:

- Es zeigt die Einstellungen an, die für die auf dem Remote-Computer hergestellte Verbindung zwischen dem Administrationsagenten und dem Administrationsserver angegeben wurden, oder es speichert sie in einer Datei.
- Es speichert die Statistik zum Administrationsagenten (seit dem letzten Start des Administrationsagenten) und die Ergebnisse der des Tools in einer Datei, oder zeigt diese Informationen auf dem Bildschirm an.
- Es versucht, eine Verbindung zwischen dem Administrationsagenten und dem Administrationsserver herzustellen.
- Wenn das Tool keine Verbindung herstellen kann, sendet es ein ICMP-Paket, um den Status des Computers zu überprüfen, auf dem der Administrationsserver installiert ist.

Navigieren Sie vor dem Aufruf des Tools in der Befehlszeile zu /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntax des Befehls:

```
sudo ./klnagchk [-logfile <Dateiname>] [-sp] [-savecert <Pfad der Zertifikatsdatei>] [-restart]
```

Wichtig: Zum Ausführen des Tools sind Administratorrechte erforderlich.

Beschreibungen der Parameter

`-logfile <Dateiname>` – Speichert die Einstellungen für die Verbindung zwischen dem Administrationsagenten und dem Administrationsserver sowie die Ergebnisse der Dienstprogrammausführung in einer Datei. Wenn dieser Parameter nicht angegeben ist, werden die Einstellungen der Serververbindung, die Ausführungsergebnisse und die Fehlermeldungen auf dem Bildschirm angezeigt.

`-sp` – Zeigt das Kennwort für die Proxyserver-Authentifizierung auf dem Bildschirm an oder speichert es in einer Datei. Dieser Parameter wird verwendet, wenn der Administrationsagent über einen Proxyserver eine Verbindung zum Administrationsserver herstellt. Dieser Parameter wird standardmäßig nicht verwendet.

`-savecert <Dateiname>` – Speichert das Zertifikat zur Authentifizierung auf dem Administrationsserver in der festgelegten Datei.

`-restart` – Administrationsagent neu starten, nachdem das Dienstprogramm abgeschlossen wurde.

Beispiel:
sudo ./klnagchk -logfile klnagchk.log -sp

Einen Remote-Computer manuell mit dem Administrationsserver verbinden. Tool Klmover

Einen Remote-Computer mit dem Administrationsserver verbinden

Führen Sie auf dem Remote-Computer über die Befehlszeile das Tool klmover aus.

Das Tool klmover ist im Installationspaket für den Administrationsagenten enthalten.

Das Tool klmover befindet sich nach der Installation des Administrationsagenten im Ordner /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Abhängig von den Parametern, die Sie angeben, führt das Tool klmover beim Ausführen über die Befehlszeile die folgenden Aktionen aus:

- Es verbindet den Administrationsagenten nach den festgelegten Parametern mit dem Administrationsserver.
- Es speichert die Ergebnisse der Ausführung eines Tools in einer Datei oder zeigt sie auf dem Bildschirm an.

Navigieren Sie vor dem Aufruf des Tools in der Befehlszeile zu /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntax der Befehlszeile:

```
sudo ./klmover [-logfile <Dateiname>] [-address <Serveradresse>] [-pn <Portnummer>] [-
ps <SSL-Portnummer>] [-nossl] [-cert <Pfad der Zertifikatsdatei>] [-silent] [-dupfix]
```

Wichtig: Für den Start des Tools sind Administratorrechte erforderlich.

Beschreibungen der Parameter

`-logfile <Dateiname>` – Speichert die Ausführungsergebnisse in einer Datei. Wenn dieser Parameter nicht angegeben wurde, werden die Ergebnisse der Ausführung und Fehlermeldungen auf dem Bildschirm angezeigt.

`-address <Serveradresse>` – Adresse, die der Administrationsagent verwendet, um eine Verbindung zum Administrationsserver herzustellen. Sie können entweder die IP-Adresse oder den DNS-Namen des Servers angeben.

Hinweis: Sie können den Befehl auch mit diesem Parameter verwenden, um die Adresse des Administrationsservers zu ändern, mit dem Remote-Computer verbunden sind.

`-pn <Portnummer>` – Nummer des Ports, über den die nicht gesicherte Verbindung mit dem Administrationsserver erfolgt. Standardmäßig wird Port 14000 verwendet.

`-ps <SSL-Portnummer>` – Nummer des Ports, über den die nicht gesicherte Verbindung mithilfe des SSL-Protokolls mit dem Administrationsserver erfolgt. Standardmäßig wird Port 13000 verwendet.

`-nossl` – Eine unverschlüsselte Verbindung mit dem Administrationsserver wird verwendet. Wenn dieser Parameter nicht angegeben ist, stellt der Administrationsagent über das verschlüsselte SSL-Protokoll eine sichere Verbindung zum Administrationsserver her.

`-cert <Pfad der Zertifikatsdatei>` – Angegebene Zertifikatsdatei für die Authentifizierung auf einem neuen Administrationsserver verwenden. Wenn dieser Parameter nicht angegeben ist, erhält der Administrationsagent bei der ersten Verbindung mit dem Administrationsserver ein Zertifikat.

`-silent` – Dienstprogramm im Silent-Modus starten

`-dupfix` – Dieser Parameter wird verwendet, wenn der Administrationsagent auf eine andere Weise installiert wurde als in dieser Hilfe beschrieben. Beispiel: Wenn der Administrationsagent von einem Datenträgerabbild wiederhergestellt wurde, während der Administrationsagent installiert war. Falls die automatische Selbstidentifizierung des Administrationsagenten dazu führt, dass die Symbole des ursprünglichen Computers und anderer Computer in der Verwaltungskonsole dupliziert werden, versuchen Sie, die duplizierten Computer erneut zu verbinden.

Hinweis: Wenn das Tool klmover ausgeführt wird, wird empfohlen, Werte für alle Parameter anzugeben.

Beispiel:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

Ein Remote-Computer, der über den Administrationsagenten mit dem Administrationsserver verbunden ist, wird als *Client-Computer* bezeichnet.

Deinstallieren des Administrationsagenten

Syntax des Befehls:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Kaspersky Endpoint Security installieren und deinstallieren

Dieser Abschnitt beschreibt, wie Kaspersky Endpoint Security auf einem Client-Computer per Fernzugriff installiert und deinstalliert wird.

Die Installation oder Deinstallation von Kaspersky Endpoint Security ist auch lokal oder über Kaspersky Security Center Web Console oder Kaspersky Security Center Cloud Console möglich.

Installation der Anwendung über das SSH-Protokoll

Bevor Sie Kaspersky Endpoint Security auf einem Remote-Computer installieren, vergewissern Sie sich, ob folgende Bedingungen erfüllt sind:

- Der Administrationsserver für Kaspersky Security Center wurde im Unternehmensnetzwerk verteilt.
- Die Verwaltungskonsole wurde am Arbeitsplatz des Administrator für Kaspersky Security Center installiert.
- Es wurde ein Installationspaket für Kaspersky Endpoint Security erstellt und in einem gemeinsam genutzten Ordner auf dem Administrationsserver abgelegt.
- Eine Schlüsseldatei für Kaspersky Endpoint Security wurde im gemeinsam genutzten Ordner auf dem Administrationsserver abgelegt (optional).
- Auf dem Remote-Computer wird Anmeldung per Fernzugriff aktiviert.
- Die für die Installation der Anwendung verwendeten Anmeldedaten sind in sudoers-Dateien enthalten.

Installieren von Kaspersky Endpoint Security mit dem SSH-Protokoll auf einem Client-Computer:

1. Starten Sie am Arbeitsplatz des Kaspersky Security Center-Administrators den SSH-Client.
2. Stellen Sie eine Verbindung mit dem entfernten Remote-Computer her.
3. Verbinden Sie den gemeinsam genutzten Ordner des Administrationsservers als Netzlaufwerk mit dem Remote-Computer. Geben Sie dazu im SSH-Client den folgenden Befehl ein:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<Administratorkonto>:<Kennwort>@<IP-Adresse des
   Administrationsservers>/KLSHARE /Volumes/KLSHARE
   ```

   Beschreibungen der Parameter:

   - `<Administratorkonto>` – Name des Administratorkontos auf dem Administrationsserver.
   - `<Kennwort>` – Kennwort des Administratorkontos auf dem Administrationsserver.
   - `<IP-Adresse des Administrationsservers>` – IP-Adresse des Host-Servers für Kaspersky Security Center.

4. Starten Sie das Installationsskript. Geben Sie dazu im SSH-Client den folgenden Befehl ein:

```
cd /Volumes/KLSHARE/<Ordner des KES-Pakets>
./install.sh --accept_eula
```

wobei `<Ordner des KES-Pakets>` der Ordner ist, in dem sich das Installationspaket für Kaspersky Endpoint Security befindet.

Wichtig: Für diesen Befehl sind Administratorrechte erforderlich.

5. Trennen Sie das Netzlaufwerk auf dem Remote-Computer. Geben Sie dazu im SSH-Client den folgenden Befehl ein:
   ```
   umount /Volumes/KLSHARE
   ```

Installation der Anwendung über Kaspersky Security Center

Bevor Sie Kaspersky Endpoint Security auf einem Client-Computer installieren, vergewissern Sie sich, ob folgende Bedingungen erfüllt sind:

- Der Administrationsserver für Kaspersky Security Center wurde im Unternehmensnetzwerk verteilt.
- Die Verwaltungskonsole wurde am Arbeitsplatz des Administrator für Kaspersky Security Center installiert.
- Der Administrationsagent ist auf dem Client-Computer installiert.
- Es wurde ein Installationspaket für Kaspersky Endpoint Security erstellt und im gemeinsam genutzten Ordner auf dem Administrationsserver abgelegt.
- Eine Schlüsseldatei für Kaspersky Endpoint Security wurde in einem gemeinsam genutzten Ordner auf dem Administrationsserver abgelegt (optional).
- Der Client-Computer wurde zur Administrationsgruppe **Verwaltete Geräte** auf dem Administrationsserver hinzugefügt (optional).

Ausführliche Informationen über Administrationsgruppen auf dem Administrationsserver finden Sie in der Hilfe zu Kaspersky Security Center.

Um Kaspersky Endpoint Security unter Verwendung von Kaspersky Security Center auf einem Client-Computer zu installieren, müssen Sie die Aufgabe **Remote-Installation eines Programms** erstellen und starten.

Aufgabe für die Remote-Installation von Kaspersky Endpoint Security auf einem Client-Computer erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie den Ordner **Aufgaben** aus.
4. Um den Assistenten für neue Aufgaben zu starten, klicken Sie im Arbeitsbereich auf **Neue Aufgabe**.
5. Folgen Sie den nachfolgenden Anweisungen des Assistenten für neue Aufgaben, um eine Aufgabe für die Remote-Installation von Kaspersky Endpoint Security auf einem Client-Computer zu erstellen.

Um zum nächsten Schritt des Assistenten zu gehen, klicken Sie auf **Weiter**. Um zum vorherigen Schritt des Assistenten zurückzukehren, klicken Sie auf ←. Um den Assistenten bei einem beliebigen Schritt abzubrechen, klicken Sie auf **Abbrechen**.

Hinweis: Das Aussehen der Schaltflächen kann je nach Windows-Version unterschiedlich sein.

Schritt 1. Aufgabentyp auswählen

1. Maximieren Sie im Fenster **Aufgabentyp auswählen** den Knoten **Kaspersky Security Center Administrationsserver**.
2. Wählen Sie die Aufgabe **Remote-Installation eines Programms** aus.

Schritt 2. Installationspaket auswählen

Führen Sie im Fenster **Installationspaket auswählen** eine der folgenden Aktionen aus:

- Falls bereits ein Installationspaket für Kaspersky Endpoint Security mit den erforderlichen Einstellungen erstellt wurde, wählen Sie das Paket oben im Fenster **Installationspaket auswählen** in der Liste der Installationspakete aus.
- Wenn das erforderliche Installationspaket noch nicht erstellt wurde, klicken Sie auf **Neu**, um den Assistenten für neue Pakete zu starten.

Schritt 3. Zusätzliche Anwendungen installieren

Aktivieren Sie im Fenster **Erweitert** die Kontrollkästchen **Administrationsagent gemeinsam mit diesem Programm installieren** und **<Name des Installationspakets des Administrationsagenten>**, wenn der Administrationsagent auch auf dem Client-Computer installiert werden soll.

Hinweis: Das Installationspaket für den Administrationsagenten muss zuvor erstellt werden. Wenn es noch nicht erstellt wurde, klicken Sie auf **Erstellen**, um den Assistenten für neue Pakete zu starten.

Schritt 4. Installationseinstellungen anpassen

Passen Sie im Fenster **Einstellungen** die Remote-Installation der Anwendung an.

Schritt 5. Administrationsgruppe auswählen, der nach der Installation Computer hinzugefügt werden sollen

Wählen Sie im Fenster **In die Liste mit verwalteten Geräten verschieben** eine Gruppe aus, in welche Computer falls nötig nach der Installation verschoben werden.

Hinweis: Das Fenster **In die Liste mit verwalteten Geräten verschieben** wird angezeigt, wenn Sie bei Schritt 3 die Installation des Administrationsagenten auswählen.

Schritt 6. Festlegen einer Methode zur Auswahl der Client-Computer, für die diese Aufgabe erstellt wird

Wählen Sie im Fenster **Geräte auswählen, denen die Aufgabe zugewiesen wird** das Verfahren aus, mit dem Client-Computer festgelegt werden sollen:

- Um die Client-Computer aus den Computern auszuwählen, die vom Administrationsserver im Netzwerk gefunden wurden, wählen Sie die Option **Geräte auswählen, die vom Administrationsserver erkannt wurden** aus.
- Um die IP-Adressen der Computer manuell anzugeben oder die IP-Adressen der Computer aus einer Datei zu importieren, wählen Sie die Variante **Geräteadressen manuell festlegen oder Adressen aus Liste importieren** aus.
- Um eine Aufgabe zu erstellen, mit der Geräte nach einem vordefinierten Kriterium ausgewählt werden, wählen Sie die Variante **Aufgabe einer Geräteauswahl zuordnen** aus.
- Um Computer aus einer bestimmten Administrationsgruppe auszuwählen, wählen Sie die Variante **Aufgabe einer Administrationsgruppe zuweisen** aus.

Schritt 7. Client-Computer auswählen

Im folgenden Fenster (**Geräte auswählen**, **Geräteauswahl** oder **Administrationsgruppe auswählen**, je nachdem, welche Variante Sie im vorherigen Schritt ausgewählt haben) können Sie die Client-Computer auswählen, die IP-Adressen der Computer angeben, die Computerauswahl angeben oder die Administrationsgruppe auswählen, auf die die Aufgabe angewendet werden soll.

Schritt 8. Benutzerkonto zum Ausführen der Aufgabe auswählen

Aktivieren Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** das Kontrollkästchen **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**.

Es wird davon ausgegangen, dass Sie den Administrationsagenten vor dem Starten dieses Assistenten installiert haben.

Schritt 9. Startzeitplan für die Aufgabe anpassen

1. Wählen Sie im Fenster **Aufgabenzeitplan anpassen** in der Dropdown-Liste **Start nach Zeitplan** einen Startmodus aus.
2. Konfigurieren Sie erforderlichenfalls den automatischen Start einer geplanten Aufgabe (indem Sie Datum und Uhrzeit des Aufgabenstarts festlegen).
3. Damit Aufgaben gestartet werden, die von der Anwendung nicht nach Zeitplan ausgeführt werden konnten (weil der Computer zum betreffenden Zeitpunkt beispielsweise ausgeschaltet war), aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

   Kaspersky Endpoint Security startet die Aufgabe, sobald der Aufgabenstart möglich ist.

Schritt 10. Name der Aufgabe festlegen

Geben Sie im Fenster **Aufgabenname festlegen** im Feld **Name** den Namen der zu erstellenden Aufgabe ein.

Schritt 11. Erstellen der Aufgabe abschließen

Gehen Sie im Fenster **Erstellung der Aufgabe abschließen** wie folgt vor:

1. Damit die Aufgabe gestartet wird, sobald der Assistent abgeschlossen wird, aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**.
2. Klicken Sie auf **Fertigstellen**, um den Assistenten abzuschließen.

Die erstellte Aufgabe wird im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

Installationspaket erstellen

Wenn Sie die Aufgabe **Remote-Installation eines Programms** erstellen, können Sie entweder ein vorhandenes Installationspaket verwenden oder ein neues erstellen. Um eine Liste der erstellten Installationspakete anzuzeigen, klicken Sie auf **Erweitert** > **Remote-Installation** > **Installationspakete**.

Installationspaket in Kaspersky Security Center erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie in der Baumstruktur den Ordner **Erweitert**, danach den Unterordner **Remote-Installation** und dann den Unterordner **Installationspakete** aus.
4. Klicken Sie im Arbeitsbereich auf **Installationspaket erstellen**.
5. Klicken Sie im Fenster **Typ des Installationspakets auswählen** auf **Installationspaket für eine Kaspersky-Anwendung erstellen**.
6. Geben Sie im Fenster **Name des Installationspakets festlegen** im Feld **Name** einen Namen für das neue Installationspaket ein und klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster **Programmpaket für die Installation auswählen** auf **Durchsuchen**.

   Im folgenden Fenster können Sie eine Datei zum Erstellen des Installationspakets auswählen.
8. Öffnen Sie den Ordner mit dem Installationspaket für Kaspersky Endpoint Security und wählen Sie die Datei kesmac.kud aus.

   Im Fenster **Programmpaket für die Installation auswählen** werden Name und Version der Anwendung genannt, die mit der hinzugefügten Datei per Fernzugriff installiert werden kann.
9. Aktivieren Sie das Kontrollkästchen **Updates aus der Datenverwaltung ins Installationspaket kopieren**, um bei Bedarf Updates für die Anwendung aus dem Speicher von Kaspersky Security Center in das Installationspaket zu kopieren, und klicken Sie auf **Weiter**.

   Das Installationspaket wird auf den Administrationsserver hochgeladen. Sobald der Upload abgeschlossen ist, wird das Fenster **Installationstyp** geöffnet.
10. Aktivieren oder deaktivieren Sie im Fenster **Installationstyp** im Abschnitt **Zu installierende Pakete** die Kontrollkästchen für jene Komponenten, die nicht auf dem Client-Computer installiert werden sollen. Klicken Sie dann auf **Weiter**.

    Ein Installationspaket für Kaspersky Endpoint Security wird mit den angegebenen Einstellungen erstellt.
11. Klicken Sie im letzten Fenster des Assistenten auf **Fertig**, um den Assistenten für neue Pakete abzuschließen.

Deinstallation der Anwendung über Kaspersky Security Center

Bevor Sie Kaspersky Endpoint Security über Kaspersky Security Center von einem Client-Computer entfernen, vergewissern Sie sich, dass folgende Bedingungen erfüllt sind:

- Der Administrationsserver für Kaspersky Security Center wurde im Unternehmensnetzwerk verteilt.
- Die Verwaltungskonsole wurde am Arbeitsplatz des Administrator für Kaspersky Security Center installiert.
- Der Administrationsagent ist auf dem Client-Computer installiert.

Um Kaspersky Endpoint Security über Kaspersky Security Center von einem Client-Computer zu entfernen, müssen Sie die Aufgabe **Remote-Deinstallation des Programms** erstellen und starten.

Wichtig: Wenn Sie Kaspersky Endpoint Security von einem Client-Computer entfernen, besteht für den Computer ein Infektionsrisiko.

Aufgabe für die Remote-Deinstallation von Kaspersky Endpoint Security von einem Client-Computer erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie den Ordner **Aufgaben** aus.
4. Um den Assistenten für neue Aufgaben zu starten, klicken Sie im Arbeitsbereich auf **Neue Aufgabe**.
5. Folgen Sie den nachfolgenden Anweisungen des Assistenten für neue Aufgaben, um eine Aufgabe für die Remote-Deinstallation von Kaspersky Endpoint Security von einem Client-Computer zu erstellen.

Um zum nächsten Schritt des Assistenten zu gehen, klicken Sie auf **Weiter**. Um zum vorherigen Schritt des Assistenten zurückzukehren, klicken Sie auf ←. Um den Assistenten bei einem beliebigen Schritt abzubrechen, klicken Sie auf **Abbrechen**.

Hinweis: Das Aussehen der Schaltflächen kann je nach Windows-Version unterschiedlich sein.

Schritt 1. Aufgabentyp auswählen

1. Maximieren Sie im Fenster **Aufgabentyp auswählen** den Knoten **Kaspersky Security Center Administrationsserver**.
2. Öffnen Sie den untergeordneten Knoten **Erweitert**.
3. Wählen Sie die Aufgabe **Remote-Deinstallation des Programms** aus.

Schritt 2. Zu entfernendes Programm auswählen

Wählen Sie im Fenster **Wählen Sie das zu deinstallierende Programm aus** die Variante **Programm deinstallieren, das von Kaspersky Security Center unterstützt wird** aus.

Schritt 3. Deinstallationseinstellungen anpassen

Gehen Sie im Fenster **Einstellungen** wie folgt vor:

1. Wählen Sie in der Dropdown-Liste **Zu deinstallierendes Programm** den Punkt **Kaspersky Endpoint Security for Mac 12.2** aus.

2. Klicken Sie auf **Weiter**.

3. Passen Sie die Remote-Deinstallation der Anwendung an.

Schritt 4. Option für den Neustart des Betriebssystems auswählen

Wählen Sie im Fenster **Methode zum Neustart des Betriebssystems** die Option **Gerät nicht neu starten** aus.

Schritt 5. Methode zur Auswahl der Client-Computer festlegen, für die diese Aufgabe erstellt wird

Wählen Sie im Fenster **Geräte auswählen, denen die Aufgabe zugewiesen wird** das Verfahren aus, mit dem Client-Computer festgelegt werden sollen:

- Um die Client-Computer aus den Computern auszuwählen, die vom Administrationsserver im Netzwerk gefunden wurden, wählen Sie die Option **Geräte auswählen, die vom Administrationsserver erkannt wurden** aus.

- Um die IP-Adressen der Computer manuell anzugeben oder die IP-Adressen der Computer aus einer Datei zu importieren, wählen Sie die Variante **Geräteadressen manuell festlegen oder Adressen aus Liste importieren** aus.

- Um eine Aufgabe zu erstellen, mit der Geräte nach einem vordefinierten Kriterium ausgewählt werden, wählen Sie die Variante **Aufgabe einer Geräteauswahl zuordnen** aus.

- Um Computer aus einer bestimmten Administrationsgruppe auszuwählen, wählen Sie die Variante **Aufgabe einer Administrationsgruppe zuweisen** aus.

Schritt 6. Client-Computer auswählen

Im folgenden Fenster (**Geräte auswählen**, **Geräteauswahl** oder **Administrationsgruppe auswählen**, je nachdem, welche Variante Sie im vorherigen Schritt ausgewählt haben) können Sie die Client-Computer auswählen, die IP-Adressen der Computer angeben, die Computerauswahl angeben oder die Administrationsgruppe auswählen, auf die die Aufgabe angewendet werden soll.

Schritt 7. Benutzerkonto für den Aufgabenstart auswählen

Aktivieren Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** das Kontrollkästchen **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**.

Es wird davon ausgegangen, dass Sie den Administrationsagenten vor dem Starten dieses Assistenten installiert haben.

Schritt 8. Startzeitplan für die Aufgabe anpassen

1. Wählen Sie im Fenster **Aufgabenzeitplan anpassen** in der Dropdown-Liste **Start nach Zeitplan** einen Startmodus aus.

2. Konfigurieren Sie erforderlichenfalls den automatischen Start einer geplanten Aufgabe (indem Sie Datum und Uhrzeit des Aufgabenstarts festlegen).

3. Damit Aufgaben gestartet werden, die von der Anwendung nicht nach Zeitplan ausgeführt werden konnten (weil der Computer zum betreffenden Zeitpunkt beispielsweise ausgeschaltet war), aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

   Kaspersky Endpoint Security startet die Aufgabe, sobald der Aufgabenstart möglich ist.

Schritt 9. Aufgabenname festlegen

Geben Sie im Fenster **Aufgabenname festlegen** im Feld **Name** den Namen der zu erstellenden Aufgabe ein.

Schritt 10. Erstellen der Aufgabe abschließen

Gehen Sie im Fenster **Erstellung der Aufgabe abschließen** wie folgt vor:

1. Damit die Aufgabe gestartet wird, sobald der Assistent abgeschlossen wird, aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**.
2. Klicken Sie auf **Fertigstellen**, um den Assistenten abzuschließen.

Die erstellte Aufgabe wird im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

Anwendung über Kaspersky Security Center starten oder beenden

Sie können Kaspersky Endpoint Security auf einem ausgewählten Computer in der Liste der über Kaspersky Security Center verwalteten Geräte starten oder beenden.

Kaspersky Endpoint Security über Kaspersky Security Center starten oder beenden

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie die Registerkarte **Geräte**.
6. Wählen Sie in der Liste der Client-Computer einen Computer aus.
7. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des Client-Computers.
   - Klicken Sie mit der rechten Maustaste auf den Client-Computer und wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
8. Gehen Sie zum Abschnitt **Programme**.

9. Gehen Sie zur Liste **Auf dem Gerät installierte Kaspersky-Anwendungen** und rechtsklicken Sie auf den Eintrag **Kaspersky Endpoint Security for Mac 12.2**, um das Kontextmenü zu öffnen, und führen Sie dann eine der folgenden Aktionen aus:

   - Um die Anwendung zu starten, wählen Sie **Starten** aus.
   - Um die Anwendung zu beenden, wählen Sie **Beenden** aus.

Wichtig: Nachdem Kaspersky Endpoint Security beendet wurde, läuft der Client-Computer im ungeschützten Modus weiter und unterliegt einem Infektionsrisiko.

Aufgaben erstellen und verwalten

Dieser Abschnitt informiert darüber, wie in Kaspersky Security Center Aufgaben erstellt und angepasst werden, die Kaspersky Endpoint Security auf einem Client-Computer oder einer Gruppe von Computern ausführt.

Eine Aufgabe ist eine Auswahl konfigurierbarer Aktionen, die von Kaspersky Endpoint Security auf einem Client-Computer ausgeführt werden.

In Kaspersky Security Center können Sie folgende Aufgaben erstellen:

- Schlüssel hinzufügen
- Schnelle Untersuchung
- Rollback
- Virensuche
- Aktualisieren

Mit Aufgaben sind folgende Aktionen möglich:

- Aufgaben starten und beenden
- Aufgabeneinstellungen konfigurieren
- Fortschritt einer Aufgabe verfolgen
- Aufgaben aus einer Gruppe in eine andere Gruppe kopieren und verschieben
- Aufgaben löschen
- Aufgaben importieren und exportieren

Ausführliche Informationen über Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Aufgaben erstellen

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center verwalten, können Sie folgende Aufgabentypen erstellen:

- Lokale Aufgaben *Eine lokale Aufgabe* ist eine Aufgabe, die auf einem separaten Client-Computer ausgeführt wird.
- Gruppenaufgaben *Eine Gruppenaufgabe* ist eine Aufgabe, die auf Computern in einer Administrationsgruppe ausgeführt werden kann.
- Aufgaben für mehrere beliebige Computer Sie können eine Aufgabe erstellen, um sie auf beliebigen Computern auszuführen, unabhängig davon, ob diese zu einer Administrationsgruppe oder einer Computerauswahl gehören.

Lokale Aufgabe für einen einzelnen Client-Computer erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Geräte**.
6. Wählen Sie in der Liste der Client-Computer den gewünschten Computer aus.
7. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des Client-Computers.
   - Klicken Sie mit der rechten Maustaste auf den Client-Computer und wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
8. Gehen Sie im Fenster **Eigenschaften: <Computername>** zum Abschnitt **Aufgaben**.

   Im Arbeitsbereich wird rechts eine Liste der Systemaufgaben und benutzerdefinierten Aufgaben für den ausgewählten Client-Computer angezeigt.
9. Klicken Sie unten im Arbeitsbereich auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.
10. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben, um eine lokale Aufgabe für einen einzelnen Client-Computer zu erstellen.

Aufgabe für Client-Computer in einer Administrationsgruppe erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.

4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Aufgaben**.
6. Klicken Sie im Arbeitsbereich auf **Neue Aufgabe,** um den Assistenten für neue Aufgaben zu starten.
7. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben, um eine Aufgabe für die Client-Computer zu erstellen, die zu einer Administrationsgruppe gehören.

Details zum Erstellen von Gruppenaufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Aufgaben für mehrere beliebige Computer erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Aufgaben**.
4. Klicken Sie im Arbeitsbereich auf **Neue Aufgabe,** um den Assistenten für neue Aufgaben zu starten.
5. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben, um eine Aufgabe für eine bestimmte Auswahl von Computern zu erstellen.

Um zum nächsten Schritt des Assistenten zu gehen, klicken Sie auf **Weiter**. Um zum vorherigen Schritt des Assistenten zurückzukehren, klicken Sie auf ←. Um den Assistenten bei einem beliebigen Schritt abzubrechen, klicken Sie auf **Abbrechen**.

Hinweis: Das Aussehen der Schaltflächen kann je nach Windows-Version unterschiedlich sein.

Schritt 1. Programm auswählen und Aufgabentyp angeben

1. Maximieren Sie im Fenster **Aufgabentyp auswählen** den Knoten **Kaspersky Endpoint Security for Mac 12.2**.
2. Wählen Sie den Typ der Aufgabe aus, die Sie erstellen möchten:
   - Um eine Aufgabe zum Hinzufügen eines Schlüssels zu erstellen, wählen Sie **Schlüssel hinzufügen** aus.
   - Um eine Untersuchungsaufgabe für kritische Bereiche zu erstellen, wählen Sie die Variante **Schnelle Untersuchung** aus.
   - Um eine Aufgabe zum Rollback des letzten Updates zu erstellen, wählen Sie **Rollback** aus.
   - Um eine Untersuchungsaufgabe zu erstellen, wählen Sie den Punkt **Untersuchung** aus.
   - Um eine Update-Aufgabe zu erstellen, wählen Sie **Update** aus.

Schritt 2. Einstellungen für den ausgewählten Aufgabentyp anpassen

Abhängig davon, welcher Aufgabentyp beim vorherigen Schritt ausgewählt wurde, kann sich das Aussehen des Konfigurationsfensters für die Aufgabe unterscheiden. Für die Aufgabe für ein Rollback wird dieses Fenster nicht angezeigt.

Anwendungsaktivierung

Gehen Sie im Fenster **Aktivierung der App** wie folgt vor:

1. Wählen Sie einen Aktivierungscode oder Schlüssel aus dem Speicher von Kaspersky Security Center aus, oder fügen Sie eine auf Ihrem Computer gespeicherte Schlüsseldatei hinzu.

2. Wenn Sie den angegebenen Schlüssel als Reserveschlüssel hinzufügen möchten, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel hinzufügen**.

   Der Reserveschlüssel wird aktiviert, wenn der aktuelle aktive Schlüssel abläuft.

Informationen über den angegebenen Schlüssel (Schlüssel sowie Typ und Gültigkeitsdauer des Schlüssels) werden im Fenster **Aktivierung der App** angezeigt.

Aktualisieren

Die grundlegende Update-Quelle für Kaspersky Endpoint Security sind die dedizierten Kaspersky-Update-Server. Kaspersky Endpoint Security kann auch Verteilungspunkte, lokale Ordner oder andere Webserver als *Update-Quelle* verwenden.

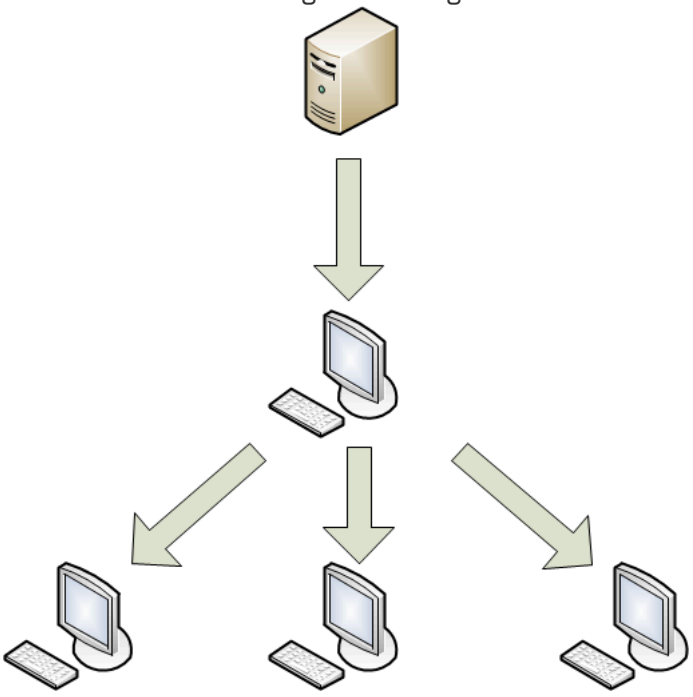
Sie können heruntergeladene Updates in einem lokalen Ordner ablegen, um die Anwendungsdatenbanken und Module von Kaspersky Endpoint Security auf anderen Computern des Unternehmensnetzwerks zu aktualisieren. Dadurch wird das Volumen des Internet-Datenverkehrs reduziert.

Sie können die Update-Verteilung wie folgt einrichten:

1. Ein Computer im Netzwerk lädt das Update-Paket für Kaspersky Endpoint Security von den Kaspersky-Update-Servern oder aus einer anderen Update-Quelle herunter. Die heruntergeladenen Updates werden in einem gemeinsam genutzten lokalen Ordner abgelegt.

   Hinweis: Der freigegebene lokale Ordner muss zuvor erstellt werden.

2. Die anderen Computer im Netzwerk verwenden den gemeinsam genutzten lokalen Ordner als Update-Quelle.



Update-Verteilung über einen lokalen Computer

Ändern Sie im Fenster **Aktualisieren** bei Bedarf die Einstellungen der Update-Aufgabe:

1. Um das Update der Anwendungsmodule auszuschalten, deaktivieren Sie das Kontrollkästchen **App-Module aktualisieren**.

2. Um die Update-Quellen zu ändern:

   a. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen: Update** wird geöffnet.

   b. Aktivieren Sie die Kontrollkästchen für jene Update-Quellen, die Sie verwenden möchten.

3. Wenn Sie eine andere Update-Quelle angeben möchten, klicken Sie auf **Hinzufügen**.

   Das Fenster **Update-Quelle** wird geöffnet.

   a. Geben Sie entweder die Webadresse der Update-Quelle oder den Pfad eines lokalen Ordners oder eines Netzwerkordner an, der als Update-Quelle dient, und klicken Sie auf **OK**.

   b. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Update** zu schließen.

Untersuchung und Schnelle Untersuchung

Kaspersky Endpoint Security verwendet standardmäßig die Sicherheitsstufe **Empfohlen**, fragt beim Fund eines infizierten Objekts am Ende der Untersuchung nach einer Aktion und untersucht die folgenden Objekte:

- Alle Wechseldatenträger
- Alle internen Laufwerke

- Alle Netzlaufwerke
- Arbeitsspeicher

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Ändern Sie im Fenster **Untersuchung** bei Bedarf die Untersuchungseinstellungen:

1. Wählen Sie eine der vordefinierten Sicherheitsstufen aus oder passen Sie die Sicherheitseinstellungen an.
2. Legen Sie fest, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.
3. Legen Sie den Untersuchungsbereich fest.

Schritt 3. Methode zur Auswahl der Client-Computer festlegen, für die diese Aufgabe erstellt wird

Hinweis: Dieser Schritt ist für lokale Aufgaben oder Gruppenaufgaben nicht relevant.

Wählen Sie im Fenster **Geräte auswählen, denen die Aufgabe zugewiesen wird** das Verfahren aus, mit dem Client-Computer festgelegt werden sollen:

- Um die Client-Computer aus den Computern auszuwählen, die vom Administrationsserver im Netzwerk gefunden wurden, wählen Sie die Option **Geräte auswählen, die vom Administrationsserver erkannt wurden** aus.
- Um die IP-Adressen der Computer manuell anzugeben oder die IP-Adressen der Computer aus einer Datei zu importieren, wählen Sie die Variante **Geräteadressen manuell festlegen oder Adressen aus Liste importieren** aus.
- Um eine Aufgabe zu erstellen, mit der Geräte nach einem vordefinierten Kriterium ausgewählt werden, wählen Sie die Variante **Aufgabe einer Geräteauswahl zuordnen** aus.
- Um Computer aus einer bestimmten Administrationsgruppe auszuwählen, wählen Sie die Variante **Aufgabe einer Administrationsgruppe zuweisen** aus.

Schritt 4. Client-Computer auswählen

Hinweis: Dieser Schritt ist für lokale Aufgaben oder Gruppenaufgaben nicht relevant.

Im folgenden Fenster (**Geräte auswählen**, **Geräteauswahl** oder **Administrationsgruppe auswählen**, je nachdem, welche Variante Sie im vorherigen Schritt ausgewählt haben) können Sie die Client-Computer auswählen, die IP-Adressen der Computer angeben, die Computerauswahl angeben oder die Administrationsgruppe auswählen, auf die die Aufgabe angewendet werden soll.

Schritt 5. Startzeitplan für die Aufgabe anpassen

1. Wählen Sie im Fenster **Aufgabenzeitplan anpassen** in der Dropdown-Liste **Start nach Zeitplan** einen Startmodus aus.

2. Konfigurieren Sie erforderlichenfalls den automatischen Start einer geplanten Aufgabe (indem Sie Datum und Uhrzeit des Aufgabenstarts festlegen).

3. Damit Aufgaben gestartet werden, die von der Anwendung nicht nach Zeitplan ausgeführt werden konnten (weil der Computer zum betreffenden Zeitpunkt beispielsweise ausgeschaltet war), aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

   Kaspersky Endpoint Security startet die Aufgabe, sobald der Aufgabenstart möglich ist.

4. Damit Kaspersky Security Center automatisch festlegt, in welchem Intervall die Aufgaben auf unterschiedlichen Computern gestartet werden, aktivieren Sie das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**.

   So kann die Last des Administrationsservers für Kaspersky Security Center reduziert werden.

5. Wenn Sie das Intervall, in dem die Aufgaben auf unterschiedlichen Computern gestartet werden sollen, manuell festlegen möchten, aktivieren Sie das Kontrollkästchen **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.):** und geben Sie einen Zeitraum (in Minuten) an.

   So kann die Last des Administrationsservers für Kaspersky Security Center reduziert werden.

Schritt 6. Aufgabenname festlegen

Geben Sie im Fenster **Aufgabenname festlegen** im Feld **Name** den Namen der zu erstellenden Aufgabe ein.

Schritt 7. Erstellen der Aufgabe abschließen

Gehen Sie im Fenster **Erstellung der Aufgabe abschließen** wie folgt vor:

1. Damit die Aufgabe gestartet wird, sobald der Assistent abgeschlossen wird, aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**.

2. Klicken Sie auf **Fertigstellen**, um den Assistenten abzuschließen.

Aufgaben manuell starten und beenden

Geplante Aufgaben werden automatisch nach Zeitplan gestartet und beendet. Sie können eine Aufgabe jedoch jederzeit manuell starten.

Hinweis: Aufgaben werden nur dann auf einem Client-Computer gestartet, wenn der Administrationsagent läuft. Wenn der Administrationsagent beendet wird, werden alle aktiven Aufgaben abgebrochen.

Aufgaben manuell starten und beenden

1. Öffnen Sie die Aufgabenliste mit der Aufgabe, die Sie starten oder beenden möchten.

2. Wählen Sie die Aufgabe aus, die Sie starten oder beenden möchten.

3. Verwenden Sie eine der folgenden Methoden, um die Aufgabe zu starten oder zu beenden:

   - Öffnen Sie durch Rechtsklick das Kontextmenü für die Aufgabe und wählen Sie den Punkt **Starten** oder **Beenden**.
   - Klicken Sie im Arbeitsbereich auf **Starten** oder **Beenden**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü für die Aufgabe und wählen Sie den Punkt **Eigenschaften**. Klicken Sie im folgenden Fenster auf **Starten** oder **Beenden**.

Aufgaben importieren und exportieren

Sie können Gruppenaufgaben und Aufgaben für eine beliebige Auswahl von Computern in eine Datei exportieren.

Aufgabe exportieren

1. Wählen Sie die Aufgabenliste aus, aus der Sie die Aufgabe exportieren möchten:

   - Wählen Sie die Administrationsgruppe aus und öffnen Sie dann die Registerkarte **Aufgaben**.
   - Klicken Sie in der Konsolenstruktur auf **Aufgaben**.

2. Klicken Sie mit der rechten Maustaste auf die Aufgabe, die Sie exportieren möchten, und wählen Sie im Kontextmenü der Aufgabe **Alle Aufgaben** > **Exportieren** aus.
3. Geben Sie im Fenster **Speichern unter** den Dateinamen an und den Ordner, in dem die exportierte Aufgabe gespeichert werden soll.
4. Klicken Sie auf **Speichern**.

Aufgabe importieren

1. Wählen Sie die Aufgabenliste aus, in die Sie die Aufgabe importieren möchten:

   - Wählen Sie die Administrationsgruppe aus und öffnen Sie dann die Registerkarte **Aufgaben**.
   - Klicken Sie in der Konsolenstruktur auf **Aufgaben**.

2. Verwenden Sie eine der folgenden Methoden, um die Aufgabe zu importieren:

   - Wählen Sie im Kontextmenü der Aufgabenliste **Alle Aufgaben** > **Importieren** aus.
   - Klicken Sie auf **Aufgabe aus Datei importieren**.

3. Geben Sie im Fenster **Öffnen** den Pfad zu der Aufgabendatei an, die Sie importieren möchten.
4. Klicken Sie auf **Öffnen**.

Die Aufgabe wird in der Aufgabenliste angezeigt.

Aufgaben anzeigen

Sie können die Liste der Aufgaben anzeigen, die für einen bestimmten Computer oder für Computer in einer bestimmten Administrationsgruppe erstellt wurden, oder die Liste aller nicht lokalen Aufgaben.

Aufgaben für eine bestimmte Administrationsgruppe anzeigen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Aufgaben**.

Eine Liste der Aufgaben für die Computer in der ausgewählten Administrationsgruppe wird angezeigt.

Lokale Aufgaben anzeigen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Geräte**.
6. Wählen Sie in der Liste der Client-Computer den gewünschten Computer aus.
7. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des Client-Computers.
   - Klicken Sie mit der rechten Maustaste auf den Client-Computer und wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
8. Gehen Sie im Fenster **Eigenschaften: <Computername>** zum Abschnitt **Aufgaben**.

Im Arbeitsbereich wird rechts eine Liste der Systemaufgaben und benutzerdefinierten Aufgaben für den ausgewählten Client-Computer angezeigt.

Nicht lokale Aufgaben anzeigen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Aufgaben**.

Eine Liste der nicht lokalen Aufgaben für Computer, die nicht unbedingt zu einer Administrationsgruppe gehören müssen, wird angezeigt.

Aufgabenspezifische Einstellungen verwalten

Einstellungen einer lokalen Aufgabe anzeigen

1. Öffnen Sie die Liste der lokalen Aufgaben.
2. Wählen Sie in der Liste eine Aufgabe aus und verwenden Sie eine der folgenden Methoden, um die Aufgabeneinstellungen zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

Einstellungen einer Gruppenaufgabe anzeigen

1. Öffnen Sie die Liste der Gruppenaufgaben für eine Administrationsgruppe.
2. Wählen Sie in der Liste eine Aufgabe aus und verwenden Sie eine der folgenden Methoden, um die Aufgabeneinstellungen zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.
   - Klicken Sie im Arbeitsbereich auf den Link **Aufgabeneinstellungen anpassen**.

Einstellungen einer nicht lokalen Aufgabe anzeigen

1. Öffnen Sie die Liste der nicht lokalen Aufgaben.
2. Wählen Sie in der Liste eine Aufgabe aus und verwenden Sie eine der folgenden Methoden, um die Aufgabeneinstellungen zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.
   - Klicken Sie im Arbeitsbereich auf den Link **Aufgabeneinstellungen anpassen**.

Details zu Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Für lokale Aufgaben, Gruppenaufgaben oder Aufgaben für mehrere beliebige Computer

Einstellungen für die Aufgabe „Schlüssel hinzufügen“ verwalten

1. Öffnen Sie das Fenster mit den Einstellungen für die Aufgabe **Schlüssel hinzufügen**.
2. Gehen Sie zum Abschnitt **Aktivierung der App**.

3. Verwenden Sie, falls erforderlich, eine der folgenden Methoden, um einen anderen Schlüssel hinzuzufügen:

   - Um einen Schlüssel oder einen Aktivierungscode aus der Liste der Aktivierungscodes im Speicher von Kaspersky Security Center auszuwählen:

     a. Wählen Sie die Option **Schlüssel oder Aktivierungscode** aus.

     b. Klicken Sie auf **Durchsuchen**.

     Das Fenster **Schlüssel und Aktivierungscodes im Speicher von Kaspersky Security Center** wird geöffnet.

     c. Wählen Sie einen Schlüssel oder einen Aktivierungscode aus.

     d. Klicken Sie auf **OK**.

   - Um eine Schlüsseldatei hinzuzufügen:

     a. Wählen Sie die Option **Schlüsseldatei** aus.

     b. Klicken Sie auf **Hinzufügen**.

     Ein Fenster zur Dateiauswahl wird geöffnet.

     c. Wählen Sie eine Schlüsseldatei aus.

     d. Klicken Sie auf **Öffnen**.

   Hinweis: Der aktuelle Schlüssel wird gelöscht, wenn ein anderer Schlüssel hinzugefügt wird.

4. Um den angegebenen Schlüssel als Reserveschlüssel hinzuzufügen, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel hinzufügen**.

   Der Reserveschlüssel wird aktiviert, wenn der aktuelle Schlüssel abläuft.

   Hinweis: Das Ablaufdatum des Reserveschlüssels muss später liegen als das Ablaufdatum des aktuellen Schlüssels.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.
   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

Einstellungen für die Aufgabe „Schnelle Untersuchung“ verwalten

1. Öffnen Sie das Fenster mit den Einstellungen der Aufgabe **Schnelle Untersuchung**.
2. Wählen Sie den Abschnitt **Schnelle Untersuchung** aus.

3. Um die Sicherheitsstufe zu ändern, mit der Kaspersky Endpoint Security die Aufgabe „Schnelle Untersuchung“ ausführt, führen Sie im Abschnitt **Sicherheitsstufe** eine der folgenden Aktionen aus:

   - Wählen Sie mit dem Schieberegler eine vordefinierte Sicherheitsstufe aus.

     Folgende Sicherheitsstufen stehen zur Auswahl:

     - **Maximaler Schutz**. Kaspersky Endpoint Security überwacht die Dateien, die geöffnet, gespeichert und ausgeführt werden, mit höchster Genauigkeit.
     - **Empfohlen**. Um Dateien zu überwachen, verwendet Kaspersky Endpoint Security die von Kaspersky empfohlenen Einstellungen.

       Diese Sicherheitsstufe gilt als Standard.
     - **Maximale Geschwindigkeit**. Kaspersky Endpoint Security überwacht eine minimale Auswahl von Dateien. Diese Sicherheitsstufe ist geeignet, wenn Sie andere Anwendungen verwenden möchten, die den Arbeitsspeicher stark beanspruchen.

   - Passen Sie die Sicherheitseinstellungen manuell an:

     a. Klicken **Einstellungen**.

        Das Fenster **Einstellungen: Untersuchung** wird geöffnet.

     b. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security im Rahmen der Aufgabe „Schnelle Untersuchung“ untersuchen soll.

     c. Passen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** die Leistungseinstellungen der Untersuchung an.

     d. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien Kaspersky Endpoint Security auf bedrohliche Objekte untersuchen soll.

     e. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Erweiterte Einstellungen** die Verwendung der iSwift-Technologie und die Aufzeichnung von Informationen über erkannte Objekte in der Anwendungsstatistik an.

     f. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** die Verwendung der „Heuristischen Analyse“ an und wählen Sie aus, welche Schutzstufe der „Heuristischen Analyse“ bei Schadsoftware-Untersuchungen verwenden werden soll.

     g. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Untersuchung** zu schließen.

        Die Sicherheitsstufe ändert sich in **Benutzerdefiniert**.

   - Um die Standardeinstellungen wiederherzustellen, klicken Sie auf **Standard**.

     Die Sicherheitsstufe ändert sich in **Empfohlen**.

4. Wählen Sie im Abschnitt **Aktion** bei Bedarf aus, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.

5. Um einen Untersuchungsbereich anzugeben, klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen** und gehen Sie im folgenden Fenster **Untersuchungsbereich** wie folgt vor:

   a. Damit Kaspersky Endpoint Security den Arbeitsspeicher des Computers untersucht, aktivieren Sie das Kontrollkästchen **Arbeitsspeicher**.

   b. Damit Kaspersky Endpoint Security die Autostart-Objekte untersucht, aktivieren Sie das Kontrollkästchen **Anmeldeobjekte**.

   c. Wenn Sie mit Kaspersky Endpoint Security zusätzliche Dateien oder Ordner untersuchen möchten, klicken Sie auf **Hinzufügen** und geben eine Datei, einen Ordner oder eine Maske für Datei- oder Ordnernamen an.

   d. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Untersuchungsbereich** zu schließen.

6. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

Einstellungen für die Untersuchungsaufgabe verwalten

1. Öffnen Sie das Fenster mit den Einstellungen für die Aufgabe **Untersuchung**.

2. Gehen Sie zum Abschnitt **Untersuchung**.

3. Um die Sicherheitsstufe zu ändern, mit der Kaspersky Endpoint Security die Untersuchungsaufgabe ausführt, führen Sie im Abschnitt **Sicherheitsstufe** eine der folgenden Aktionen aus:

   - Wählen Sie mit dem Schieberegler eine vordefinierte Sicherheitsstufe aus.

     Folgende Sicherheitsstufen stehen zur Auswahl:

     - **Maximaler Schutz**. Kaspersky Endpoint Security überwacht die Dateien, die geöffnet, gespeichert und ausgeführt werden, mit höchster Genauigkeit.

     - **Empfohlen**. Um Dateien zu überwachen, verwendet Kaspersky Endpoint Security die von Kaspersky empfohlenen Einstellungen.

       Diese Sicherheitsstufe gilt als Standard.

     - **Maximale Geschwindigkeit**. Kaspersky Endpoint Security überwacht eine minimale Auswahl von Dateien. Diese Sicherheitsstufe ist geeignet, wenn Sie andere Anwendungen verwenden möchten, die den Arbeitsspeicher stark beanspruchen.

   - Passen Sie die Sicherheitseinstellungen manuell an:

     a. Klicken Sie auf **Einstellungen**.

        Das Fenster **Einstellungen: Untersuchung** wird geöffnet.

     b. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security im Rahmen der Untersuchungsaufgabe scannen soll.

     c. Passen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** die Leistungseinstellungen der Untersuchung an.

d. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien Kaspersky Endpoint Security auf bedrohliche Objekte untersuchen soll.

e. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Erweiterte Einstellungen** die Verwendung der iSwift-Technologie und die Aufzeichnung von Informationen über erkannte Objekte in der Anwendungsstatistik an.

f. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** die Verwendung der „Heuristischen Analyse“ an und wählen Sie aus, welche Schutzstufe der „Heuristischen Analyse“ bei Schadsoftware-Untersuchungen verwenden werden soll.

g. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Untersuchung** zu schließen.

Die Sicherheitsstufe ändert sich in **Benutzerdefiniert**.

- Um die Standardeinstellungen wiederherzustellen, klicken Sie auf **Standard**.

  Die Sicherheitsstufe ändert sich in **Empfohlen**.

4. Wählen Sie im Abschnitt **Aktion** bei Bedarf aus, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.

5. Um einen Untersuchungsbereich anzugeben, klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen** und gehen Sie im folgenden Fenster **Untersuchungsbereich** wie folgt vor:

   a. Damit Kaspersky Endpoint Security alle Wechseldatenträger untersucht, aktivieren Sie das Kontrollkästchen **Alle Wechseldatenträger**.

   b. Damit Kaspersky Endpoint Security alle internen Datenträger untersucht, aktivieren Sie das Kontrollkästchen **Alle internen Datenträger**.

   c. Damit Kaspersky Endpoint Security alle Netzlaufwerke untersucht, aktivieren Sie das Kontrollkästchen **Alle Netzlaufwerke**.

   d. Damit Kaspersky Endpoint Security den Arbeitsspeicher des Computers untersucht, aktivieren Sie das Kontrollkästchen **Arbeitsspeicher**.

   e. Damit Kaspersky Endpoint Security die Autostart-Objekte untersucht, aktivieren Sie das Kontrollkästchen **Anmeldeobjekte**.

   f. Um mit Kaspersky Endpoint Security andere Dateien oder Ordner zu untersuchen, klicken Sie auf **Hinzufügen** und geben eine Datei, einen Ordner oder eine Maske für Datei- oder Ordnernamen an.

   g. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Untersuchungsbereich** zu schließen.

6. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

Einstellungen für die Update-Aufgabe verwalten

1. Öffnen Sie das Fenster mit den Einstellungen für die Aufgabe **Update**.
2. Gehen Sie zum Abschnitt **Aktualisieren**.
3. Damit Kaspersky Endpoint Security die Anwendungsmodule zusammen mit den Anwendungsdatenbanken aktualisiert, aktivieren Sie das Kontrollkästchen **App-Module aktualisieren**.
4. Um eine Update-Quelle auszuwählen:
   a. Klicken Sie auf **Einstellungen**.
      Das Fenster **Einstellungen: Update** wird geöffnet.
   b. Verwenden Sie eine der folgenden Methoden, um eine Update-Quelle anzugeben:
      - Damit die Anwendung die Updates vom Administrationsserver herunterlädt, aktivieren Sie das Kontrollkästchen **Kaspersky Security Center**.
      - Damit die Anwendung die Updates von den Kaspersky-Update-Servern herunterlädt, aktivieren Sie das Kontrollkästchen **Kaspersky-Update-Server**.
      - Um eine andere Update-Quelle hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster den Pfad der Update-Quelle ein.
        Standardmäßig lädt Kaspersky Endpoint Security die Updates von den Kaspersky-Update-Servern herunter.
   c. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Update** zu schließen.
5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:
   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.
   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Aufgabe>** zu schließen.

Nur für lokale Aufgaben

Einstellungen für die Aufgabe „Schutz vor bedrohlichen Dateien“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.
2. Wählen Sie in der Liste der lokalen Aufgaben die Aufgabe „Schutz vor bedrohlichen Dateien“ aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf **Eigenschaften**.

3. Wählen Sie den Abschnitt **Schutz vor bedrohlichen Dateien** aus.

4. Passen Sie falls nötig die folgenden Einstellungen an:

   - Aktivieren oder deaktivieren Sie den „Schutz vor bedrohlichen Dateien“ auf dem Client-Computer.

   - Um eine der vordefinierten Sicherheitsstufen auszuwählen, verwenden Sie den Schieberegler im Abschnitt **Sicherheitsstufe**.

   - Um die Sicherheitseinstellungen manuell anzupassen, klicken Sie auf **Einstellungen** und gehen Sie im Fenster **Einstellungen: Schutz vor bedrohlichen Dateien** wie folgt vor:

     a. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security beim Öffnen, Ausführen und Speichern untersuchen soll.

     b. Gehen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** wie folgt vor: Passen Sie die Leistungseinstellungen für die Untersuchung an, wählen Sie die Untersuchungstechnologie aus und legen Sie fest, ob Kaspersky Endpoint Security das schreibgeschützte Systemvolume bei der Untersuchung auf Client-Computern überspringen soll.

     c. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien auf erkennbare Objekte untersucht werden sollen, und legen Sie eine Beschränkung für die Untersuchung großer Objekte fest.

     d. Geben Sie auf der Registerkarte **Schutzbereich** die Dateien oder Ordner an, die vom „Schutz vor bedrohlichen Dateien“ untersucht werden sollen.

        Standardmäßig werden alle Objekte untersucht, die sich auf mit dem Client-Computer verbundenen Wechseldatenträgern, internen Laufwerken und Netzlaufwerken befinden. Sie können ein Objekt zum Schutzbereich hinzufügen, ein Objekt aus der Liste ändern, die Untersuchung eines Objekts vorübergehend deaktivieren oder ein Objekt löschen.

     e. Wählen Sie auf der Registerkarte **Erweitert** im Abschnitt **Untersuchungsmodus** den Modus für den „Schutz vor bedrohlichen Dateien“ aus.

     f. Legen Sie auf der Registerkarte **Erweitert** im Abschnitt **Aufgabe anhalten** fest, ob der „Schutz vor bedrohlichen Dateien“ nach Zeitplan angehalten werden soll, und passen Sie einen Zeitplan für das automatische Anhalten von Aufgaben an.

     g. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** an, wie der „Schutz vor bedrohlichen Dateien“ die „Heuristische Analyse“ verwenden soll.

     h. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Schutz vor bedrohlichen Dateien** zu schließen.

   - Wählen Sie im Abschnitt **Beim Erkennen eines schädlichen Objekts** aus, welche Aktion der „Schutz vor bedrohlichen Dateien“ beim Fund eines infizierten Objekts ausführen soll.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Schutz vor bedrohlichen Dateien** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Schutz vor bedrohlichen Dateien** zu schließen.

Einstellungen für die Aufgabe „Schutz vor Web-Bedrohungen“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.
2. Wählen Sie in der Liste der lokalen Aufgaben die Aufgabe „Schutz vor Web-Bedrohungen“ aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf **Eigenschaften**.
3. Wählen Sie den Abschnitt **Schutz vor Web-Bedrohungen** aus.
4. Passen Sie falls nötig die folgenden Einstellungen an:
   - Aktivieren oder deaktivieren Sie den „Schutz vor Web-Bedrohungen“ auf dem Client-Computer.
   - Um eine der vordefinierten Sicherheitsstufen auszuwählen, verwenden Sie den Schieberegler im Abschnitt **Sicherheitsstufe**.
   - Um die Sicherheitseinstellungen manuell anzupassen, klicken Sie auf **Einstellungen** und gehen Sie im Fenster **Einstellungen: Schutz vor Web-Bedrohungen** wie folgt vor:
     a. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Untersuchungsmodus** die Untersuchung von Webadressen unter Verwendung der Datenbank für bösartige Webadressen.
     b. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Anti-Phishing-Einstellungen** die Untersuchung von Webadressen unter Verwendung der Datenbank für Phishing-Webadressen.
     c. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Anti-Phishing-Einstellungen** die Verwendung der „Heuristischen Analyse“ zum Erkennen von Phishing-Links.
     d. Aktivieren oder deaktivieren Sie auf der Registerkarte **Vertrauenswürdige Webadressen** die Untersuchung des Web-Datenverkehrs von vertrauenswürdigen Webadresse, und erstellen oder bearbeiten Sie eine Liste mit vertrauenswürdigen Webadressen.
     e. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Schutz vor Web-Bedrohungen** zu schließen.
5. Wählen Sie im Abschnitt **Beim Erkennen eines schädlichen Objekts** aus, welche Aktion der „Schutz vor Web-Bedrohungen“ ausführen soll, wenn im Web-Datenverkehr ein gefährliches Objekt gefunden wird.
6. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:
   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Schutz vor Web-Bedrohungen** zu schließen.
   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Schutz vor Web-Bedrohungen** zu schließen.

Einstellungen für die Aufgabe „Schnelle Untersuchung“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.
2. Wählen Sie in der Liste der lokalen Aufgaben die schnelle Untersuchung aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:
   - Doppelklicken Sie auf den Aufgabennamen.
   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf **Eigenschaften**.
3. Gehen Sie zum Abschnitt **Untersuchung**.
4. Passen Sie falls nötig die folgenden Einstellungen an:
   - Um eine der vordefinierten Sicherheitsstufen auszuwählen, verwenden Sie den Schieberegler im Abschnitt **Sicherheitsstufe**.
   - Um die Sicherheitseinstellungen manuell anzupassen, klicken Sie auf **Einstellungen** und gehen Sie im Fenster **Einstellungen: Untersuchung** wie folgt vor:
     a. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security untersuchen soll.
     b. Passen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** die Leistungseinstellungen der Untersuchung an.
     c. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien Kaspersky Endpoint Security untersuchen soll.
     d. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Erweiterte Einstellungen** Folgendes an: Verwendung der iSwift-Technologie und Protokollierung erkannter Objekte in der Anwendungsstatistik.
     e. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** die Verwendung der „Heuristischen Analyse“ an und wählen Sie aus, welche Schutzstufe für die „Heuristische Analyse“ verwendet werden soll.
     f. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Untersuchung** zu schließen.
   - Wählen Sie im Abschnitt **Aktion** aus, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.
   - Um einen Untersuchungsbereich anzugeben, klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen** und gehen Sie im folgenden Fenster **Untersuchungsbereich** wie folgt vor:
     - Wenn Sie möchten, dass Kaspersky Endpoint Security die Objekte in der Standardliste untersucht, aktivieren Sie das Kontrollkästchen neben dem entsprechenden Objekt.
     - Um mit Kaspersky Endpoint Security andere Dateien oder Ordner zu untersuchen, klicken Sie auf **Hinzufügen** und geben eine Datei, einen Ordner oder eine Maske für Datei- oder Ordnernamen an.
     - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Untersuchungsbereich** zu schließen.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Schnelle Untersuchung** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Schnelle Untersuchung** zu schließen.

Einstellungen für die Aufgabe „Vollständige Untersuchung“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.

2. Wählen Sie in der Liste der lokalen Aufgaben die Aufgabe „Vollständige Untersuchung“ aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:

   - Doppelklicken Sie auf den Aufgabennamen.

   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf **Eigenschaften**.

3. Gehen Sie zum Abschnitt **Untersuchung**.

4. Passen Sie falls nötig die folgenden Einstellungen an:

   - Um eine der vordefinierten Sicherheitsstufen auszuwählen, verwenden Sie den Schieberegler im Abschnitt **Sicherheitsstufe**.

   - Um die Sicherheitseinstellungen manuell anzupassen, klicken Sie auf **Einstellungen** und gehen Sie im Fenster **Einstellungen: Untersuchung** wie folgt vor:

     a. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security untersuchen soll.

     b. Passen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** die Leistungseinstellungen der Untersuchung an.

     c. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien Kaspersky Endpoint Security untersuchen soll.

     d. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Erweiterte Einstellungen** Folgendes an: Verwendung der iSwift-Technologie und Protokollierung erkannter Objekte in der Anwendungsstatistik.

     e. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** die Verwendung der „Heuristischen Analyse“ an und wählen Sie aus, welche Schutzstufe für die „Heuristische Analyse“ verwendet werden soll.

     f. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Untersuchung** zu schließen.

   - Wählen Sie im Abschnitt **Aktion** aus, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.

- Um einen Untersuchungsbereich anzugeben, klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen** und gehen Sie im folgenden Fenster **Untersuchungsbereich** wie folgt vor:

  - Wenn Sie möchten, dass Kaspersky Endpoint Security die Objekte in der Standardliste untersucht, aktivieren Sie das Kontrollkästchen neben dem entsprechenden Objekt.

  - Um mit Kaspersky Endpoint Security andere Dateien oder Ordner zu untersuchen, klicken Sie auf **Hinzufügen** und geben eine Datei, einen Ordner oder eine Maske für Datei- oder Ordnernamen an.

  - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Untersuchungsbereich** zu schließen.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Vollständige Untersuchung** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Vollständige Untersuchung** zu schließen.

Einstellungen für die Aufgabe „Benutzerdefinierte Untersuchung“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.

2. Wählen Sie in der Liste der lokalen Aufgaben die Aufgabe „Benutzerdefinierte Untersuchung“ aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:

   - Doppelklicken Sie auf den Aufgabennamen.

   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf **Eigenschaften**.

3. Gehen Sie zum Abschnitt **Untersuchung**.

4. Passen Sie falls nötig die folgenden Einstellungen an:

   - Um eine der vordefinierten Sicherheitsstufen auszuwählen, verwenden Sie den Schieberegler im Abschnitt **Sicherheitsstufe**.

   - Um die Sicherheitseinstellungen manuell anzupassen, klicken Sie auf **Einstellungen** und gehen Sie im Fenster **Einstellungen: Untersuchung** wie folgt vor:

     a. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** die Dateitypen aus, die Kaspersky Endpoint Security untersuchen soll.

     b. Passen Sie auf der Registerkarte **Allgemein** im Abschnitt **Optimierung** die Leistungseinstellungen der Untersuchung an.

     c. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Zusammengesetzte Dateien** aus, welche zusammengesetzten Dateien Kaspersky Endpoint Security untersuchen soll.

     d. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Erweiterte Einstellungen** Folgendes an: Verwendung der iSwift-Technologie und Protokollierung erkannter Objekte in der Anwendungsstatistik.

e. Passen Sie auf der Registerkarte **Erweitert** im Abschnitt **Heuristische Analyse** die Verwendung der „Heuristischen Analyse“ an und wählen Sie aus, welche Schutzstufe für die „Heuristische Analyse“ verwendet werden soll.

f. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Einstellungen: Untersuchung** zu schließen.

- Wählen Sie im Abschnitt **Aktion** aus, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.

- Um einen Untersuchungsbereich anzugeben, klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen** und gehen Sie im folgenden Fenster **Untersuchungsbereich** wie folgt vor:

  - Klicken Sie auf **Hinzufügen** und geben eine Datei, einen Ordner oder eine Namensmaske für eine Datei oder einen Ordner an.

  - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Untersuchungsbereich** zu schließen.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

   - Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Benutzerdefinierte Untersuchung** zu schließen.

   - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Benutzerdefinierte Untersuchung** zu schließen.

Einstellungen für die Aufgabe „Schutz vor Netzwerkbedrohungen“ verwalten

1. Öffnen Sie die Liste der lokalen Aufgaben für einen Client-Computer.

2. Wählen Sie in der Liste der lokalen Aufgaben die Aufgabe „Schutz vor Netzwerkbedrohungen“ aus und verwenden Sie eine der folgenden Methoden, um ihre Eigenschaften zu öffnen:

   - Doppelklicken Sie auf den Aufgabennamen.

   - Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf **Eigenschaften**.

3. Wählen Sie den Abschnitt **Schutz vor Netzwerkbedrohungen** aus.

4. Passen Sie falls nötig die folgenden Einstellungen an:

   - Aktivieren oder deaktivieren Sie den „Schutz vor Netzwerkbedrohungen“ auf dem Client-Computer.

   - Aktivieren oder deaktivieren Sie im Abschnitt **Einstellungen für den Schutz vor Netzwerkbedrohungen** das Kontrollkästchen **Angreifenden Computer sperren für <Wert> Min.** und geben Sie den Wert an.

   - Sie können zusätzlich die IP-Adressen von Computern angeben, deren Netzwerkaktivität nicht blockiert werden soll. Gehen Sie dazu wie folgt vor:

     a. Klicken Sie auf **Ausnahmen**.

     Das Fenster **Ausnahmen** wird geöffnet.

b. Klicken Sie auf **Hinzufügen**.

Das Fenster **IP-Adresse** wird geöffnet.

c. Geben Sie die IP-Adresse des Computers an, dessen Netzwerkaktivität nicht blockiert werden soll, und klicken Sie auf **OK**.

d. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Ausnahmen** zu schließen.

5. Verwenden Sie eine der folgenden Methoden, um die Änderungen zu speichern:

- Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne das Fenster **Eigenschaften: Schutz vor Netzwerkbedrohungen** zu schließen.
- Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster **Eigenschaften: Schutz vor Netzwerkbedrohungen** zu schließen.

Richtlinien erstellen und verwalten

Dieser Abschnitt enthält Informationen darüber, wie Sie Richtlinien für Kaspersky Endpoint Security erstellen und konfigurieren.

Eine Richtlinie legt die Einstellungen einer Anwendung fest und bestimmt, ob diese Anwendung auf Computern innerhalb einer Administrationsgruppe angepasst werden kann. Für jede Anwendung muss eine eigene Richtlinie erstellt werden. Sie können mehrere Richtlinien für die Anwendungen erstellen, die auf Computern unterschiedlicher Administrationsgruppen installiert sind. Allerdings kann jeweils nur eine Richtlinie auf eine bestimmte Anwendung in der Administrationsgruppe angewandt werden.

Hinweis: Wenn Sie eine Richtlinie erstellen oder anpassen, können Sie mithilfe der Schaltflächen und Änderungen von Einstellungsgruppen in den Richtlinien erlauben oder verbieten.

Mit benutzerdefinierten Aufgaben können Sie folgende Aktionen ausführen:

- Richtlinien erstellen.
- Richtlinien konfigurieren.
- Richtlinien aus einer Gruppe in eine andere kopieren oder entfernen.
- Richtlinien löschen.
- Status von Richtlinien ändern.
- Richtlinien in eine Datei exportieren.
- Richtlinien aus einer Datei importieren.

Ausführliche Informationen über die Richtlinien von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinie erstellen

Dieser Abschnitt enthält Anweisungen darüber, wie der Assistent für neue Richtlinien gestartet wird, wenn Sie eine Richtlinie erstellen möchten.

Richtlinie aus dem Ordner einer Administrationsgruppe erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus und klicken Sie auf **Neue Richtlinie**.

   Der Assistent für neue Richtlinien wird geöffnet.
6. Folgen Sie den Anweisungen des Assistenten für neue Richtlinien, um eine Richtlinie zu erstellen.

Richtlinie aus dem Richtlinien-Ordner erstellen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Richtlinien**.
4. Klicken Sie im Arbeitsbereich auf **Neue Richtlinie**.

   Der Assistent für neue Richtlinien wird geöffnet.
5. Folgen Sie den Anweisungen des Assistenten für neue Richtlinien, um eine Richtlinie zu erstellen.

Um zum nächsten Schritt des Assistenten zu gehen, klicken Sie auf **Weiter**. Um zum vorherigen Schritt des Assistenten zurückzukehren, klicken Sie auf ←. Um den Assistenten bei einem beliebigen Schritt abzubrechen, klicken Sie auf **Abbrechen**.

> **Hinweis:** Das Aussehen der Schaltflächen kann je nach Windows-Version unterschiedlich sein.

Schritt 1. Programm auswählen

Wählen Sie im Fenster **Anwendung für das Erstellen einer Gruppenrichtlinie auswählen** in der Anwendungsliste den Punkt **Kaspersky Endpoint Security for Mac (12.2)** aus.

Schritt 2. Namen der Richtlinie angeben

1. Geben Sie im Fenster **Name der Gruppenrichtlinie eingeben** im Feld **Name** den Namen der zu erstellenden Richtlinie ein. Folgende Zeichen sind in einem Namen nicht zulässig: “ * < : > ? \ |.

2. Aktivieren Sie das Kontrollkästchen **Richtlinieneinstellungen für die vorherige Version der Anwendung verwenden**, um die Einstellungen einer vorhandenen Richtlinie für Kaspersky Endpoint Security in eine neue Richtlinie zu importieren.

Schritt 3. Schutzeinstellungen angeben

Passen Sie im Fenster **Schutz** bei Bedarf die folgenden Einstellungen an:

- Konfigurieren Sie Schutzeinstellungen für das Betriebssystem auf dem Client-Computer.
- Passen Sie die vertrauenswürdige Zone an.

  Sie können eine Liste mit Objekten erstellen, die von Kaspersky Endpoint Security nicht untersucht oder überwacht werden.
- Passen Sie die vertrauenswürdigen Anwendungen an.

  Sie können eine Liste mit Anwendungen erstellen, deren Netzwerk- und Dateiaktivitäten nicht von Kaspersky Endpoint Security überwacht werden sollen.
- Wählen Sie die zu erkennenden Objekttypen aus.
- Legen Sie fest, ob der Start geplanter Aufgaben unterbunden werden soll, wenn der Computer im Akkubetrieb läuft.
- Maximale CPU-Last für Untersuchungen.

Schritt 4. Einstellungen für den „Schutz vor bedrohlichen Dateien“ anpassen

Führen Sie im Fenster **Schutz vor bedrohlichen Dateien** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie den „Schutz vor bedrohlichen Dateien“.

  Der „Schutz vor bedrohlichen Dateien“ ist standardmäßig aktiviert.
- Wählen Sie eine Sicherheitsstufe aus.

  Standardmäßig ist die von Kaspersky empfohlene Sicherheitsstufe ausgewählt.
- Passen Sie die Einstellungen für den „Schutz vor bedrohlichen Dateien“ an.
- Wählen Sie die Aktion aus, die nach dem Fund eines schädlichen Objekts ausgeführt werden soll.

Schritt 5. Einstellungen für den „Schutz vor Web-Bedrohungen“ anpassen

Führen Sie im Fenster **Schutz vor Web-Bedrohungen** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie den „Schutz vor Web-Bedrohungen“.

  Der „Schutz vor Web-Bedrohungen“ ist standardmäßig aktiviert.
- Wählen Sie eine Sicherheitsstufe aus.

  Standardmäßig ist die von Kaspersky empfohlene Sicherheitsstufe ausgewählt.

- Passen Sie die Einstellungen für den „Schutz vor Web-Bedrohungen“ an.
- Wählen Sie die Aktion, die nach Löschen eines schädlichen Objekts im Web-Datenverkehr ausgeführt werden soll.

Schritt 6. Einstellungen für den „Schutz vor Netzwerkbedrohungen“ anpassen

Führen Sie im Fenster **Schutz vor Netzwerkbedrohungen** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie den „Schutz vor Netzwerkbedrohungen“.

  Der „Schutz vor Netzwerkbedrohungen“ ist standardmäßig aktiviert.
- Passen Sie die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ an.
- Erstellen oder bearbeiten Sie eine Liste mit IP-Adressen von Remote-Computern, deren Netzwerkaktivität Kaspersky Endpoint Security nicht blockiert.

Schritt 7. Update-Einstellungen konfigurieren

Führen Sie im Fenster **Aktualisieren** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie das Update der Anwendungsmodule.
- Geben Sie die Update-Quellen an.

Schritt 8. KSN-Einstellungen konfigurieren

Gehen Sie im Fenster **Kaspersky Security Network** bei Bedarf wie folgt vor:

- Klicken Sie auf **KSN-Erklärung** und lesen Sie den vollständigen Text der Erklärung zu Kaspersky Security Network.
- Sehen Sie sich die Informationen über die KSN-Infrastruktur an, die von Kaspersky Security Center angeboten wird.
- Geben Sie an, ob Sie Kaspersky Security Network verwenden wollen.
- Aktivieren oder deaktivieren Sie den erweiterten KSN-Modus.
- Aktivieren oder deaktivieren Sie die Verwendung eines KSN-Proxys.
- Aktivieren oder deaktivieren Sie die Verwendung der Kaspersky-Server, wenn der KSN-Proxy nicht verfügbar ist.

> **Hinweis:** Die Verwendung von Kaspersky Security Network und eines KSN-Proxys auf Remote-Computern ist nur verfügbar, wenn der Administrationsserver von Kaspersky Security Center als Proxy-Server verwendet wird. Ausführliche Informationen über die Eigenschaften des Administrationsservers finden Sie in der Hilfe zu Kaspersky Security Center.

Wenn Kaspersky Security Center die „Global KSN“-Infrastruktur verwendet und Sie in den Richtlinieneinstellungen die Teilnahme an Kaspersky Security Network festlegen, sendet Kaspersky Endpoint Security von den Client-Computern, für welche die Richtlinie gilt, automatisch Statistiken an Kaspersky. Dadurch wird der Schutz dieser Computer verbessert.

Hinweis: Ohne Ihre ausdrückliche Zustimmung empfängt, verarbeitet oder speichert Kaspersky keine personenbezogenen Daten.

Daten, die an Kaspersky bereitgestellt werden, wenn Kaspersky Security Network in der Global KSN-Infrastruktur verwendet wird

Wenn das Kontrollkästchen **Ich stimme der Verwendung von Kaspersky Security Network zu** aktiviert ist und das Kontrollkästchen **Erweiterten KSN-Modus aktivieren** deaktiviert ist, stellt Kaspersky Endpoint Security die folgenden Daten an Kaspersky bereit:

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Vollversion der installierten Software;
  Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; einmalige Geräte-ID Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

Wenn die Kontrollkästchen **Ich stimme der Verwendung von Kaspersky Security Network zu** und **Erweiterten KSN-Modus aktivieren** aktiviert sind, stellt Kaspersky Endpoint Security die folgenden Daten an Kaspersky bereit:

- Informationen über die Version des Betriebssystems (OS) und die auf dem Computer installierten Service Packs, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems, Parameter des Funktionsmodus des Betriebssystems; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Windows Service Packs; Datum und Uhrzeit des Betriebssystemstarts; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Verhaltensanalyse-Subsystem; Anzahl der verzögerten Aktionsereignisse des Betriebssystems des aktuellen Typs; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Subsystem für den proaktiven Schutz; Anzahl der verarbeiteten Aktionsereignisse des Betriebssystems; Anzahl der verarbeiteten synchronen Aktionsereignisse des Betriebssystems; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems des aktuellen Typs; Verarbeitungsverzögerungszeit des Ereignisses über die Betriebssystemaktion im Subsystem für die persistente Ereignisspeicherung; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems; Anzahl der wartenden synchronen Aktionsereignisse des Betriebssystems; Datum und Uhrzeit des empfangenen Ereignisses über eine Aktion im Betriebssystem.

- Informationen über den fehlgeschlagenen letzten Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.

- Informationen über die installierte Anwendung des Rechtsinhabers und den Status des Antiviren-Schutzes: ID der Software-Installation (PCID) Version des Software-Datenbankeintrags; eindeutige ID der Instanz der Anwendungsinstallation auf dem Computer, Anwendungstyp, Anwendungstyp-ID, die Vollversion der installierten Anwendung, ID der Version der Anwendungseinstellungen, ID des Computertyps, eindeutige ID des Computers, auf dem die Anwendung installiert ist, eindeutige Benutzer-ID beim Dienst des Rechteinhabers, lokale Sprache und Betriebszustand, Version der installierten Softwarekomponenten und ihr Betriebszustand, Version des verwendeten Protokolls zur Verbindungsherstellung zum Dienst des Rechteinhabers; Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Anzahl der Update-Anwendungs-Zyklen für die Antiviren-Datenbanken; Zeitpunkt (Datum und Uhrzeit), an dem die Antiviren-Datenbanken zuletzt aktualisiert und angewendet wurden; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version der Software-Komponente; ID des Software-Updates; Typ der installierten Software; Startdatum und -uhrzeit vom Aktivitätsmonitor; Installationsdatum und -uhrzeit der Software; Wahrscheinlichkeit der Übermittlung von Statistiken durch den Aktivitätsmonitor; Code des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Datenbank-Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; maximal zulässige Zeit für die Verarbeitung eines Ereignisses durch den Aktivitätsmonitor; Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Gesamtzahl der Ereignisse, die länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert haben.

- Informationen über alle verarbeiteten Objekte und Vorgänge: Verdikt der Software für das verarbeitete Objekt; Verzeichniscode; Größe des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Anzahl der erkannten Software im Kontext des „Aktivitätsmonitors"; Zeitpunkt (Datum und Uhrzeit), zu dem der „Aktivitätsmonitor" die Software erkannt hat; Erkennungscharakteristiken; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Grund, aus dem der „Aktivitätsmonitor" die Software erkannt hat; Prüfsumme (MD5) des verarbeiteten Objekts; Ergebnis der Modul-Integritätsprüfung; Name des verarbeiteten Objekts; Typ des ausgelösten Eintrags der Antiviren-Datenbanken der Software; Speicherpfad des verarbeiteten Objekts; Name des untersuchten Objekts; Datum und Uhrzeit der Untersuchung; URL-Adresse und Referenzadresse, von denen es heruntergeladen wurde; Größe und Pfade der untersuchten Dateien; Zeichen des Archivs; Datum und Uhrzeit der Dateierstellung; Name, Größe und Prüfsummen (MD5, SHA2-256) des Packers (falls die Datei gepackt wurde); Entropie der Datei; Typ der Datei; Code des Dateityps; Zeichen, ID und Format der ausführbaren Datei; Prüfsumme des Objekts (MD5, SHA2-256); Typ und Wert der zusätzlichen Prüfsumme des Objekts; Daten über die digitale Signatur des Objekts (Zertifikat): Daten über den Herausgeber des Zertifikats, Anzahl der Starts des Objekts seit der letzten Übermittlung von Statistiken, ID der Überprüfungsaufgabe der Anwendung, Mittel zum Erhalt von Informationen über den Ruf des Objekts, Wert des Zielfilters, technische Parameter der anwendbaren Erkennungstechnologien; Speicherpfad des verarbeiteten Objekts; Verzeichniscode.

- Für ausführbare Dateien: Entropie der Dateiabschnitte, Kennzeichen der Reputations-Überprüfung oder Kennzeichen der Dateisignatur, Name, Typ, ID-Typ, Prüfsumme (MD5) und Größe der Anwendung, die vom zu validierenden Objekt geladen wurde, Anwendungspfad und Vorlagenpfade, Attribut, das das Vorhandensein in der Autostart-Liste angibt, Datum des Eintrags, Liste mit Attributen, Name des Packers, Informationen über die digitale Signatur der Anwendung: Herausgeberzertifikat, Name der hochgeladenen Datei im MIME-Format, Datum und Uhrzeit der Dateierstellung.

- Informationen über die gestarteten Anwendungen und deren Module: Prüfsummen (MD5, SHA2-256) von ausgeführten Dateien, Größe, Attribute, Erstellungsdatum, Name des Packers (falls die Datei gepackt wurde), Dateinamen, Informationen über die im System ausgeführten Prozesse (Prozess-ID (PID), Prozessname, Informationen über das Benutzerkonto, aus dem der Prozess gestartet wurde, Anwendung und Befehl, mit dem der Prozess gestartet wurde, vollständiger Pfad der Dateien des Prozesses sowie auszuführende Befehlszeile, Beschreibung der Anwendung, zu dem der Prozess gehört (Name der Anwendung und Informationen über den Herausgeber) sowie die verwendeten digitalen Zertifikate und Informationen, die zur Überprüfung ihrer Authentizität dienen, oder Informationen über das Fehlen einer digitalen Signatur einer Datei) und Informationen über die in die Prozesse geladenen Module: deren Namen, Größen, Typen, Erstellungsdaten, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfade, Header-Informationen der PE-Datei, Namen der Packer (falls die Datei gepackt wurde), Informationen über die Verfügbarkeit und Gültigkeit dieser Statistiken, ID des Modus zur Erstellung von zu sendenden Statistiken.

- Falls Bedrohungen oder Schwachstellen erkannt werden, werden zusätzlich zu den Informationen über das erkannte Objekt auch die folgenden Informationen bereitgestellt: ID, Version und Typ des Eintrags in der Antiviren-Datenbank, Name der Bedrohung, basierend auf der Klassifikation von Kaspersky, Datum und Uhrzeit der letzten Aktualisierung der Antiviren-Datenbank, Name der ausführbaren Datei, Prüfsumme (MD5) der Anwendungsdatei, welche die Webadresse, unter der die Bedrohung erkannt wurde, angefordert hat, IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, ID der Schwachstelle und ihre Gefahrenstufe, URL und Referenz der Webseite, auf der die Schwachstelle gefunden wurde.

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt.

- Informationen über einen Netzwerkangriff: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.

- Informationen zu Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, aus der der Prozess gestartet wurde, der den Port geöffnet hat, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Verbindungsports, Verbindungsstatus, Zeitstempel für das Öffnen des Ports.

- URL- und IP-Adresse der Webseite, auf der schädliche oder verdächtige Inhalte erkannt wurden, Name, Größe und Prüfsumme der Datei, die die URL anforderte, Kennung, Priorität und Grad der Regel, die für die Entscheidung verwendet wurde, Ziel des Angriffs.

- Informationen über Updates der installierten App- und Antiviren-Datenbanken: Bearbeitungsstand der Update-Aufgabe, Art des Fehlers, der möglicherweise während des Update-Vorgangs aufgetreten ist, Anzahl der fehlgeschlagenen Updates, ID der Anwendungskomponente, die die Updates ausführt.

- Informationen über die Nutzung von Kaspersky Security Network (KSN): KSN-ID, Anwendungs-ID, vollständige Version der Anwendung, anonymisierte IP-Adresse des Benutzergerätes, Indikatoren für die Qualität der Ausführung von KSN-Anfragen, Indikatoren für die Qualität der Verarbeitung von KSN-Paketen, Indikatoren für die Anzahl der KSN-Anfragen und Informationen über die Arten von KSN-Anfragen, Datum und Uhrzeit für den Beginn des Sendevorgangs von Statistiken, Datum und Uhrzeit für das Ende des Sendevorgangs von Statistiken, Informationen über die Aktualisierung der KSN-Konfiguration: ID der aktiven Konfiguration, ID der empfangenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen zu Systemprotokoll-Ereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.

- Informationen zur Bestimmung der Reputation von Dateien und URL-Adressen: URL-Adresse, unter der die Reputation angefordert wird, und Referrer, Protokolltyp der Verbindung, interne ID des Anwendungstyps, Nummer des verwendeten Ports, Benutzer-ID, Prüfsumme der untersuchten Datei (MD5), Typ der erkannten Bedrohung, Informationen über den Datensatz, der zum Erkennen der Bedrohung verwendet wurde (ID des Datensatzes für die Antiviren-Datenbanken, Zeitstempel und Typ des Datensatzes); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

- Daten zur geografischen Verteilung der Anwendung: Datum der Anwendungsinstallation und -aktivierung, ID des Partners, der die Lizenz für die Anwendungsaktivierung bereitstellt, Anwendungs-ID, Lokalisierungs-ID der Anwendungssprache, Lizenz-Seriennummer für die Anwendungsaktivierung, Merkmal für die KSN-Teilnahme.

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Informationen über die auf dem Computer installierte Hardware: Typ, Name, Modellname, Firmware-Version, Parameter der integrierten und angeschlossenen Geräte.

- Informationen über das Gerät: Geräte-ID.

- Informationen zum Betrieb der Komponente Web-Kontrolle:
  Komponentenversion, Kategorisierungsgrund, zusätzliche Informationen zum Kategorisierungsgrund, kategorisierte URL, Host-IP-Adresse des blockierten/kategorisierten Objekts.

Wenn Kaspersky Security Center die „Private KSN"-Infrastruktur verwendet und Sie in den Richtlinieneinstellungen die Teilnahme an Kaspersky Security Network festlegen, sendet Kaspersky Endpoint Security keine Statistiken von den Client-Computern, für welche die Richtlinie gilt.

Wenn eine Richtlinie gelöscht oder deaktiviert wird, werden die KSN-Einstellungen auf dem Client-Computer auf die ursprünglichen Werte zurückgesetzt.

Schritt 9. Einstellungen für die Interaktion mit dem Benutzer anpassen

Passen Sie im Fenster **Interaktion mit dem Benutzer** bei Bedarf die Einstellungen für die Interaktion mit dem Benutzer auf dem Client-Computer an.

Schritt 10. Einstellungen für die Netzwerkverbindung anpassen

Gehen Sie im Fenster **Netzwerk** bei Bedarf wie folgt vor:

- Verbindung mit dem Proxy-Server anpassen.
- Aktivieren oder deaktivieren Sie die Untersuchung des eingehenden und ausgehenden HTTPS-Datenverkehrs.
- Wählen Sie den Zertifikatspeicher für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Mozilla Firefox-Browser aus.
- Verwalten Sie die Liste der vertrauenswürdigen Stammzertifikate.
- Passen Sie die überwachten Ports an.

  Sie können eine Liste der Ports erstellen, die von Kaspersky Endpoint Security überwacht werden sollen.

Schritt 11. Einstellungen für „Berichte und Backup“ anpassen

Gehen Sie im Fenster **Berichte und Backup** bei Bedarf wie folgt vor:

- Passen Sie Einstellungen zum Generieren und Speichern von Berichten an.
- Passen Sie die Einstellungen für die Speicherung von Objekten im Backup an.

Schritt 12. FileVault-Volume-Verschlüsselung anpassen

Gehen Sie im Fenster **FileVault-Volume-Verschlüsselung** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Verwaltung der FileVault-Volume-Verschlüsselung für das Startvolume des Benutzers.

  Die FileVault-Volume-Verschlüsselung ist standardmäßig deaktiviert.

- Wählen Sie die Option **Volume verschlüsseln** aus, wenn das Startvolume des Benutzers beim Anwenden der Richtlinie auf einen Client-Computer verschlüsselt werden soll.

Ist das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** deaktiviert, so können Benutzer mit Administratorrechten ihre Mac-Startvolumes aus den Systemeinstellungen verschlüsseln und entschlüsseln.

Sind das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** und die Option **Volume verschlüsseln** ausgewählt, so können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen entschlüsseln.

Sind das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** und die Option **Volume entschlüsseln** ausgewählt, so können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen verschlüsseln.

Schritt 13. Web-Kontrolle anpassen

Führen Sie im Fenster **Web-Kontrolle** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie die Web-Kontrolle.

  Hinweis: Wenn Sie die „Web-Kontrolle“ aktivieren, um den Zugriff auf gefährliche Webressourcen zu blockieren, zeigt Kaspersky Endpoint Security im „Schutz-Center“ auf dem Remote-Computer die Benachrichtigung **Die Web-Kontrolle ist aktiviert** an.
  Kaspersky Endpoint Security zeigt Benachrichtigungen an, wenn der Benutzer auf dem Remote-Computer auf Webressourcen zugreift, die durch die „Web-Kontrolle“ blockiert werden, vorausgesetzt das Kontrollkästchen **Sichere Verbindungen (HTTPS) untersuchen** im Fenster **Netzwerk** des Assistenten für neue Richtlinien ist aktiviert.

- Fügen Sie durch Klick auf **Hinzufügen** eine neue Regel für die „Web-Kontrolle“ hinzu.

  Sie können einen Regelnamen eingeben; festlegen, ob die Regel aktiv sein soll; einen Bereich für die Regel angeben, indem Sie eine Liste mit speziellen Webadressen erstellen oder Website-Kategorien auswählen; und eine Aktion auswählen, die Kaspersky Endpoint Security ausführen soll, wenn ein Benutzer auf eine Website zugreift, die in dieser Regel enthalten ist.

- Bearbeiten, löschen oder organisieren Sie die erstellten Regeln in der Liste.

  Die Reihenfolge, in der die Regeln angeordnet sind, entspricht der Priorität, nach welcher die Regeln durch Kaspersky Endpoint Security angewendet werden.

Schritt 14. Managed Detection and Response konfigurieren

Gehen Sie im Fenster **Managed Detection and Response** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie Managed Detection and Response.

  Standardmäßig ist Managed Detection and Response deaktiviert.

- Importieren oder löschen Sie eine Konfigurationsdatei, um die Komponente Managed Detection and Response auf verwalteten Geräten zu aktivieren.

Wenn das Kontrollkästchen für **Managed Detection and Response** ausgewählt und die MDR-Konfigurationsdatei importiert wird, ist die Komponente Managed Detection and Response aktiv und interagiert mit dem Dienst Kaspersky Managed Detection and Response. Dieser Dienst erkennt fortwährend Sicherheitsbedrohungen, die auf Ihr Unternehmen abzielen, und eliminiert sie.

Schritt 15. Endpoint Detection and Response (KATA) konfigurieren

Gehen Sie im Fenster **Endpoint Detection and Response (KATA)** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie Endpoint Detection and Response (KATA).

  Endpoint Detection and Response (KATA) ist standardmäßig deaktiviert.

- Konfigurieren Sie die Einstellungen für die Serververbindung und fügen Sie ein TLS-Zertifikat hinzu.

- Fügen Sie einen KATA-Server hinzu.

Wenn das Kontrollkästchen **Endpoint Detection and Response (KATA)** ist und ein TLS-Zertifikat und ein KATA-Server hinzugefügt wurden, ist die Komponente Endpoint Detection and Response (KATA) aktiv und interagiert mit der Lösung Kaspersky Anti Targeted Attack Platform. Diese Lösung kann komplexe Bedrohungen sofort erkennen. Dazu zählen beispielsweise gezielte Angriffe, hochentwickelte, hartnäckige Bedrohungen und Zero-Day-Angriffe.

Schritt 16. Untersuchung externer Datenträger konfigurieren

Nehmen Sie im Fenster **Untersuchung externer Datenträger** die folgenden Einstellungen vor:

- Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein externer Datenträger angeschlossen wird.
- Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein schädliches Objekt erkannt wurde.

Schritt 17. Verhaltenserkennung konfigurieren

Führen Sie im Fenster **Verhaltensanalyse** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie die Verhaltensanalyse.
  Die Verhaltensanalyse ist standardmäßig aktiviert.
- Wählen Sie aus, welche Aktion ausgeführt werden soll, wenn Malware-Aktivitäten erkannt werden.
- Aktivieren oder deaktivieren Sie den Schutz vor der externen Verschlüsselung freigegebener Ordner.
  - Wählen Sie aus, welche Aktion ausgeführt werden soll, wenn Malware-Aktivitäten erkannt werden.

Schritt 18. Schutz vor E-Mail-Bedrohungen konfigurieren

Gehen Sie im Fenster **Schutz vor E-Mail-Bedrohungen** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie den Schutz vor E-Mail-Bedrohungen.
  Der Schutz vor E-Mail-Bedrohungen ist standardmäßig aktiviert.
- Wählen Sie die Aktion aus, die nach dem Fund eines schädlichen Objekts ausgeführt werden soll.
- Konfigurieren Sie die Einstellungen für den Schutz vor E-Mail-Bedrohungen.

Schritt 19. Exploit-Prävention konfigurieren

Gehen Sie im Fenster **Exploit-Prävention** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Exploit-Prävention.
  Die Exploit-Prävention ist standardmäßig aktiviert.
- Wählen Sie die Aktion aus, die beim Fund eines Exploits ausgeführt werden soll.

Schritt 20. Rollback von schädlichen Aktionen konfigurieren

Gehen Sie im Fenster **Rollback von schädlichen Aktionen** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie das Rollback von schädlichen Aktionen.
  Das Rollback von schädlichen Aktionen ist standardmäßig aktiviert.

Schritt 21. Gerätekontrolle konfigurieren

Gehen Sie im Fenster **Gerätekontrolle** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Gerätekontrolle.
  Die Gerätekontrolle ist standardmäßig aktiviert.
- Konfigurieren Sie die Einstellungen der Gerätekontrolle.

Schritt 22. Firewall konfigurieren

Gehen Sie im Fenster **Firewall** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Firewall.

  Die Firewall ist standardmäßig aktiviert.

- Konfigurieren Sie die Einstellungen der Firewall.

Schritt 23. Administrationsgruppe festlegen, auf welche die Richtlinie angewendet wird

Klicken Sie im Fenster **Zielgruppe** auf **Durchsuchen**, um eine Administrationsgruppe auszuwählen, auf welche Sie die Richtlinie anwenden möchten.

Schritt 24. Richtlinienstatus auswählen und Erstellung einer Richtlinie abschließen

Führen Sie im Fenster **Erstellen einer neuen Gruppenrichtlinie für die Anwendung** die folgenden Schritte durch:

1. Wählen Sie den Status aus, der der Richtlinie zugewiesen wird:

   - *Aktive Richtlinie* – Die Richtlinie wird für die ausgewählte Administrationsgruppe verwendet.
   - *Inaktive Richtlinie* – Die Richtlinie wird nicht verwendet.
   - *Mobile Richtlinie* – Die Richtlinie wird für die ausgewählte Administrationsgruppe verwendet, wenn keine Verbindung zum Unternehmensnetzwerk besteht.

   Hinweis: Für eine Anwendung in der Administrationsgruppe können Sie mehrere Richtlinien erstellen, von denen allerdings nur eine aktiviert sein kann.

   Ausführliche Informationen über die Statusvarianten für Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

2. Wenn Sie die Richtlinie nach Erstellung überprüfen möchten, aktivieren Sie das Kontrollkästchen **Richtlinieneigenschaften sofort nach ihrer Erstellung anzeigen**.

3. Klicken Sie auf **Fertig**, um den Assistenten für neue Richtlinien zu schließen.

   Die neue Richtlinie erscheint auf der Registerkarte **Richtlinien** im Arbeitsbereich der entsprechenden Administrationsgruppe. Die Richtlinie wird für die Client-Computer übernommen, wenn die Client-Computer zum ersten Mal mit dem Administrationsserver synchronisiert werden.

Sie können die Einstellungen der neuen Richtlinie ändern. Außerdem können Sie können Sie mithilfe der Schaltflächen und das Ändern einzelner Einstellungsabschnitte auf einem Client-Computer verbieten oder erlauben. Die Schaltfläche neben einer Gruppe von Einstellungen bedeutet, dass der Benutzer des Client-Computers diese Einstellungen auf seinem Computer nicht ändern kann. Die Schaltfläche neben einer Gruppe von Einstellungen bedeutet, dass der Benutzer des Client-Computers diese Einstellungen auf seinem Computer ändern kann.

Liste der Richtlinien anzeigen

Sie können eine unbeschränkte Anzahl verschiedener Richtlinien für Anwendungen erstellen, die auf Computern in jeder Administrationsgruppe installiert wurden. Es kann aber jeweils nur eine Richtlinie auf jede Anwendung in der Administrationsgruppe angewandt werden.

Richtlinienliste einer Administrationsgruppe anzeigen

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

   Die Liste der Richtlinien wird angezeigt.

Richtlinieneinstellungen konfigurieren

Sie können die erstellte Richtlinie in Kaspersky Security Center ändern und Sie können festlegen, dass die Einstellungen in den Richtlinien untergeordneter Gruppen und in den Aufgabeneinstellungen nicht geändert werden dürfen.

Die Einstellungen der Richtlinie für Kaspersky Endpoint Security umfassen Anwendungseinstellungen und Aufgabeneinstellungen.

Richtlinieneinstellungen konfigurieren

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
5. Rechtsklicken Sie auf die Richtlinie, die Sie anpassen möchten, und wählen Sie **Eigenschaften**.
6. Passen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** die Richtlinieneinstellungen an:

   - Im Abschnitt **Basisschutz**

     Passen Sie die folgenden Einstellungen für den „Schutz vor bedrohlichen Dateien“ an.

     - Aktivieren oder deaktivieren Sie den „Schutz vor bedrohlichen Dateien“.
     - Wählen Sie eine der vordefinierten Sicherheitsstufen aus oder passen Sie die Sicherheitseinstellungen manuell an.
     - Wählen Sie die Aktion aus, die nach dem Fund eines schädlichen Objekts ausgeführt werden soll.

     Passen Sie die folgenden Einstellungen für den „Schutz vor Web-Bedrohungen“ an.

     - Aktivieren oder deaktivieren Sie den „Schutz vor Web-Bedrohungen“.
     - Wählen Sie eine der vordefinierten Sicherheitsstufen aus oder passen Sie die Sicherheitseinstellungen manuell an.

- Aktivieren oder deaktivieren Sie die Untersuchung von Webadressen mithilfe der Datenbank für bösartige Webadressen.
- Passen Sie die Anti-Phishing-Einstellungen an.
- Fügen Sie die vertrauenswürdigen Adressen hinzu, deren Datenverkehr nicht durch den „Schutz vor Web-Bedrohungen“ untersucht werden soll.
- Wählen Sie die Aktion, die nach Löschen eines schädlichen Objekts im Web-Datenverkehr ausgeführt werden soll.

Konfigurieren Sie die folgenden Einstellungen für den Schutz vor E-Mail-Bedrohungen

- Aktivieren oder deaktivieren Sie den Schutz vor E-Mail-Bedrohungen.
- Wählen Sie die Aktion aus, die nach dem Fund eines schädlichen Objekts ausgeführt werden soll.
- Konfigurieren Sie die Einstellungen für den Schutz vor E-Mail-Bedrohungen.

Passen Sie die folgenden Einstellungen für den „Schutz vor Netzwerkbedrohungen“ an.

- Aktivieren oder deaktivieren Sie den „Schutz vor Netzwerkbedrohungen“.
- Passen Sie die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ an.
- Geben Sie die IP-Adressen der Computer an, deren Netzwerkaktivität nicht blockiert werden soll.

Konfigurieren Sie die folgenden Einstellungen der Firewall

- Aktivieren oder deaktivieren Sie die Firewall.
- Konfigurieren Sie die Einstellungen der Firewall.

- Im Abschnitt **Erweiterter Schutz**

  Passen Sie die folgenden KSN-Einstellungen an.

  - Lesen Sie den vollständigen Text der Erklärung zu Kaspersky Security Network. Klicken Sie dazu auf KSN-Erklärung.
  - Geben Sie an, ob Sie Kaspersky Security Network verwenden wollen.
  - Aktivieren oder deaktivieren Sie den erweiterten KSN-Modus.
  - Aktivieren oder deaktivieren Sie den Cloud-Modus.
  - Aktivieren oder deaktivieren Sie die Verwendung eines KSN-Proxys.
  - Aktivieren oder deaktivieren Sie die Verwendung der Kaspersky-Server, wenn der KSN-Proxy nicht verfügbar ist.

  Hinweis: Die Verwendung von Kaspersky Security Network und eines KSN-Proxys auf Remote-Computern ist nur verfügbar, wenn der Administrationsserver von Kaspersky Security Center als Proxy-Server verwendet wird. Ausführliche Informationen über die Eigenschaften des Administrationsservers finden Sie in der Hilfe zu Kaspersky Security Center.

Konfigurieren Sie die folgenden Einstellungen für die Verhaltensanalyse

- Aktivieren oder deaktivieren Sie die Verhaltensanalyse.

  Die Verhaltensanalyse ist standardmäßig aktiviert.

- Wählen Sie aus, welche Aktion ausgeführt werden soll, wenn Malware-Aktivitäten erkannt werden.

Konfigurieren Sie die folgenden Einstellungen der Exploit-Prävention

- Aktivieren oder deaktivieren Sie die Exploit-Prävention.
- Wählen Sie die Aktion aus, die beim Fund eines Exploits ausgeführt werden soll.

Konfigurieren Sie die folgenden Einstellungen für das Rollback von schädlichen Aktionen

Aktivieren oder deaktivieren Sie das Rollback von schädlichen Aktionen.

- Im Abschnitt **Sicherheitskontrolle**

  Konfigurieren Sie die folgenden Einstellungen der Gerätekontrolle

  - Aktivieren oder deaktivieren Sie die Gerätekontrolle.
  - Konfigurieren Sie die Einstellungen der Gerätekontrolle.

  Passen Sie die folgenden Einstellungen für die Web-Kontrolle an.

  - Aktivieren oder deaktivieren Sie die Web-Kontrolle.
  - Fügen Sie durch Klick auf **Hinzufügen** eine neue Regel für die „Web-Kontrolle“ hinzu.
  - Bearbeiten, löschen oder organisieren Sie die erstellten Regeln in der Liste.

- Im Abschnitt **Datenverschlüsselung**

  Passen Sie die folgenden Einstellungen für die FileVault-Volume-Verschlüsselung an.

  - Aktivieren oder deaktivieren Sie die Verwaltung für FileVault-Volume-Verschlüsselung auf den Client-Computern.
  - Verschlüsseln oder entschlüsseln Sie das Startvolume auf den Client-Computern.

    Ist das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** deaktiviert, so können Benutzer mit Administratorrechten ihre Mac-Startvolumes aus den Systemeinstellungen verschlüsseln und entschlüsseln.

    Sind das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** und die Option **Volume verschlüsseln** ausgewählt, so können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen entschlüsseln.

    Sind das Kontrollkästchen **Verwaltung für die FileVault-Volume-Verschlüsselung aktivieren** und die Option **Volume entschlüsseln** ausgewählt, so können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen verschlüsseln.

- Konfigurieren Sie im Abschnitt **Detection and Response**

die folgenden Einstellungen für Managed Detection and Response.

- Aktivieren oder deaktivieren Sie Managed Detection and Response.
- Importieren oder löschen Sie eine Konfigurationsdatei, die zum Aktivieren der Komponente Managed Detection and Response auf verwalteten Geräten verwendet wird.

Konfigurieren Sie die folgenden Einstellungen für Endpoint Detection and Response (KATA)

- Aktivieren oder deaktivieren Sie Endpoint Detection and Response (KATA).
- Konfigurieren Sie die Einstellungen für die Serververbindung und fügen Sie ein TLS-Zertifikat hinzu.
- Fügen Sie einen KATA-Server hinzu.

- Im Abschnitt **Lokale Aufgaben**

  Passen Sie die folgenden Einstellungen der Untersuchung externer Datenträger an

  - Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein externer Datenträger angeschlossen wird.
  - Die Aktion, die Kaspersky Endpoint Security ausführt, sobald ein schädliches Objekt erkannt wurde.

- Im Abschnitt **Aktualisieren**

  Passen Sie die folgenden Update-Einstellungen an.

  - Aktivieren oder deaktivieren Sie das Update der Anwendungsmodule.
  - Geben Sie die Update-Quellen an.

- Im Abschnitt **Weitere Einstellungen**

  Passen Sie die folgenden Schutzeinstellungen an.

  - Aktivieren oder deaktivieren Sie den Echtzeitschutz für den Client-Computer.
  - Legen Sie fest, ob Kaspersky Endpoint Security beim Hochfahren des Client-Computers gestartet werden soll oder nicht.
  - Passen Sie die vertrauenswürdige Zone an.
  - Passen Sie die vertrauenswürdigen Anwendungen an.
  - Wählen Sie die zu erkennenden Objekttypen aus.
  - Legen Sie fest, ob der Start geplanter Aufgaben unterbunden werden soll, wenn der Computer im Akkubetrieb läuft.

  Passen Sie die folgenden Netzwerkeinstellungen an.

  - Legen Sie fest, ob ein Proxy-Server verwendet werden soll.
  - Geben Sie die Adresse des Proxy-Servers an.
  - Legen Sie fest, ob der Proxy-Server für lokale Adressen verwendet werden soll.

- Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung auf dem Proxy-Server an.
- Aktivieren oder deaktivieren Sie die Untersuchung des eingehenden und ausgehenden HTTPS-Datenverkehrs.
- Wählen Sie den Zertifikatspeicher für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Mozilla Firefox-Browser aus.
- Passen Sie die überwachten Ports an.

Passen Sie die folgenden Einstellungen für „Berichte und Backup“ an.

- Legen Sie fest, ob nicht-kritische Ereignisse protokolliert werden sollen.
- Legen Sie fest, ob nur aktuelle Ereignisse gespeichert werden sollen.
- Legen Sie fest, ob Ereignisse nach einem bestimmten Zeitraum gelöscht werden sollen.
- Geben Sie die Speicherdauer für Ereignissen an.
- Legen Sie fest, ob Objekte nach dem angegebenen Zeitraum aus dem Backup gelöscht werden sollen.
- Geben Sie die Speicherdauer für Objekte im Backup an.

Passen Sie die folgenden Einstellungen für die Interaktion mit dem Benutzer an.

- Aktivieren oder deaktivieren Sie die Ereignisbenachrichtigungen.
- Legen Sie fest, auf welche Weise Kaspersky Endpoint Security den Benutzer über Ereignisse benachrichtigen soll.
- Legen Sie fest, ob das Symbol von Kaspersky Endpoint Security in der Menüleiste angezeigt werden soll.
- Legen Sie fest, ob ein Benutzer das Hauptfenster von Kaspersky Endpoint Security öffnen kann und die Anwendungsoberfläche auf dem Client-Computer verwenden darf.
- Legen Sie fest, ob der Befehl **Beenden** im Kontextmenü des Symbols von Kaspersky Endpoint Security auf dem Client-Computer verfügbar sein soll.
- Wählen Sie die Sprache aus, die zum Anzeigen von Kaspersky Security Center-Ereignissen verwendet werden soll.
- Passen Sie die Einstellungen für Kaspersky Endpoint Security an, die Benutzern auf einem Client-Computer zur Verfügung stehen sollen.
- Konfigurieren Sie den Kennwortschutz, um unerwünschte Aktionen auf den Benutzergeräten einzuschränken.

7. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu schließen.

Richtlinienstatus ändern

Der Richtlinienstatus gibt den Betriebszustand einer Richtlinie an. Als Varianten für den Richtlinienstatus sind möglich: aktiv, mobil oder inaktiv. Sie können den Richtlinienstatus in den Richtlinieneinstellungen ändern.

Richtlinienstatus ändern

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
6. Klicken Sie mit der rechten Maustaste auf die Richtlinie, deren Status Sie ändern möchten, und wählen Sie aus dem Kontextmenü **Eigenschaften** aus.
7. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Allgemein** aus.
8. Wählen Sie im Fenster **Richtlinienstatus** eine der folgenden Varianten für den Status der Richtlinie aus:
   - **Aktive Richtlinie**. Die Richtlinie wird immer auf die ausgewählte Administrationsgruppe angewendet.
   - **Mobile Richtlinie**. Die Richtlinie wird für die ausgewählte Administrationsgruppe verwendet, wenn keine Verbindung zum Unternehmensnetzwerk besteht.
   - **Inaktive Richtlinie**. Die Richtlinie wird nicht auf die ausgewählte Administrationsgruppe angewendet.
9. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern und das Fenster **Eigenschaften: <Name der Richtlinie>** zu schließen.

Richtlinie in eine KLP-Datei exportieren

Sie können eine benutzerdefinierte Richtlinie in eine Datei exportieren, um die Richtlinie auf einem anderen Administrationsserver zu verwenden.

Richtlinie in eine KLP-Datei exportieren

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

6. Klicken Sie mit der rechten Maustaste im Kontextmenü auf die anzuzeigende Richtlinie und wählen Sie **Exportieren**.

   Das Fenster **Speichern unter** wird geöffnet.

7. Wählen Sie den Ordner aus, in dem Sie die KLP-Datei für die Richtlinie speichern möchten.

8. Geben Sie einen Dateinamen an.

9. Klicken Sie auf **Speichern**, um die Datei im ausgewählten Ordner zu speichern.

Richtlinie aus einer KLP-Datei importieren

Sie können eine vorhandene Richtlinie mit vordefinierten Einstellungen aus einer Datei importieren.

Richtlinie aus einer KLP-Datei importieren

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.

2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.

3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.

4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.

5. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

6. Verwenden Sie eine der folgenden Methoden, um das Auswahlfenster für eine Datei zu öffnen:

   - Durch Klicken auf die Schaltfläche **Richtlinie aus Datei importieren**.
   - Durch Rechtsklick in einen leeren Bereich im Arbeitsbereich, um das Kontextmenü zu öffnen, und das Menü **Importieren** zu wählen.

7. Wählen Sie eine KLP-Datei mit einer Richtlinie aus und klicken Sie auf **Öffnen**.

Die importierte Richtlinie wird der Liste der Richtlinien im Arbeitsbereich hinzugefügt.

Richtlinienprofile erstellen und verwalten

Als Richtlinienprofil wird ein Satz variabler Einstellungen für eine Richtlinie bezeichnet, die auf einem Client-Computer aktiviert werden, wenn bestimmte Bedingungen erfüllt werden. Durch die Aktivierung eines Profils werden die Richtlinieneinstellungen modifiziert, die auf dem Gerät gelten, wenn das Richtlinienprofil aktiviert wird.

Richtlinienprofil erstellen

1. Wählen Sie in der Baumstruktur die Administrationsgruppe aus, für die Sie ein Richtlinienprofil erstellen möchten.

2. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

3. Führen Sie zum Öffnen der Eigenschaften der Richtlinie, für die Sie ein Profil erstellen möchten, eine der folgenden Aktionen aus:

   - Doppelklick auf den Namen der Richtlinie.
   - Klicken Sie mit der rechten Maustaste auf den Richtliniennamen, der im Kontextmenü angezeigt werden soll, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie anpassen**.

4. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Richtlinienprofile** aus.

5. Klicken Sie im Arbeitsbereich auf **Hinzufügen**.

6. Lesen Sie im Fenster **Zuweisen von Richtlinienprofilen** die Informationen über Richtlinien und klicken Sie auf **Weiter**.

   Wenn dieses Fenster beim Erstellen neuer Richtlinienprofile nicht angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**, bevor Sie auf **Weiter** klicken.

7. Gehen Sie im Fenster **Name des Richtlinienprofils** wie folgt vor, um das Richtlinienprofil anzupassen:

   - Geben Sie den Namen des neuen Richtlinienprofils ein.

     Hinweis: Der Name eines Profils darf höchstens 100 Zeichen lang sein.

   - Wählen Sie im Abschnitt **Status des Richtlinienprofils** aus, ob das Richtlinienprofil aktiviert oder deaktiviert sein soll.
   - Wählen Sie in der Dropdown-Liste im Abschnitt **Status des Richtlinienprofils** aus, ob das Richtlinienprofil bearbeitet werden darf.
   - Wenn Sie Aktivierungsregeln für das Richtlinienprofil festlegen möchten, aktivieren Sie das Kontrollkästchen **Nach Beendigung des Assistenten für neue Richtlinienprofile zur Konfiguration der Aktivierungsregeln für das Richtlinienprofil wechseln**.

8. Klicken Sie auf **Fertigstellen**.

9. Wenn Sie das Kontrollkästchen **Nach Beendigung des Assistenten für neue Richtlinienprofile zur Konfiguration der Aktivierungsregeln für das Richtlinienprofil wechseln** aktiviert haben, führen Sie die Schritte des Assistenten für neue Aktivierungsregeln für ein Richtlinienprofil aus.

Das erstellte Richtlinienprofil wird im Abschnitt **Richtlinienprofile** des Fensters **Eigenschaften**:**<Name der Richtlinie>** angezeigt.

Aktivierungsregel für ein Richtlinienprofil erstellen

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, in der Sie eine Aktivierungsregel für das Richtlinienprofil erstellen möchten.

2. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

3. Führen Sie eine der folgenden Aktionen aus, um die Eigenschaften der Richtlinie zu öffnen:

   - Doppelklick auf den Namen der Richtlinie.
   - Klicken Sie mit der rechten Maustaste auf den Richtliniennamen, der im Kontextmenü angezeigt werden soll, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie anpassen**.

4. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Richtlinienprofile** aus.

5. Wählen Sie im Arbeitsbereich das Richtlinienprofil aus, für das Sie eine Aktivierungsregel erstellen möchten und klicken Sie auf **Eigenschaften**.

   Das Fenster **Eigenschaften: <Name des Richtlinienprofils>** wird geöffnet.

6. Wählen Sie den Abschnitt **Aktivierungsregeln** aus.

7. Klicken Sie im Arbeitsbereich auf **Hinzufügen**.

   Der Assistent für neue Aktivierungsregeln für ein Richtlinienprofil wird gestartet.

Folgen Sie den Schritten des Assistenten für neue Aktivierungsregeln für ein Richtlinienprofil.

Richtlinienprofil modifizieren

1. Wählen Sie in der Baumstruktur die Administrationsgruppe aus, bei der Sie ein Richtlinienprofil bearbeiten möchten.

2. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.

3. Führen Sie zum Öffnen der Eigenschaften der Richtlinie, für die Sie ein Profil bearbeiten möchten, eine der folgenden Aktionen aus:

   - Doppelklick auf den Namen der Richtlinie.
   - Klicken Sie mit der rechten Maustaste auf den Richtliniennamen, der im Kontextmenü angezeigt werden soll, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie anpassen**.

4. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Richtlinienprofile** aus.

5. Wählen Sie im Arbeitsbereich das Richtlinienprofil aus, das Sie bearbeiten möchten, und klicken Sie auf **Eigenschaften**.

   Das Fenster **Eigenschaften: <Name des Richtlinienprofils>** wird geöffnet.

6. Passen Sie das Profil falls nötig an:

   - Benennen Sie das Profil im Abschnitt **Allgemein** um, oder aktivieren/deaktivieren Sie das Profil, indem Sie das Kontrollkästchen **Profil aktivieren** aktivieren/deaktivieren.
   - Erstellen, bearbeiten oder löschen Sie im Abschnitt **Aktivierungsregeln** die Aktivierungsregeln.

- Wählen Sie im Abschnitt **Geräte** die Geräte aus, auf die das Richtlinienprofil angewendet werden soll.
- Bearbeiten Sie die Richtlinieneinstellungen in den relevanten Abschnitten.

7. Klicken Sie auf **OK**.

Wenn das Richtlinienprofil aktiv ist, werden die modifizierten Einstellungen angewandt, nachdem der Client-Computer mit dem Administrationsserver synchronisiert wurde. Wenn das Richtlinienprofil inaktiv ist, wird es nach Auslösen der Aktivierungsregel aktiviert.

Priorität des Richtlinienprofils ändern

1. Wählen Sie in der Baumstruktur die Administrationsgruppe aus, bei der Sie die Priorität eines Richtlinienprofils ändern möchten.
2. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
3. Führen Sie zum Öffnen der Eigenschaften der Richtlinie, deren Priorität Sie ändern möchten, eine der folgenden Aktionen aus:
   - Doppelklick auf den Namen der Richtlinie.
   - Klicken Sie mit der rechten Maustaste auf den Richtliniennamen, der im Kontextmenü angezeigt werden soll, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie anpassen**.
4. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Richtlinienprofile** aus.
5. Wählen Sie im Arbeitsbereich das Richtlinienprofil aus, dessen Priorität Sie ändern möchten.
6. Erhöhen/reduzieren Sie die Priorität des ausgewählten Profils mithilfe der Schaltflächen .

Richtlinienprofil löschen

1. Wählen Sie in der Baumstruktur die Administrationsgruppe aus, bei der Sie ein Richtlinienprofil löschen möchten.
2. Öffnen Sie im Arbeitsbereich die Registerkarte **Richtlinien**.
3. Führen Sie zum Öffnen der Eigenschaften der Richtlinie, für die Sie ein Profil löschen möchten, eine der folgenden Aktionen aus:
   - Doppelklick auf den Namen der Richtlinie.
   - Klicken Sie mit der rechten Maustaste auf den Richtliniennamen, der im Kontextmenü angezeigt werden soll, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie anpassen**.
4. Wählen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Richtlinienprofile** aus.
5. Wählen Sie im Arbeitsbereich das Profil aus, das Sie löschen möchten, und klicken Sie auf **Löschen**.

Ausführliche Informationen über Richtlinienprofilen finden Sie in der Hilfe zu Kaspersky Security Center.

Bericht über erkannte Objekte generieren

Bericht über erkannte Objekte generieren

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Klicken Sie in der Konsolenstruktur auf **Verwaltete Geräte**.
4. Wählen Sie die Administrationsgruppe aus, die den gewünschten Client-Computer enthält.
5. Öffnen Sie die Registerkarte **Geräte**.
6. Wählen Sie in der Liste der Client-Computer den gewünschten Computer aus.
7. Öffnen Sie durch Rechtsklick auf den ausgewählten Computer das Kontextmenü und wählen Sie **Alle Aufgaben** > **Bericht über Bedrohungen anzeigen** aus.

Der generierte Bericht wird im Browserfenster geöffnet.

Informationen über andere Möglichkeiten, einen Bericht über Objekte zu erstellen, die von der App auf dem Client-Computer erkannt werden, finden Sie in der Hilfe zu Kaspersky Security Center.

Wiederherstellungsschlüssel für einen verschlüsselten Datenträger anfordern

Wenn der Benutzer eines Client-Computers seine Anmeldedaten vergisst oder verliert, und deshalb nicht mehr auf einen verschlüsselten Datenträger zugreifen kann, können Sie einen Wiederherstellungsschlüssel anfordern.

Wiederherstellungsschlüssel anfordern

1. Starten Sie die Kaspersky Security Center-Administrationskonsole.
2. Erweitern Sie den Knoten **Administrationsserver <Servername>**.
3. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert**, danach den Unterordner **Verschlüsselung und Datenschutz** und dann den Unterordner **Verschlüsselte Laufwerke** aus.
4. Klicken Sie im Arbeitsbereich mit der rechten Maustaste auf das Gerät mit dem verschlüsselten Datenträger, um das Kontextmenü anzuzeigen, und wählen Sie **Wiederherstellungsschlüssel für macOS anfordern** aus.

   Ein Fenster mit dem Wiederherstellungsschlüssel wird geöffnet.
5. Speichern Sie den Wiederherstellungsschlüssel.

Sie können den Wiederherstellungsschlüssel auf einem Client-Computer verwenden, um auf den verschlüsselten Datenträger zuzugreifen.

Remote-Verwaltung der Anwendung über Kaspersky Security Center Web Console und Cloud Console

Kaspersky Security Center Web Console (Web Console) ist eine Web-Anwendung, mit der grundlegende Aufgaben für die Verwaltung und Wartung der Sicherheit eines Unternehmensnetzwerks zentralisiert gelöst werden können. „Web Console" ist eine Komponente von Kaspersky Security Center. Mit ihrer Benutzeroberfläche kann Kaspersky Endpoint Security in einem Browserfenster verwaltet werden. Ausführliche Informationen zu Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

Kaspersky Security Center Cloud Console (Cloud Console) ist eine cloudbasierte Lösung für den Schutz und die Verwaltung eines Unternehmensnetzwerks. Ausführliche Informationen zu Kaspersky Security Center Cloud Console finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console.

Sie können Kaspersky Endpoint Security auch über die grafische Benutzeroberfläche der Anwendung, die Kaspersky Security Center Verwaltungskonsole und über die Befehlszeile verwalten.

Web-Plug-in für Kaspersky Endpoint Security installieren

Das Web-Plug-in von Kaspersky Endpoint Security ermöglicht die Interaktion zwischen Kaspersky Endpoint Security und Kaspersky Security Center. Das Web-Plug-in muss auf einem Gerät installiert werden, auf dem bereits die Kaspersky Security Center Web Console installiert ist. Die Funktionen des Web-Plug-ins stehen allen Administratoren zur Verfügung, sofern diese über einen Browser den Zugriff auf die Kaspersky Security Center Web Console haben.

Sie können das Web-Plug-in wie folgt installieren:

- Unter Verwendung des Schnellstartassistenten der Kaspersky Security Center Web Console.

  Wenn Sie die Web Console zum ersten Mal mit dem Administrationsserver verbinden, fordert die Web Console Sie automatisch auf, den Schnellstartassistenten auszuführen. Außerdem können den Schnellstartassistenten auch über die Benutzeroberfläche der Web Console starten (**Entdeckung und Bereitstellung** → **Bereitstellung und Zuweisung** → **Schnellstartassistent**). Der Schnellstartassistent kann auch überprüfen, ob die installierten Web-Plug-ins auf dem neuesten Stand sind, und erforderliche Updates herunterladen. Weitere Informationen zum Schnellstartassistenten für „Kaspersky Security Center Web Console" finden Sie in der Hilfe zu Kaspersky Security Center.

- Manuell, unter Verwendung eines Programmpaket der Web Console aus einer externen Quelle.

  Um das Web-Plug-in zu installieren, fügen Sie das zip-Archiv des Programmpakets für das Web-Plug-in von Kaspersky Endpoint Security über die Benutzeroberfläche der Web Console hinzu: **Konsoleneinstellungen** > **Web-Plug-ins**. Das Programmpaket des Web-Plug-ins kann von der Kaspersky-Website heruntergeladen werden.

So installieren Sie das Web-Plug-in von Kaspersky Endpoint Security manuell:

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console **Konsoleneinstellungen** > **Web-Plug-ins** aus.

   Es wird eine Liste der installierten Web-Plug-ins geöffnet.

2. Starten Sie die Installation des Web-Plug-ins von Kaspersky Endpoint Security auf eine der folgenden Arten:

- Installation aus der Liste der Web-Plug-ins von Kaspersky:

  a. Klicken Sie auf **Hinzufügen**.

  Es wird die Liste aller verfügbaren Web-Plug-ins von Kaspersky geöffnet. Die Liste wird automatisch aktualisiert, sobald von Web-Plug-ins neue Versionen veröffentlicht werden.

  b. Suchen Sie in der Liste nach dem Web-Plug-in von Kaspersky Endpoint Security for Mac 12.2 und klicken Sie auf dessen Namen.

  c. Klicken Sie im folgenden Fenster mit einer Beschreibung des Web-Plug-ins auf die Schaltfläche **Plug-in installieren**.

  d. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie im Informationsfenster auf **OK**.

- Installation des Web-Plug-ins aus einer externen Quelle (die für die Installation der Web-Plug-ins erforderlichen Archive sind im Lieferumfang enthalten):

  a. Klicken Sie auf **Aus Datei hinzufügen**.

  b. Geben Sie im folgenden Fenster den Pfad des zip-Archivs mit dem Web-Plug-in und den Pfad der Signaturdatei im txt-Format an. Diese Datei befindet sich im Archiv zusammen mit dem Web-Plug-in.

  c. Klicken Sie auf **Hinzufügen**.

  d. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie im Informationsfenster auf **OK**.

Das neue Plug-in wird in der Liste der installierten Web-Plug-ins angezeigt (**Konsoleneinstellungen** > **Web-Plug-ins**).

Hinweis: Wenn Sie in den Eigenschaften des Kaspersky Security Center Administrationsservers eine Sprache auswählen, die nicht im Programmpaket für Kaspersky Endpoint Security enthalten ist, werden der Lizenzvertrag und die gesamte Benutzeroberfläche von Kaspersky Security Center Web Console in Englisch angezeigt.

Richtlinien erstellen

Dieser Abschnitt informiert darüber, wie mithilfe von Kaspersky Security Center Web Console und Cloud Console die Richtlinien für Kaspersky Endpoint Security erstellt und angepasst werden.

Eine Richtlinie legt die Einstellungen einer Anwendung fest und bestimmt, ob diese Anwendung auf Computern innerhalb einer Administrationsgruppe angepasst werden kann. Für jede Anwendung muss eine eigene Richtlinie erstellt werden. Sie können mehrere Richtlinien für die Anwendungen erstellen, die auf Computern unterschiedlicher Administrationsgruppen installiert sind. Allerdings kann jeweils nur eine Richtlinie auf eine bestimmte Anwendung in der Administrationsgruppe angewandt werden.

Hinweis: Wenn Sie eine Richtlinie erstellen und anpassen, können Sie mithilfe des Umschalters **Erzwingen** Änderungen in einer beliebigen Einstellungsgruppen in den Richtlinien verbieten oder erlauben.

Richtlinie erstellen

1. Wählen Sie im Abschnitt **Geräte** links den Abschnitt **Richtlinien und Profile** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie die Anwendung aus, für die Sie eine Richtlinie erstellen möchten, und klicken Sie auf **Weiter**.

   Das Fenster **Neue Richtlinie** wird geöffnet.
4. Geben Sie auf der Registerkarte **Allgemein** einen Namen für die Richtlinie an und passen Sie den Richtlinienstatus und die Richtlinieneinstellungen für die Vererbungsoptionen an.
5. Passen Sie auf der Registerkarte **Anwendungseinstellungen** die Einstellungen an, die auf Kaspersky Endpoint Security auf dem Client-Computer angewendet werden, wenn die Richtlinie durchgesetzt wird.
6. Klicken Sie auf **Speichern**.

Mit benutzerdefinierten Aufgaben können Sie folgende Aktionen ausführen:

- Richtlinien erstellen.
- Richtlinien konfigurieren.
- Richtlinien aus einer Gruppe in eine andere kopieren oder entfernen.
- Richtlinien löschen.
- Status von Richtlinien ändern.

Ausführliche Informationen über die Richtlinien von Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

Ausführliche Informationen über die Richtlinien von Kaspersky Security Center Cloud Console finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console.

Hinweis: Nachdem Sie mithilfe von Kaspersky Security Center Web Console und Cloud Console ein Richtlinienprofil für eine Kaspersky Endpoint Security-Richtlinie erstellt haben, müssen Sie überprüfen, ob die Einstellungen auf den Client-Computern korrekt angewendet wurden.

Einstellungen für den „Erweiterten Schutz“ anpassen

Im Abschnitt **Erweiterter Schutz** können Sie festlegen, ob Kaspersky Endpoint Security auf den Client-Computern an Kaspersky Security Network teilnimmt, und Sie können die Verwendung von KSN Proxy anpassen.

Gehen Sie bei Bedarf wie folgt vor:

- Lesen Sie den vollständigen Text der Erklärung zu Kaspersky Security Network. Klicken Sie dazu auf den Link **KSN-Erklärung**.
- Sehen Sie sich die Informationen über die KSN-Infrastruktur an, die von Kaspersky Security Center angeboten wird. Klicken Sie dazu auf den Link **KSN-Erklärung**.

  Hinweis: In Kaspersky Security Center wird standardmäßig die „Global KSN"-Infrastruktur verwendet. Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Web Console verwalten, ist es von den Einstellungen für Kaspersky Security Center abhängig, ob Sie anstelle von Kaspersky Endpoint Security an Kaspersky Private Security Network teilnehmen können. Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, ist eine Teilnahme an Kaspersky Private Security Network nicht möglich. Ausführliche Informationen zur Teilnahme an Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center.

- Aktivieren/deaktivieren Sie die Verwendung von Kaspersky Security Network.
- Aktivieren/deaktivieren Sie den erweiterten KSN-Modus.
- Aktivieren bzw. deaktivieren Sie den Cloud-Modus.
- Aktivieren oder deaktivieren Sie die Verwendung eines KSN-Proxys.
- Aktivieren oder deaktivieren Sie die Verwendung der Kaspersky-Server, wenn der KSN-Proxy nicht verfügbar ist.

Hinweis: Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Web Console verwalten, ist die Verwendung von Kaspersky Security Network und eines KSN-Proxys auf Remote-Computern nur dann verfügbar, wenn der Administrationsserver von Kaspersky Security Center als Proxy-Server verwendet wird. Ausführliche Informationen über die Administrationsserver-Eigenschaften finden Sie in der Hilfe zu Kaspersky Security Center.
Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, können Sie Verteilungspunkte mit einem Windows-Betriebssystem nutzen, um Kaspersky Security Network und einen KSN-Proxy auf Remote-Computern zu verwenden.

Wenn Kaspersky Security Center die „Global KSN"-Infrastruktur verwendet und Sie in den Richtlinieneinstellungen die Teilnahme an Kaspersky Security Network festlegen, sendet Kaspersky Endpoint Security von den Client-Computern, für welche die Richtlinie gilt, automatisch Statistiken an Kaspersky. Dadurch wird der Schutz dieser Computer verbessert.

Hinweis: Ohne Ihre ausdrückliche Zustimmung empfängt, verarbeitet oder speichert Kaspersky keine personenbezogenen Daten.

Daten, die an Kaspersky bereitgestellt werden, wenn Kaspersky Security Network in der Global KSN-Infrastruktur verwendet wird

Wenn der Umschalter **Kaspersky Security Network** aktiviert ist und der Umschalter **Erweiterter KSN-Modus** deaktiviert ist, stellt Kaspersky Endpoint Security, das auf Client-Computern läuft, die folgenden Daten an Kaspersky bereit:

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Vollversion der installierten Software;
  Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; einmalige Geräte-ID Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

Wenn die Umschalter **Kaspersky Security Network** und **Erweiterter KSN-Modus** aktiviert sind, stellt Kaspersky Endpoint Security, das auf Client-Computern läuft, die folgenden Daten an Kaspersky bereit:

- Informationen über die Version des Betriebssystems (OS) und die auf dem Computer installierten Service Packs, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems, Parameter des Funktionsmodus des Betriebssystems; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Windows Service Packs; Datum und Uhrzeit des Betriebssystemstarts; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Verhaltensanalyse-Subsystem; Anzahl der verzögerten Aktionsereignisse des Betriebssystems des aktuellen Typs; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Subsystem für den proaktiven Schutz; Anzahl der verarbeiteten Aktionsereignisse des Betriebssystems; Anzahl der verarbeiteten synchronen Aktionsereignisse des Betriebssystems; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems des aktuellen Typs; Verarbeitungsverzögerungszeit des Ereignisses über die Betriebssystemaktion im Subsystem für die persistente Ereignisspeicherung; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems; Anzahl der wartenden synchronen Aktionsereignisse des Betriebssystems; Datum und Uhrzeit des empfangenen Ereignisses über eine Aktion im Betriebssystem.

- Informationen über den fehlgeschlagenen letzten Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.

- Informationen über die installierte Anwendung des Rechtsinhabers und den Status des Antiviren-Schutzes: ID der Software-Installation (PCID) Version des Software-Datenbankeintrags; eindeutige ID der Instanz der Anwendungsinstallation auf dem Computer, Anwendungstyp, Anwendungstyp-ID, die Vollversion der installierten Anwendung, ID der Version der Anwendungseinstellungen, ID des Computertyps, eindeutige ID des Computers, auf dem die Anwendung installiert ist, eindeutige Benutzer-ID beim Dienst des Rechteinhabers, lokale Sprache und Betriebszustand, Version der installierten Softwarekomponenten und ihr Betriebszustand, Version des verwendeten Protokolls zur Verbindungsherstellung zum Dienst des Rechteinhabers; Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Anzahl der Update-Anwendungs-Zyklen für die Antiviren-Datenbanken; Zeitpunkt (Datum und Uhrzeit), an dem die Antiviren-Datenbanken zuletzt aktualisiert und angewendet wurden; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version der Software-Komponente; ID des Software-Updates; Typ der installierten Software; Startdatum und -uhrzeit vom Aktivitätsmonitor; Installationsdatum und -uhrzeit der Software; Wahrscheinlichkeit der Übermittlung von Statistiken durch den Aktivitätsmonitor; Code des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Datenbank-Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; maximal zulässige Zeit für die Verarbeitung eines Ereignisses durch den Aktivitätsmonitor; Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Gesamtzahl der Ereignisse, die länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert haben.

- Informationen über alle verarbeiteten Objekte und Vorgänge: Verdikt der Software für das verarbeitete Objekt; Verzeichniscode; Größe des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Anzahl der erkannten Software im Kontext des „Aktivitätsmonitors“; Zeitpunkt (Datum und Uhrzeit), zu dem der „Aktivitätsmonitor“ die Software erkannt hat; Erkennungscharakteristiken; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Grund, aus dem der „Aktivitätsmonitor“ die Software erkannt hat; Prüfsumme (MD5) des verarbeiteten Objekts; Ergebnis der Modul-Integritätsprüfung; Name des verarbeiteten Objekts; Typ des ausgelösten Eintrags der Antiviren-Datenbanken der Software; Speicherpfad des verarbeiteten Objekts; Name des untersuchten Objekts; Datum und Uhrzeit der Untersuchung; URL-Adresse und Referenzadresse, von denen es heruntergeladen wurde; Größe und Pfade der untersuchten Dateien; Zeichen des Archivs; Datum und Uhrzeit der Dateierstellung; Name, Größe und Prüfsummen (MD5, SHA2-256) des Packers (falls die Datei gepackt wurde); Entropie der Datei; Typ der Datei; Code des Dateityps; Zeichen, ID und Format der ausführbaren Datei; Prüfsumme des Objekts (MD5, SHA2-256); Typ und Wert der zusätzlichen Prüfsumme des Objekts; Daten über die digitale Signatur des Objekts (Zertifikat): Daten über den Herausgeber des Zertifikats, Anzahl der Starts des Objekts seit der letzten Übermittlung von Statistiken, ID der Überprüfungsaufgabe der Anwendung, Mittel zum Erhalt von Informationen über den Ruf des Objekts, Wert des Zielfilters, technische Parameter der anwendbaren Erkennungstechnologien; Speicherpfad des verarbeiteten Objekts; Verzeichniscode.

- Für ausführbare Dateien: Entropie der Dateiabschnitte, Kennzeichen der Reputations-Überprüfung oder Kennzeichen der Dateisignatur, Name, Typ, ID-Typ, Prüfsumme (MD5) und Größe der Anwendung, die vom zu validierenden Objekt geladen wurde, Anwendungspfad und Vorlagenpfade, Attribut, das das Vorhandensein in der Autostart-Liste angibt, Datum des Eintrags, Liste mit Attributen, Name des Packers, Informationen über die digitale Signatur der Anwendung: Herausgeberzertifikat, Name der hochgeladenen Datei im MIME-Format, Datum und Uhrzeit der Dateierstellung.

- Informationen über die gestarteten Anwendungen und deren Module: Prüfsummen (MD5, SHA2-256) von ausgeführten Dateien, Größe, Attribute, Erstellungsdatum, Name des Packers (falls die Datei gepackt wurde), Dateinamen, Informationen über die im System ausgeführten Prozesse (Prozess-ID (PID), Prozessname, Informationen über das Benutzerkonto, aus dem der Prozess gestartet wurde, Anwendung und Befehl, mit dem der Prozess gestartet wurde, vollständiger Pfad der Dateien des Prozesses sowie auszuführende Befehlszeile, Beschreibung der Anwendung, zu dem der Prozess gehört (Name der Anwendung und Informationen über den Herausgeber) sowie die verwendeten digitalen Zertifikate und Informationen, die zur Überprüfung ihrer Authentizität dienen, oder Informationen über das Fehlen einer digitalen Signatur einer Datei) und Informationen über die in die Prozesse geladenen Module: deren Namen, Größen, Typen, Erstellungsdaten, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfade, Header-Informationen der PE-Datei, Namen der Packer (falls die Datei gepackt wurde), Informationen über die Verfügbarkeit und Gültigkeit dieser Statistiken, ID des Modus zur Erstellung von zu sendenden Statistiken.

- Falls Bedrohungen oder Schwachstellen erkannt werden, werden zusätzlich zu den Informationen über das erkannte Objekt auch die folgenden Informationen bereitgestellt: ID, Version und Typ des Eintrags in der Antiviren-Datenbank, Name der Bedrohung, basierend auf der Klassifikation von Kaspersky, Datum und Uhrzeit der letzten Aktualisierung der Antiviren-Datenbank, Name der ausführbaren Datei, Prüfsumme (MD5) der Anwendungsdatei, welche die Webadresse, unter der die Bedrohung erkannt wurde, angefordert hat, IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, ID der Schwachstelle und ihre Gefahrenstufe, URL und Referenz der Webseite, auf der die Schwachstelle gefunden wurde.

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt.

- Informationen über einen Netzwerkangriff: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.

- Informationen zu Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, aus der der Prozess gestartet wurde, der den Port geöffnet hat, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Verbindungsports, Verbindungsstatus, Zeitstempel für das Öffnen des Ports.

- URL- und IP-Adresse der Webseite, auf der schädliche oder verdächtige Inhalte erkannt wurden, Name, Größe und Prüfsumme der Datei, die die URL anforderte, Kennung, Priorität und Grad der Regel, die für die Entscheidung verwendet wurde, Ziel des Angriffs.

- Informationen über Updates der installierten App- und Antiviren-Datenbanken: Bearbeitungsstand der Update-Aufgabe, Art des Fehlers, der möglicherweise während des Update-Vorgangs aufgetreten ist, Anzahl der fehlgeschlagenen Updates, ID der Anwendungskomponente, die die Updates ausführt.

- Informationen über die Nutzung von Kaspersky Security Network (KSN): KSN-ID, Anwendungs-ID, vollständige Version der Anwendung, anonymisierte IP-Adresse des Benutzergerätes, Indikatoren für die Qualität der Ausführung von KSN-Anfragen, Indikatoren für die Qualität der Verarbeitung von KSN-Paketen, Indikatoren für die Anzahl der KSN-Anfragen und Informationen über die Arten von KSN-Anfragen, Datum und Uhrzeit für den Beginn des Sendevorgangs von Statistiken, Datum und Uhrzeit für das Ende des Sendevorgangs von Statistiken, Informationen über die Aktualisierung der KSN-Konfiguration: ID der aktiven Konfiguration, ID der empfangenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen zu Systemprotokoll-Ereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.

- Informationen zur Bestimmung der Reputation von Dateien und URL-Adressen: URL-Adresse, unter der die Reputation angefordert wird, und Referrer, Protokolltyp der Verbindung, interne ID des Anwendungstyps, Nummer des verwendeten Ports, Benutzer-ID, Prüfsumme der untersuchten Datei (MD5), Typ der erkannten Bedrohung, Informationen über den Datensatz, der zum Erkennen der Bedrohung verwendet wurde (ID des Datensatzes für die Antiviren-Datenbanken, Zeitstempel und Typ des Datensatzes); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

- Daten zur geografischen Verteilung der Anwendung: Datum der Anwendungsinstallation und -aktivierung, ID des Partners, der die Lizenz für die Anwendungsaktivierung bereitstellt, Anwendungs-ID, Lokalisierungs-ID der Anwendungssprache, Lizenz-Seriennummer für die Anwendungsaktivierung, Merkmal für die KSN-Teilnahme.

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Informationen über die auf dem Computer installierte Hardware: Typ, Name, Modellname, Firmware-Version, Parameter der integrierten und angeschlossenen Geräte.

- Informationen über das Gerät: Geräte-ID.

- Informationen zum Betrieb der Komponente Web-Kontrolle:
  Komponentenversion, Kategorisierungsgrund, zusätzliche Informationen zum Kategorisierungsgrund, kategorisierte URL, Host-IP-Adresse des blockierten/kategorisierten Objekts.

Wenn Kaspersky Security Center die „Private KSN“-Infrastruktur verwendet und Sie in den Richtlinieneinstellungen die Teilnahme an Kaspersky Security Network festlegen, sendet Kaspersky Endpoint Security keine Statistiken von den Client-Computern, für welche die Richtlinie gilt.

Einstellungen für den „Basisschutz“ anpassen

Im Abschnitt **Basisschutz** können Sie die folgenden Komponenten anpassen:

- Schutz vor bedrohlichen Dateien
- Schutz vor Web-Bedrohungen
- Schutz vor Netzwerkbedrohungen

Sie können ein Fenster öffnen, um die Komponenteneinstellungen anzupassen. Klicken Sie dazu auf den entsprechenden Link.

Einstellungen für den „Schutz vor bedrohlichen Dateien“ anpassen

Führen Sie im Fenster **Schutz vor bedrohlichen Dateien** bei Bedarf die folgenden Schritte durch:

- Aktivieren/deaktivieren Sie den „Schutz vor bedrohlichen Dateien“.

  Der „Schutz vor bedrohlichen Dateien“ ist standardmäßig aktiviert.

- Erstellen Sie einen Schutzbereich.
- Wählen Sie die Aktion aus, die nach dem Fund eines schädlichen Objekts ausgeführt werden soll.
- Legen Sie fest, ob Kaspersky Endpoint Security nur neue und geänderte Dateien oder alle Dateien untersuchen soll.
- Legen Sie fest, ob Kaspersky Endpoint Security auf Client-Computern das schreibgeschützte Systemvolume bei der Untersuchung überspringen soll.
- Legen Sie fest, ob Kaspersky Endpoint Security bei der Untersuchung die iSwift-Technologie verwenden soll.

  Hinweis: iSwift bietet in Kaspersky Endpoint Security einen speziellen Algorithmus, um bestimmte Objekte von der Untersuchung auszuschließen und dadurch die Untersuchung zu beschleunigen.

- Legen Sie fest, welche Dateitypen Kaspersky Endpoint Security untersuchen soll.
- Legen Sie fest, welche Aktionen Kaspersky Endpoint Security mit zusammengesetzten Dateien ausführen soll.

Einstellungen für den „Schutz vor Web-Bedrohungen“ anpassen

Führen Sie im Fenster **Schutz vor Web-Bedrohungen** bei Bedarf die folgenden Schritte durch:

- Aktivieren/deaktivieren Sie den „Schutz vor Web-Bedrohungen“.

  Der „Schutz vor Web-Bedrohungen“ ist standardmäßig aktiviert.
- Wählen Sie die Aktion, die nach Löschen eines schädlichen Objekts im Web-Datenverkehr ausgeführt werden soll.
- Erstellen oder bearbeiten Sie eine Liste für vertrauenswürdige Webadressen.

Einstellungen für den „Schutz vor Netzwerkbedrohungen“ anpassen

Führen Sie im Fenster **Schutz vor Netzwerkbedrohungen** bei Bedarf die folgenden Schritte durch:

- Aktivieren/deaktivieren Sie den „Schutz vor Netzwerkbedrohungen“.

  Der „Schutz vor Netzwerkbedrohungen“ ist standardmäßig aktiviert.
- Aktivieren oder deaktivieren Sie die Sperrung von angreifenden Computern.
- Erstellen oder bearbeiten Sie eine Liste mit IP-Adressen von Remote-Computern, deren Netzwerkaktivität Kaspersky Endpoint Security nicht blockiert.

Sicherheitskontrolle anpassen

Führen Sie im Fenster **Sicherheitskontrolle** bei Bedarf die folgenden Schritte durch:

- Aktivieren/deaktivieren Sie die „Web-Kontrolle“.

  Hinweis: Wenn Sie die „Web-Kontrolle“ aktivieren, um den Zugriff auf gefährliche Webressourcen zu blockieren, zeigt Kaspersky Endpoint Security im „Schutz-Center“ auf dem Remote-Computer die Benachrichtigung **Die Web-Kontrolle ist aktiviert** an.
  Kaspersky Endpoint Security zeigt Benachrichtigungen an, wenn der Benutzer auf dem Remote-Computer auf Webressourcen zugreift, die von der „Web-Kontrolle“ blockiert werden, vorausgesetzt der Schalter **Sichere Verbindungen (HTTPS) untersuchen** im Fenster **Netzwerk** des Assistenten für neue Richtlinien ist aktiviert.

- Fügen Sie Regeln hinzu, die festlegen, welche Webadressen oder Website-Kategorien von der „Web-Kontrolle“ auf einem Benutzercomputer überwacht und verwaltet werden.

- Bearbeiten, löschen oder organisieren Sie die erstellten Regeln in der Liste.

  Die Reihenfolge, in der die Regeln angeordnet sind, entspricht der Priorität, nach welcher die Regeln durch Kaspersky Endpoint Security angewendet werden.

Datenverschlüsselung anpassen

Im Abschnitt **Datenverschlüsselung** können Sie die Verschlüsselung auf dem Startvolume des Client-Computers aktivieren oder deaktivieren, um zu verhindern, dass nicht autorisierte Benutzer auf sensible Daten zugreifen. Die FileVault-Volume-Verschlüsselung ist standardmäßig deaktiviert.

Einstellungen für Detection and Response konfigurieren

Im Abschnitt **Detection and Response** können Sie die folgenden Komponenten konfigurieren:

- Managed Detection and Response
- Endpoint Detection and Response
- Endpoint Detection and Response (KATA)

Sie können ein Fenster öffnen, um die Komponenteneinstellungen anzupassen. Klicken Sie dazu auf den entsprechenden Link.

Managed Detection and Response konfigurieren

Gehen Sie im Fenster **Managed Detection and Response** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Komponente Managed Detection and Response.
- Importieren oder löschen Sie die MDR-Konfigurationsdatei.

Die Komponente Managed Detection and Response ermöglicht die Interaktion mit dem Dienst Kaspersky Managed Detection and Response, der fortwährend Sicherheitsbedrohungen erkennt, die auf Ihr Unternehmen abzielen, und diese eliminiert.

Standardmäßig ist Managed Detection and Response deaktiviert.

Endpoint Detection and Response konfigurieren

Gehen Sie im Fenster **Endpoint Detection and Response** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Komponente Endpoint Detection and Response.
- Konfigurieren Sie die Einstellungen der Netzwerkisolation für das Benutzergerät:
  - Geben Sie eine Verzögerung für die automatische Deaktivierung der Netzwerkisolation an.
  - Konfigurieren Sie die Ausnahmen für die Netzwerkisolation.
- Aktivieren oder deaktivieren Sie die Ausführungsprävention.
- Wählen Sie eine Aktion aus, die beim Ausführen oder Öffnen eines verbotenen Objekts ausgeführt werden soll.
- Erstellen Sie eine Liste mit Regeln für die Ausführungsprävention.
- Aktivieren oder deaktivieren Sie die Cloud Sandbox-Technologie.

Die Komponente Endpoint Detection and Response kombiniert die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren. Auf diese Weise werden fortschrittliche Angriffe effektiv abgewehrt. Zu diesen gehören neuartige Exploits, Ransomware, dateilose Angriffe sowie Methoden, die legitime Systemtools ausnutzen.

Endpoint Detection and Response ist standardmäßig deaktiviert.

Endpoint Detection and Response (KATA) konfigurieren

Gehen Sie im Fenster **Endpoint Detection and Response (KATA)** bei Bedarf wie folgt vor:

- Aktivieren oder deaktivieren Sie die Komponente Endpoint Detection and Response (KATA).
- Konfigurieren Sie die Einstellungen für die Serververbindung:
  - Geben Sie das Timeout für die Antwort des KATA-Servers an.
  - Fügen Sie ein TLS-Zertifikat hinzu, um eine vertrauenswürdige Verbindung zu konfigurieren.
  - Legen Sie fest, ob Kaspersky Endpoint Security die Zwei-Wege-Überprüfung verwenden soll, um eine Verbindung mit einem KATA-Server herzustellen.
  - Laden Sie einen kennwortgeschützten Krypto-Container, um die Zwei-Wege-Überprüfung zu aktivieren.
- Fügen Sie einen KATA-Server hinzu.
- Legen Sie fest, ob Kaspersky Endpoint Security eine TTL für Pakete verwenden soll, die an einen KATA-Server gesendet werden.
- Konfigurieren Sie die Einstellungen für das Senden von Daten an KATA-Server.
- Beschränken Sie die Anzahl der Ereignisse, die Kaspersky Endpoint Security an den KATA-Server überträgt.

Die Komponente Endpoint Detection and Response (KATA) vereinfacht die Interaktion mit der Lösung Kaspersky Anti Targeted Attack Platform, die komplexe Bedrohungen wie gezielte Angriffe, hochentwickelte, hartnäckige Bedrohungen, Zero-Day-Angriffe und andere sofort erkennt.

Endpoint Detection and Response (KATA) ist standardmäßig deaktiviert.

Update-Einstellungen anpassen

Führen Sie im Abschnitt **Update** bei Bedarf die folgenden Schritte durch:

- Aktivieren oder deaktivieren Sie das Update der Anwendungsmodule.
- Fügen Sie die Update-Quellen hinzu, die für das Update von Kaspersky Endpoint Security verwendet werden, oder löschen Sie nicht benötigte Update-Quellen.

Weitere Einstellungen anpassen

Führen Sie im Abschnitt **Erweiterte Einstellungen** bei Bedarf die folgenden Schritte durch:

- Konfigurieren Sie Schutzeinstellungen für das Betriebssystem auf dem Client-Computer.
- Wählen Sie die zu erkennenden Objekttypen aus.

- Legen Sie fest, ob der Start geplanter Aufgaben unterbunden werden soll, wenn der Computer im Akkubetrieb läuft.
- Passen Sie Einstellungen zum Generieren und Speichern von Berichten an.
- Passen Sie die Einstellungen für die Speicherung von Objekten im Backup an.
- Passen Sie die Einstellungen von Kaspersky Endpoint Security für die Interaktion mit dem Benutzer eines Client-Computers an.
- Verbindung mit dem Proxy-Server anpassen.
- Aktivieren oder deaktivieren Sie die Untersuchung des eingehenden und ausgehenden HTTPS-Datenverkehrs.
- Wählen Sie den Zertifikatspeicher für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Mozilla Firefox-Browser aus.
- Passen Sie die überwachten Ports an.
- Bearbeiten Sie die Listen der vertrauenswürdigen Dateien, Ordner und Anwendungen, die nicht von Kaspersky Endpoint Security überwacht werden.

Aufgaben erstellen

Dieser Abschnitt beschreibt, wie in Kaspersky Security Center Web Console und Cloud Console Aufgaben erstellt und angepasst werden, die Kaspersky Endpoint Security auf einem Client-Computer oder einer Gruppe von Computern ausführt, die von Kaspersky Security Center verwaltet werden.

Eine Aufgabe ist eine Auswahl konfigurierbarer Aktionen, die von Kaspersky Endpoint Security auf einem Client-Computer ausgeführt werden.

In Kaspersky Security Center Web Console und Cloud Console können Sie die folgenden Aufgaben erstellen:

- Virensuche
- Aktualisieren
- Rollback
- Schlüssel hinzufügen

Aufgabe erstellen

1. Wählen Sie im Abschnitt **Geräte** links den Abschnitt **Aufgaben** aus.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen einer Aufgabe wird gestartet.
3. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security for Mac 12.2** aus.
4. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die zu erstellende Aufgabe aus.
5. Ändern Sie bei Bedarf den Aufgabennamen im Feld **Aufgabenname**.

6. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen wird.
7. Passen Sie die Einstellungen für den ausgewählten Aufgabentyp an.
8. Schließen Sie den Assistenten zum Hinzufügen einer Aufgabe durch Klick auf **Fertig** ab.

> **Hinweis:** Wenn Sie das Kontrollkästchen **Nach Abschluss der Erstellung Aufgabendetails öffnen** im Fenster **Erstellung der Aufgabe abschließen** aktivieren, können Sie die Aufgabeneinstellungen anschließend ändern. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die standardmäßigen Aufgabeneinstellungen später jederzeit ändern.

Mit Aufgaben sind folgende Aktionen möglich:

- Aufgaben starten und beenden
- Aufgabeneinstellungen konfigurieren
- Fortschritt einer Aufgabe verfolgen
- Aufgaben aus einer Gruppe in eine andere Gruppe kopieren und verschieben
- Aufgaben löschen

Ausführliche Informationen über die Aufgaben von Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

Ausführliche Informationen über die Aufgaben von Kaspersky Security Center Cloud Console finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console.

Einstellungen der Aufgabe „Untersuchung“ anpassen

Auf der Registerkarte **Anwendungseinstellungen** können Sie die Einstellungen der Aufgabe **Untersuchung** für Kaspersky Endpoint Security auf den Remote-Computern anpassen.

Einstellungen der Aufgabe „Untersuchung“ öffnen

1. Gehen Sie zu **Geräte** > **Aufgaben**.
2. Doppelklicken Sie auf eine Aufgabe mit dem Aufgabentyp **Untersuchung**.
3. Klicken Sie auf die Registerkarte **Programmeinstellungen**.

Bei Bedarf können Sie wie folgt vorgehen:

- Legen Sie den Untersuchungsbereich fest.
- Legen Sie fest, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.
- Legen Sie fest, welche Dateitypen Kaspersky Endpoint Security untersuchen soll, wenn die Aufgabe „Untersuchung“ ausgeführt wird.

- Passen Sie die Leistungseinstellungen für die Untersuchung an.
- Legen Sie fest, welche zusammengesetzten Dateien Kaspersky Endpoint Security analysieren soll.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Einstellungen der Aufgabe „Schlüssel hinzufügen“ anpassen

Auf der Registerkarte **Anwendungseinstellungen** können Sie die Einstellungen der Aufgabe **Schlüssel hinzufügen** für Kaspersky Endpoint Security auf den Remote-Computern anpassen.

Einstellungen der Aufgabe „Schlüssel hinzufügen“ öffnen

1. Gehen Sie zu **Geräte** > **Aufgaben**.
2. Doppelklicken Sie auf eine Aufgabe mit dem Aufgabentyp **Schlüssel hinzufügen**.
3. Klicken Sie auf die Registerkarte **Programmeinstellungen**.

Bei Bedarf können Sie wie folgt vorgehen:

- Die aktuelle Lizenz als Reserveschlüssel festlegen.
- Einen anderen Schlüssel festlegen, mit dem Kaspersky Endpoint Security auf einem Benutzercomputer aktiviert werden soll.
- Einen neuen Lizenzschlüssel zur Datenverwaltung von Kaspersky Security Center hinzufügen.

Update-Aufgabe anpassen

Auf der Registerkarte **Programmeinstellungen** können Sie die Einstellungen der Aufgabe **Update** von Kaspersky Endpoint Security auf den Remote-Computern anpassen.

Einstellungen der Update-Aufgabe öffnen

1. Gehen Sie zu **Geräte** > **Aufgaben**.
2. Doppelklicken Sie auf eine Aufgabe mit dem Aufgabentyp **Update**.
3. Klicken Sie auf die Registerkarte **Programmeinstellungen**.

Die grundlegende Update-Quelle für Kaspersky Endpoint Security sind die dedizierten Kaspersky-Update-Server. Kaspersky Endpoint Security kann auch Verteilungspunkte, lokale Ordner oder andere Webserver als *Update-Quelle* verwenden.

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Web Console verwalten, enthält die Liste der Update-Quellen standardmäßig die Kaspersky-Update-Server und die Server von Kaspersky Security Center. Kaspersky Endpoint Security lädt Updates zuerst von den Servern von Kaspersky Security Center herunter und dann von den Kaspersky-Update-Servern.

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, enthält die Liste der Update-Quellen standardmäßig die Kaspersky-Update-Server und die Verteilungspunkte. Kaspersky Endpoint Security lädt Updates zuerst von den Verteilungspunkten herunter und dann von den Kaspersky-Update-Servern. Ausführliche Informationen über Verteilungspunkte finden Sie in der Hilfe zu Kaspersky Security Center.

Bei Bedarf können Sie wie folgt vorgehen:

- Aktivieren oder deaktivieren Sie das Update der Anwendungsmodule.
- Fügen Sie die Update-Quellen hinzu, die für das Update von Kaspersky Endpoint Security verwendet werden, oder löschen Sie nicht benötigte Update-Quellen.

Wiederherstellungsschlüssel für ein verschlüsseltes Laufwerk anfordern

Wenn der Benutzer eines Client-Computers seine Anmeldedaten vergisst oder verliert, und deshalb nicht mehr auf ein verschlüsseltes Laufwerk zugreifen kann, können Sie einen Wiederherstellungsschlüssel anfordern.

Wiederherstellungsschlüssel anfordern

1. Klicken Sie auf den Namen des Administrator-Benutzerkontos unten links im Fenster von Kaspersky Security Center Web Console oder „Cloud Console“.
2. Wählen Sie **Schnittstellen-Optionen** aus.
3. Aktivieren Sie im folgenden Dialog den Umschalter **Verschlüsselung und Datenschutz anzeigen**, um die Verwaltung der Datenverschlüsselung zu aktivieren, und klicken Sie auf **Speichern**.
4. Gehen Sie zu **Vorgänge** > **Verschlüsselung und Datenschutz** > **Verschlüsselte Laufwerke**.

   Die Liste der verschlüsselten Geräte wird geöffnet.
5. Aktivieren Sie das Kontrollkästchen neben dem Gerät mit dem verschlüsselten Laufwerk.
6. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.
7. Wählen Sie im Dialog **Zugriff auf das Gerät im autonomen Modus gewähren** das Web-Plug-in für Kaspersky Endpoint Security aus und klicken Sie auf **OK**.
8. Klicken Sie auf **Wiederherstellungsschlüssel anfordern**.

   Im aktuellen Dialogfenster erscheint ein Wiederherstellungsschlüssel.
9. Speichern Sie den Wiederherstellungsschlüssel.

Sie können den Wiederherstellungsschlüssel auf einem Client-Computer verwenden, um auf das verschlüsselte Laufwerk zuzugreifen.

Das Fenster „Installationstyp“

Im Abschnitt **Zu installierende Pakete** können Sie die Anwendungskomponenten auswählen, die auf einem Client-Computer installiert werden.

Untersuchung

Dieses Kontrollkästchen fügt die Komponente „Untersuchung“ zum Installationspaket für Kaspersky Endpoint Security hinzu.

Wenn das Kontrollkästchen aktiviert ist, ist die Komponente Grafische Benutzeroberfläche (GUI) in der Liste der Komponenten des Installationspakets von Kaspersky Endpoint Security vorhanden.

Schutz vor bedrohlichen Dateien

Dieses Kontrollkästchen aktiviert/deaktiviert das Hinzufügen der Komponente „Schutz vor bedrohlichen Dateien“ zum Installationspaket für Kaspersky Endpoint Security.

Wenn dieses Kontrollkästchen aktiviert ist, ist die Komponente „Schutz vor bedrohlichen Dateien“ im Installationspaket für Kaspersky Endpoint Security enthalten.

Wenn dieses Kontrollkästchen deaktiviert ist, ist die Komponente „Schutz vor bedrohlichen Dateien“ nicht im Installationspaket für Kaspersky Endpoint Security enthalten.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schutz vor Web-Bedrohungen

Dieses Kontrollkästchen aktiviert/deaktiviert das Hinzufügen der Komponente „Schutz vor Web-Bedrohungen“ zum Installationspaket für Kaspersky Endpoint Security.

Wenn dieses Kontrollkästchen aktiviert ist, ist die Komponente „Schutz vor Web-Bedrohungen“ im Installationspaket für Kaspersky Endpoint Security enthalten.

Wenn dieses Kontrollkästchen deaktiviert ist, ist die Komponente „Schutz vor Web-Bedrohungen“ nicht im Installationspaket für Kaspersky Endpoint Security enthalten.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schutz vor Netzwerkbedrohungen

Dieses Kontrollkästchen aktiviert/deaktiviert das Hinzufügen der Komponente „Schutz vor Netzwerkbedrohungen“ zum Installationspaket für Kaspersky Endpoint Security.

Wenn dieses Kontrollkästchen aktiviert ist, ist die Komponente „Schutz vor Netzwerkbedrohungen“ im Installationspaket für Kaspersky Endpoint Security enthalten.

Wenn dieses Kontrollkästchen deaktiviert ist, ist die Komponente „Schutz vor Netzwerkbedrohungen“ nicht im Installationspaket für Kaspersky Endpoint Security enthalten.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Administrationsagent-Connector

Dieses Kontrollkästchen fügt die Komponente „Administrationsagent-Connector“ zum Installationspaket für Kaspersky Endpoint Security hinzu.

Wenn das Kontrollkästchen aktiviert ist, ist die Komponente Grafische Benutzeroberfläche (GUI) in der Liste der Komponenten des Installationspakets von Kaspersky Endpoint Security vorhanden.

Fenster „Lizenzinformationen“

Im Fenster **Lizenzinformationen** können Sie Informationen über eine Lizenz anzeigen. Dazu gehören: Ablaufdatum, Anzahl der Computer, auf denen Kaspersky Endpoint Security im Rahmen dieser Lizenz genutzt werden darf, und Lizenztyp.

Als Reserveschlüssel hinzufügen

Dieses Kontrollkästchen aktiviert/deaktiviert das Hinzufügen einer bestimmten Schlüsseldatei oder eines Aktivierungscodes als Reserveschlüssel.

Wenn dieses Kontrollkästchen aktiviert ist, fügt Kaspersky Endpoint Security die angegebene Schlüsseldatei oder den Aktivierungscode als Reserveschlüssel hinzu.

Wenn das Kontrollkästchen deaktiviert ist, fügt Kaspersky Endpoint Security die angegebene Schlüsseldatei oder den Aktivierungscode als aktiven Schlüssel hinzu.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster „Virensuche“

Untersuchungsbereich

Dieser Link öffnet ein Fenster, in dem Sie den Untersuchungsbereich erstellen können.

Im Abschnitt **Beim Erkennen eines schädlichen Objekts** können Sie auswählen, welche Aktion Kaspersky Endpoint Security beim Fund eines infizierten Objekts ausführen soll.

Nach Abschluss der Untersuchung Aktion erfragen

Kaspersky Endpoint Security verarbeitet Objekte erst nach Abschluss der Untersuchung. An diesem Punkt zeigt Kaspersky Endpoint Security eine Benachrichtigung mit Informationen über jedes infizierte Objekt an und fordert den Benutzer auf, über das weitere Vorgehen zu entscheiden. Die verfügbaren Optionen sind vom Objekttyp abhängig.

Diese Variante ist standardmäßig ausgewählt.

Während der Untersuchung Aktion erfragen

Kaspersky Endpoint Security zeigt eine Benachrichtigung mit Informationen über jedes von der Anwendung gefundene infizierte Objekt an und fordert den Benutzer auf, über das weitere Vorgehen zu entscheiden. Die verfügbaren Optionen sind vom Objekttyp abhängig.

Aktion nicht erfragen

Kaspersky Endpoint Security protokolliert Informationen über erkannte Objekte, ohne die gefundenen Objekte zu bearbeiten.

Automatisch desinfizieren

Dieses Kontrollkästchen aktiviert/deaktiviert die Desinfektion von infizierten Objekten, die Kaspersky Endpoint Security gefunden hat, wobei der Benutzer nicht nach Bestätigung gefragt wird.

Wenn dieses Kontrollkästchen aktiviert ist, werden infizierte Objekte automatisch von Kaspersky Endpoint Security desinfiziert.

Wenn dieses Kontrollkästchen deaktiviert ist, überspringt Kaspersky Endpoint Security die infizierten Objekte.

Das Kontrollkästchen ist verfügbar, wenn die Variante **Aktion nicht erfragen** ausgewählt ist.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Desinfizieren – Löschen, wenn Desinfektion fehlschlägt

Dieses Kontrollkästchen aktiviert/deaktiviert die Löschung von infizierten und möglicherweise infizierten Objekten, wenn ein Desinfektionsversuch erfolglos war.

Wenn dieses Kontrollkästchen aktiviert ist, werden infizierte Objekte, die nicht desinfiziert werden konnten, automatisch von Kaspersky Endpoint Security gelöscht.

Wenn dieses Kontrollkästchen deaktiviert ist, werden infizierte Dateien, die nicht desinfiziert werden konnten, nicht von Kaspersky Endpoint Security gelöscht.

Dieses Kontrollkästchen wird angezeigt, wenn die Option **Aktion nicht erfragen** ausgewählt ist und das Kontrollkästchen **Automatisch desinfizieren** aktiviert ist.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Dateitypen** können Sie das Format der Dateien auswählen, die Kaspersky Endpoint Security untersuchen soll.

Alle Dateien untersuchen

Kaspersky Endpoint Security untersucht alle Objekte, die im Dateisystem ausgeführt, geöffnet und gespeichert werden.

Anwendungen und Dokumente nach Inhalt untersuchen

Kaspersky Endpoint Security untersucht nur jene Objekte, die aufgrund des Dateiformats als infizierbar gelten.

Die Liste der Dateiformate wird von Kaspersky erstellt und ist Teil der Kaspersky Endpoint Security-Datenbanken.

Anwendungen und Dokumente nach Erweiterung untersuchen

Kaspersky Endpoint Security untersucht nur jene Objekte, die aufgrund der Dateierweiterung als infizierbar gelten.

Die Liste der Dateierweiterungen wird von Kaspersky erstellt und ist Teil der Kaspersky Endpoint Security-Datenbanken.

Dateien ohne Erweiterung werden von Kaspersky Endpoint Security immer untersucht.

Im Abschnitt **Optimierung** können Sie die Leistungseinstellungen der Untersuchungen konfigurieren.

Nur neue und veränderte Dateien untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert einen Untersuchungsmodus, in dem nur die Dateien untersucht werden, die von Kaspersky Endpoint Security als neu oder als seit der vorherigen Untersuchung verändert eingestuft werden.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security nur die Dateien, die als neu oder als seit der vorherigen Untersuchung verändert gelten.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security alle Dateien.

Schreibgeschütztes Systemvolume bei der Untersuchung überspringen

Dieses Kontrollkästchen deaktiviert/aktiviert in Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume. Dadurch wird die Untersuchungsdauer erheblich verkürzt.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security das schreibgeschützte Systemvolume.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Überspringen, wenn die Datei größer ist als MB

Dieses Kontrollkästchen aktiviert/deaktiviert einen Modus, in dem Dateien, welche die festgelegte Größe überschreiten, von der Untersuchung ausgeschlossen werden.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security Dateien, wenn deren Größe die festgelegte Dateigröße überschreitet.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Dateien unabhängig von der Dateigröße.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Standardmäßig ist die Größe auf 100 MB festgelegt.

Überspringen, wenn die Untersuchung länger dauert als Sek.

Dieses Kontrollkästchen aktiviert/deaktiviert eine Begrenzung für die Untersuchungsdauer von Dateien. Kaspersky Endpoint Security überspringt eine Datei, wenn ihre Untersuchung die festgelegte Begrenzung überschreitet.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security eine Datei, wenn ihre Untersuchung die festgelegte Dauer überschreitet.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Dateien unabhängig von der Untersuchungsdauer.

Standardmäßig ist ein Wert von 30 Sekunden eingestellt.

Im Abschnitt **Zusammengesetzte Dateien** können Sie den Typ der zusammengesetzten Dateien auswählen, die Kaspersky Endpoint Security untersuchen soll.

Archive untersuchen

Mit diesem Kontrollkästchen wird die Untersuchung von Archiven aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, werden Archive von Kaspersky Endpoint Security untersucht.

Wenn das Kontrollkästchen deaktiviert ist, werden Archive bei der Untersuchung übersprungen.

Alle

Kaspersky Endpoint Security untersucht alle Archive.

Diese Option ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** aktiviert ist.

Nur neue

Kaspersky Endpoint Security untersucht nur neue Archive.

Diese Option ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** aktiviert ist.

Kennwortgeschützte Archive untersuchen

Mit diesem Kontrollkästchen wird die Untersuchung von kennwortgeschützten Archiven aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, werden kennwortgeschützte Archive von Kaspersky Endpoint Security untersucht.

Wenn dieses Kontrollkästchen deaktiviert ist, werden kennwortgeschützte Archive bei der Untersuchung übersprungen.

Eingebettete OLE-Objekte untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Objekten, die in Dateien eingebettet sind (z. B. Excel-Tabellen, Makros oder E-Mail-Anhänge).

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security eingebettete OLE-Objekte.

Wenn dieses Kontrollkästchen deaktiviert ist, werden eingebettete OLE-Objekte bei der Untersuchung übersprungen.

Alle

Kaspersky Endpoint Security untersucht alle OLE-Objekte.

Diese Option ist verfügbar, wenn das Kontrollkästchen **Eingebettete OLE-Objekte untersuchen** aktiviert ist.

Nur neue

Kaspersky Endpoint Security untersucht nur neue eingebettete OLE-Objekte.

Diese Option ist verfügbar, wenn das Kontrollkästchen **Eingebettete OLE-Objekte untersuchen** aktiviert ist.

Dateien in Mailformaten untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Mailformat-Dateien und E-Mail-Datenbanken.

Wenn dieses Kontrollkästchen aktiviert ist, werden Dateien in Mailformaten und E-Mail-Datenbanken von Kaspersky Endpoint Security untersucht.

Wenn dieses Kontrollkästchen deaktiviert ist, überspringt Kaspersky Endpoint Security Mailformat-Dateien und E-Mail-Datenbanken bei der Untersuchung.

Fenster „Untersuchungsbereich“

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie eine Datei, einen Ordner oder eine Datei-/Ordnermaske angeben können, die zum Untersuchungsbereich hinzugefügt werden sollen.

Löschen

Durch Klick auf diese Schaltfläche wird das Objekt aus dem Untersuchungsbereich gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben dem Objekt aktiviert ist.

Die Objekte, die standardmäßig zum Untersuchungsbereich gehören, können nicht gelöscht werden.

Untersuchungsbereich

Diese Spalte enthält die Objekte, die bei einer Schadsoftware-Untersuchung gescannt werden.

Status

Der Umschalter in dieser Spalte aktiviert/deaktiviert die Untersuchung der Objekte, die zum Untersuchungsbereich hinzugefügt werden.

Wenn der Umschalter aktiviert ist, untersucht Kaspersky Endpoint Security das entsprechende Objekt.

Wenn der Umschalter deaktiviert ist, untersucht Kaspersky Endpoint Security das entsprechende Objekt nicht.

Erweitert

Diese Spalte gibt an, ob Kaspersky Endpoint Security die Unterordner des entsprechenden Objekts untersucht.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Dialog „Untersuchungsbereich hinzufügen“

Dateiname, Ordnername oder Maske eingeben

Pfad zu einer Datei, einem Ordner oder zur Maske von Datei/Ordner.

Dieses Objekt ist ein Ordner

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung eines Objekts als einen Ordner.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security das Objekt, das Sie im Feld **Dateiname, Ordnername oder Maske eingeben** als Ordner angegeben haben.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security das Objekt, das Sie im Feld **Dateiname, Ordnername oder Maske eingeben** als eine Datei angegeben haben.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Unterordner einschließen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung der Unterordner des Ordners, der im Eingabefeld **Dateiname, Ordnername oder Maske eingeben** angegeben ist.

Ist dieses Kontrollkästchen aktiviert, werden untergeordnete Ordner bei Malware-Untersuchungen von Kaspersky Endpoint Security untersucht.

Ist dieses Kontrollkästchen deaktiviert, scannt Kaspersky Endpoint Security bei Malware-Untersuchungen nur jene Dateien, die sich direkt in dem Ordner befinden, der im Feld **Dateiname, Ordnername oder Maske eingeben** angegeben ist.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Das Fenster „Dateiparameter“

Die folgenden Arten von Datei-Hashes werden unterstützt:

- **MD5**

  Ein Hash dieses Typs muss 32 Zeichen umfassen und die Zeichen 0-9, a-f und A-F enthalten.

- **SHA256**

  Ein Hash dieses Typs muss 64 Zeichen umfassen und die Zeichen 0-9, a-f und A-F enthalten.

Fenster „Netzwerk“

Im Abschnitt **Proxyserver-Einstellungen** können Sie die Verwendung eines Proxy-Servers und die Einstellungen zur Verbindung mit einem Proxy-Server konfigurieren.

Proxyserver nicht verwenden

Ist diese Option ausgewählt, so verwendet Kaspersky Endpoint Security keinen Proxy-Server, um eine Verbindung zu den Quellen für das Update der Anwendungsdatenbanken und Module herzustellen.

Proxy-Einstellungen des Systems verwenden

Ist diese Option ausgewählt, so verwendet Kaspersky Endpoint Security die in Ihrem Betriebssystem festgelegten Proxy-Server-Einstellungen, um eine Verbindung zu den Quellen für das Update der Anwendungsdatenbanken und Module herzustellen.

Diese Variante ist standardmäßig ausgewählt.

Folgende Proxy-Einstellungen verwenden

Ist diese Option ausgewählt, so verwendet Kaspersky Endpoint Security die von Ihnen angegebenen Proxy-Server-Einstellungen, um eine Verbindung zu den Quellen für das Update der Anwendungsdatenbanken und Module herzustellen.

Adresse

IP-Adresse oder symbolischer Name eines Proxy-Servers.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Port

Portnummer für den Proxy-Server.

Standardmäßig wird Port 8080 verwendet.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Authentifizierung verwenden

Mit diesem Kontrollkästchen wird die Verwendung der Authentifizierung für die Verbindung mit einem Proxy-Server aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, verlangt Kaspersky Endpoint Security bei der Verbindung mit einem Proxy-Server die Anmeldedaten des Benutzers.

Wenn dieses Kontrollkästchen deaktiviert ist, verlangt Kaspersky Endpoint Security bei der Verbindung mit dem Proxy-Server keine Anmeldedaten des Benutzers.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Dieses Kontrollkästchen ist verfügbar, wenn die Variante **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Benutzername

Benutzername für die Verbindung mit dem Proxy-Server.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** und das Kontrollkästchen **Authentifizierung verwenden** aktiviert sind.

Kennwort

Kennwort für den angegebenen Benutzernamen.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** und das Kontrollkästchen **Authentifizierung verwenden** aktiviert sind.

Anzeigen

Bei Klick auf diese Schaltfläche ist das Kennwort sichtbar, das Sie im Feld **Kennwort** eingeben.

Für lokale Adressen keinen Proxyserver verwenden

Dieses Kontrollkästchen aktiviert/deaktiviert die Verwendung eines Proxy-Servers für den Fall, dass die Anwendungsdatenbanken und Module aus einem lokalen Ordner oder aus einem Netzwerkordner aktualisiert werden.

Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security keinen Proxy-Server, wenn die Datenbanken und Module der Anwendung aus einem lokalen Ordner oder aus einem Netzwerkordner aktualisiert werden.

Wenn dieses Kontrollkästchen deaktiviert ist, verwendet Kaspersky Endpoint Security einen Proxy-Server, wenn die Datenbanken und Module der Anwendung aus einem lokalen Ordner oder aus einem Netzwerkordner aktualisiert werden.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Dieses Kontrollkästchen ist verfügbar, wenn die Variante **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Im Abschnitt **Sichere Verbindungen untersuchen** können Sie festlegen, ob Kaspersky Endpoint Security sichere Verbindungen (HTTPS) untersuchen soll.

Sichere Verbindungen (HTTPS) untersuchen

Der Umschalter **Sichere Verbindungen (HTTPS) untersuchen** aktiviert/deaktiviert die Untersuchung von sicheren Verbindungen, die über das HTTPS-Protokoll hergestellt werden, sowie die Anzeige von Benachrichtigungen, wenn die „Web-Kontrolle“ den Zugriff des Benutzers auf gefährliche Webressourcen blockiert.

Wenn der Umschalter **Sichere Verbindungen (HTTPS) untersuchen** aktiviert ist, geht Kaspersky Endpoint Security wie folgt vor:

- Der „Schutz vor Web-Bedrohungen“ untersucht die Daten, die mit dem HTTPS-Protokoll in Safari, Google Chrome und Firefox auf Ihren Computer gelangen oder von ihm gesendet werden.
- Die Anwendung zeigt Benachrichtigungen an, wenn der Benutzer auf Webressourcen zugreift, die von der Web-Kontrolle auf dem Remote-Computer blockiert werden.

Wenn der Umschalter **Sichere Verbindungen (HTTPS) untersuchen** deaktiviert ist, geht Kaspersky Endpoint Security wie folgt vor:

- Der „Schutz vor Web-Bedrohungen“ untersucht die auf Ihrem Computer über das HTTPS-Protokoll eingehenden bzw. von dem Computer ausgehenden Daten nicht.
- Die Anwendung zeigt keine Benachrichtigungen an, wenn der Benutzer auf Webressourcen zugreift, die von der Web-Kontrolle auf dem Remote-Computer blockiert werden.

Der Umschalter ist standardmäßig aktiviert.

Im Abschnitt **Wählen Sie den Zertifikatspeicher für Firefox aus** können Sie den Zertifikatspeicher für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Browser Mozilla Firefox auswählen.

Schlüsselbund "System Roots" (empfohlen)

Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Browser Mozilla Firefox ein Stammzertifikat aus dem Schlüsselbund „System Roots“.

Diese Variante ist standardmäßig ausgewählt.

Zertifikatspeicher aus den Mozilla Firefox-Einstellungen

Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security das Zertifikat aus dem Zertifikatspeicher des Browsers.

In diesem Fall müssen Sie das Kaspersky Endpoint Security-Zertifikat manuell zum Zertifikatspeicher des Browsers Mozilla Firefox hinzufügen. Weitere Informationen finden Sie unter So fügen Sie das Kaspersky-Zertifikat zum Zertifikatspeicher von Mozilla Firefox hinzu.

Im Abschnitt **Vertrauenswürdige Stammzertifikate** können Sie die Liste der vertrauenswürdigen Stammzertifikate verwalten.

Vertrauenswürdige Stammzertifikate verwalten

Durch Klick auf diesen Link wird ein Fenster geöffnet. Dort können Sie eine Liste mit vertrauenswürdigen Stammzertifikaten erstellen, um eine Verbindung zu den entsprechenden Servern herzustellen, ohne dabei Benachrichtigungen zu erhalten.

Im Abschnitt **Überwachte Ports** können Sie festlegen, welche Ports durch Kaspersky Endpoint Security überwacht werden sollen.

Ausgewählte Ports

Dieser Link öffnet ein Fenster, in dem Sie eine Liste mit Ports erstellen können, die von Kaspersky Endpoint Security überwacht werden sollen.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Vertrauenswürdige Stammzertifikate verwalten“

Hinzufügen

Ein Klick auf diese Schaltfläche öffnet einen Dialog. Dort können Sie Zertifikate hinzufügen, die als vertrauenswürdig gelten sollen.

Löschen

Bei Klick auf diese Schaltfläche wird das ausgewählte Zertifikat aus der Liste für vertrauenswürdige Zertifikate gelöscht.

Liste der vertrauenswürdigen Zertifikate

Eine Liste mit den Namen der vertrauenswürdigen Stammzertifikate.

Die Liste ist standardmäßig leer.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Überwachte Ports“

Liste der überwachten Ports

Liste der Ports, für welche Sie die Überwachung der übertragenen Daten anpassen können.

Die Portliste enthält standardmäßig jene Ports, die von gängigen Diensten häufig verwendet werden.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie einen Port hinzufügen können, der von Kaspersky Endpoint Security überwacht werden soll.

Löschen

Mit dieser Schaltfläche wird der ausgewählte Port aus der Liste gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben dem Port aktiviert ist.

Port

Diese Liste enthält die Portnummern.

Status

Diese Spalte enthält einen Umschalter, der den Überwachungsstatus für die Daten angibt, die über diesen Port übertragen werden.

Der Status **Überwacht** bedeutet, dass der Datenverkehr, der über den entsprechenden Port übertragen wird, durch Kaspersky Endpoint Security untersucht wird.

Der Status **Nicht überwacht** bedeutet, dass der Datenverkehr, der über den entsprechenden Port übertragen wird, von Kaspersky Endpoint Security nicht untersucht wird.

Beschreibung

Diese Liste enthält eine Beschreibung des Ports.

Dialog „Port hinzufügen“

Eingabefeld für einen Port

Nummer eines Ports, für den Kaspersky Endpoint Security die übermittelten Daten überwachen soll.

Eingabefeld für eine Beschreibung

Zusatzinformationen über den Port, z. B. Porttyp.

Fenster „Vertrauenswürdige Zone“: Abschnitt „Dateien und Ordner“

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie eine Datei oder einen Ordner zur „Vertrauenswürdigen Zone“ hinzufügen können.

Löschen

Durch Klick auf diese Schaltfläche wird eine ausgewählte Datei oder ein Ordner aus der Ausnahmeliste gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Datei oder dem Ordner aktiviert ist.

Datei oder Ordner

Diese Spalte enthält die Dateien oder Ordner, die zur vertrauenswürdigen Zone hinzugefügt werden.

Status

Der Umschalter in dieser Spalte aktiviert/deaktiviert die Untersuchung der Datei oder des Ordners, die zur vertrauenswürdigen Zone hinzugefügt werden.

Wenn der Umschalter aktiviert ist, untersucht Kaspersky Endpoint Security die entsprechende Datei oder den Ordner nicht.

Wenn der Umschalter deaktiviert ist, untersucht Kaspersky Endpoint Security die entsprechende Datei oder den Ordner.

Kommentar

Informationen über die Datei oder den Ordner, die zur vertrauenswürdigen Zone hinzugefügt werden.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Ausnahme hinzufügen“

Eingabefeld „Geben Sie den Dateinamen, den Ordnernamen oder die Maske ein“

Pfad zu einer Datei, einem Ordner oder zur Maske einer Datei/eines Ordners, die bzw. der aus dem Schutzbereich ausgeschlossen werden sollen.

Unterordner einschließen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung der Unterordner jenes Ordners, der im Feld **Dateiname, Ordnername oder Maske eingeben** angegeben ist.

Ist dieses Kontrollkästchen aktiviert, werden untergeordnete Ordner des betreffenden Ordners bei Malware-Untersuchungen nicht von Kaspersky Endpoint Security untersucht.

Wenn dieses Kontrollkästchen deaktiviert ist, schließt Kaspersky Endpoint Security bei Schadsoftware-Untersuchungen nur jene Dateien aus, die sich direkt in dem Ordner befinden, der im Feld **Dateiname, Ordnername oder Maske eingeben** angegeben ist. Untergeordnete Ordner des angegebenen Ordners werden untersucht.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Komponenten** können Sie auswählen, welche Komponenten die angegebene Datei oder den Ordner nicht untersuchen sollen.

Beliebig

Die Komponenten „Untersuchung“ und „Schutz vor bedrohlichen Dateien“ untersuchen die angegebene Datei oder der Ordner nicht.

Aus der Liste

Mit dieser Option können Sie die Komponenten auswählen.

Schutz vor bedrohlichen Dateien

Wenn dieses Kontrollkästchen aktiviert ist, untersucht die Komponente „Schutz vor bedrohlichen Dateien“ die angegebene Datei oder der Ordner nicht.

Dieses Kontrollkästchen ist verfügbar, wenn die Option **Aus der Liste** ausgewählt ist.

Untersuchung

Wenn dieses Kontrollkästchen aktiviert ist, untersucht die Komponente „Untersuchung“ die angegebene Datei oder der Ordner nicht.

Dieses Kontrollkästchen ist verfügbar, wenn die Option **Aus der Liste** ausgewählt ist.

Eingabefeld „Kommentar“

Informationen über die Datei oder den Ordner, die zur vertrauenswürdigen Zone hinzugefügt werden.

Im Abschnitt **Status** können Sie angeben, ob die Ausnahme aktiv oder inaktiv ist.

Deaktiviert

Kaspersky Endpoint Security untersucht die entsprechende Datei oder den Ordner.

Aktiviert

Kaspersky Endpoint Security untersucht die entsprechende Datei oder den Ordner nicht.

Fenster „Vertrauenswürdige Zone“: Abschnitt „Vertrauenswürdige Anwendungen“

Liste der vertrauenswürdigen Anwendungen

Liste der vertrauenswürdigen Anwendungen, deren Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie den Pfad einer Anwendung eingeben können, deren Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht werden soll.

Löschen

Mit dieser Schaltfläche wird die ausgewählte vertrauenswürdige Anwendung aus der Liste gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der vertrauenswürdigen Anwendung aktiviert ist.

Anwendung

Diese Spalte enthält den Anwendungsnamen oder das letzte Segment des Pfads zur Anwendung.

Status

Diese Spalte enthält einen Umschalter, der den Überwachungsstatus für die Netzwerkaktivität einer Anwendung angibt.

Der Status **Aktiviert** bedeutet, dass die Netzwerkaktivität der entsprechenden Anwendung nicht von Kaspersky Endpoint Security überwacht wird.

Der Status **Deaktiviert** bedeutet, dass die Netzwerkaktivität der entsprechenden Anwendung durch Kaspersky Endpoint Security überwacht wird.

Pfad

Diese Spalte enthält den Anwendungspfad auf dem Client-Computer, den Sie manuell hinzufügen.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Anwendung hinzufügen“

Eingabefeld für einen Pfad

Pfad einer Anwendung, deren Netzwerk- oder Dateiaktivität nicht von Kaspersky Endpoint Security überwacht werden soll.

Anforderung an die Codesignatur

Anforderungen an die Codesignatur des Programms, dessen Aktivität nicht von Kaspersky Endpoint Security überwacht wird.

Dieser Parameter ist optional.

Optionen

Wählen Sie in diesem Abschnitt die Arten der Aktivitäten aus, die Kaspersky Endpoint Security nicht überwachen soll.

Dateiaktivität nicht überwachen

Dieses Kontrollkästchen aktiviert/deaktiviert die Überwachung der Vorgänge einer Anwendung mit Dateien auf einem Client-Computer.

Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security die Dateiaktivität der Anwendung nicht.

Wenn dieses Kontrollkästchen deaktiviert ist, überwacht Kaspersky Endpoint Security die Dateiaktivität der Anwendung.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Netzwerkaktivität nicht überwachen

Dieses Kontrollkästchen aktiviert/deaktiviert die Überwachung des ein- und ausgehenden Internet-Datenverkehrs der Anwendung einem Client-Computer.

Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security die Netzwerkaktivität der Anwendung nicht.

Wenn dieses Kontrollkästchen deaktiviert ist, überwacht Kaspersky Endpoint Security die Netzwerkaktivität der Anwendung.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Der Abschnitt „Erweiterte Einstellungen“

Schutz

Dieser Link öffnet das Fenster **Schutz**. Dort können Sie allgemeine Einstellungen für Kaspersky Endpoint Security verwalten, wenn die Anwendung auf den Benutzercomputern installiert ist, und die Typen der Objekte auswählen, die Kaspersky Endpoint Security erkennen soll.

Berichte und Backup

Dieser Link öffnet das Fenster **Berichte und Backup**, in dem Sie die Einstellungen für Berichte und Backup verwalten können.

Interaktion mit dem Benutzer

Dieser Link öffnet das Fenster **Interaktion mit dem Benutzer**. Dort können Sie Einstellungen für die folgenden Funktionen vornehmen: Benachrichtigungen, die von Kaspersky Endpoint Security angezeigt werden, Anzeigesprache für die Ereignisse, die von Kaspersky Endpoint Security angezeigt werden, und weitere Einstellungen für Kaspersky Endpoint Security.

Netzwerk

Mit diesem Link wird das Fenster **Netzwerk** geöffnet, in dem Sie die Einstellungen des Proxy-Servers verwalten, die Untersuchung verschlüsselter Verbindungen (HTTPS) aktivieren oder deaktivieren, den Speicherort des Zertifikats für die Überprüfung des verschlüsselten HTTPS-Datenverkehrs im Browser Mozilla Firefox auswählen und die überwachten Ports konfigurieren können.

Vertrauenswürdige Zone

Dieser Link öffnet das Fenster **Vertrauenswürdige Zone**. Dort können Sie Ausnahmen für den Schutz vor bedrohlichen Dateien oder für Untersuchungsaufgaben hinzufügen und vertrauenswürdigen Programme konfigurieren.

Fenster „Schutz“

Im Abschnitt **Allgemein** können Sie den Schutz für Dateien auf einem Remote-Computer aktivieren oder deaktivieren. Außerdem kann hier festgelegt werden, dass das Programm automatisch gestartet werden soll, wenn der Computer eingeschaltet wird oder nachdem das Betriebssystem neu gestartet wurde.

App beim Hochfahren des Computers starten

Dieses Kontrollkästchen aktiviert/deaktiviert einen Modus, in dem Kaspersky Endpoint Security beim Einschalten des Remote-Computers oder nach dem Neustart seines Betriebssystems automatisch gestartet wird.

Wenn das Kontrollkästchen aktiviert ist, wird Kaspersky Endpoint Security automatisch gestartet, wenn der Remote-Computer eingeschaltet wird oder nachdem sein Betriebssystem neu gestartet wird.

Wenn das Kontrollkästchen deaktiviert ist, wird Kaspersky Endpoint Security nicht automatisch gestartet, wenn der Remote-Computer eingeschaltet wird oder nachdem sein Betriebssystem neu gestartet wird.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Wichtig: Wenn Sie dieses Kontrollkästchen aktivieren, während Kaspersky Endpoint Security nicht ausgeführt wird, werden die Änderungen erst übernommen, nachdem Sie die App lokal oder über Kaspersky Security Center gestartet haben.

Schutz aktivieren

Das Kontrollkästchen aktiviert/deaktiviert den Schutz für einen Remote-Computer, auf dem Kaspersky Endpoint Security installiert ist.

Wenn dieses Kontrollkästchen aktiviert ist, ist der Schutz des Remote-Computers eingeschaltet.

Wenn dieses Kontrollkästchen deaktiviert ist, ist der Schutz des Remote-Computers ausgeschaltet.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Typen der zu erkennenden Objekte** können Sie Objekttypen auswählen, die Kaspersky Endpoint Security erkennen soll.

Viren, Würmer, Trojaner, schädliche Tools, Adware und Dialer

Dieses Kontrollkästchen aktiviert/deaktiviert die Erkennung der folgenden Programmtypen:

- Alle Typen von Schadsoftware
- Anwendungen, die auf Ihrem Computer Werbung (z. B. Banner) anzeigen oder die Suchergebnisse in Ihrem Browser durch Websites mit Werbung ersetzen
- Anwendungen, die heimlich Telefonverbindungen über ein Computermodem herstellen

Wenn das Kontrollkästchen aktiviert ist, ist die Komponente Grafische Benutzeroberfläche (GUI) in der Liste der Komponenten des Installationspakets von Kaspersky Endpoint Security vorhanden.

Legale Software, mit der Angreifer den Benutzercomputer oder persönliche Daten beschädigen können

Dieses Kontrollkästchen aktiviert/deaktiviert die Erkennung von Anwendungen, die zwar nicht als schädlich oder gefährlich gelten, die aber unter bestimmten Umständen dazu verwendet werden können, um den Benutzercomputer zu beschädigen.

Wenn das Kontrollkästchen aktiviert ist, erkennt Kaspersky Endpoint Security legale Software, mit der Angreifer den Benutzercomputer oder persönliche Daten beschädigen können.

Wenn das Kontrollkästchen deaktiviert ist, erkennt Kaspersky Endpoint Security legale Software nicht, mit der Angreifer den Benutzercomputer oder persönliche Daten beschädigen können.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Im Abschnitt **Erweitert** kann der Stromsparmodus aktiviert werden.

Geplante Aufgaben bei Akkubetrieb überspringen

Dieses Kontrollkästchen aktiviert/deaktiviert den Start von geplanten Untersuchungsaufgaben auf Computern, die im Akkubetrieb laufen.

Wenn dieses Kontrollkästchen aktiviert ist, werden geplante Untersuchungsaufgaben von Kaspersky Endpoint Security auf Computern, die im Akkubetrieb laufen, nicht gestartet.

Wenn dieses Kontrollkästchen deaktiviert ist, startet Kaspersky Endpoint Security geplante Untersuchungsaufgaben auf Computern, die im Akkubetrieb laufen.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Maximale CPU-Last für Untersuchungen

Kaspersky Endpoint Security beschränkt die CPU-Nutzung des geschützten Geräts bei On-Demand-Untersuchungsaufgaben auf den Wert, der im entsprechenden Feld angegeben ist.

Die Aktivierung dieser Option kann sich negativ auf die Leistung von Kaspersky Endpoint Security auswirken.

Diese Option ist standardmäßig deaktiviert.

Obergrenze (in Prozent)

Maximal zulässige CPU-Nutzung durch Kaspersky Endpoint Security für Untersuchungsaufgaben.

Das Eingabefeld ist verfügbar, wenn die Option **Maximale CPU-Last für Untersuchungen** ausgewählt ist.

Hinweis: Dies ist ein kumulativer Grenzwert über alle CPU-Kerne. Die im Aktivitätsmonitor angezeigte CPU-Auslastung ist die Summe der Auslastung jedes CPU-Kerns und kann daher 100 Prozent überschreiten.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Berichte und Backup“

Im Abschnitt **Berichte** können Sie die Einstellungen für das Erstellen und Speichern von Berichten über die Ereignisse anpassen, die in Kaspersky Endpoint Security auftreten.

Berichte löschen nach Tagen

Mit diesem Kontrollkästchen wird ein Modus aktiviert/deaktiviert, in dem Berichte nach einem festgelegten Zeitraum gelöscht werden.

Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Endpoint Security die Berichte nach einem festgelegten Zeitraum. Standardmäßig werden Berichte für 30 Tage aufbewahrt.

Wenn das Kontrollkästchen deaktiviert ist, bewahrt Kaspersky Endpoint Security die Berichte unbefristet auf.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Nicht-kritische Ereignisse protokollieren

Dieses Kontrollkästchen aktiviert/deaktiviert die Protokollierung von nicht-kritischen Ereignissen (z. B. informative Ereignisse). Nicht-kritische Ereignisse haben keinen Einfluss auf den Schutz.

Wenn dieses Kontrollkästchen aktiviert ist, protokolliert Kaspersky Endpoint Security informative Ereignisse.

Wenn dieses Kontrollkästchen deaktiviert ist, werden informative Ereignisse nicht protokolliert.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Nur aktuelle Ereignisse beibehalten

Dieses Kontrollkästchen aktiviert/deaktiviert einen Modus, in dem nur wichtige Ereignisse über die vorhergehende Ausführung der Aufgabe beibehalten werden.

Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Endpoint Security bei jedem Aufgabenstart die Informationen über nicht-kritische Ereignisse aus der vorhergehenden Ausführung der Aufgabe, während wichtige Informationen (beispielsweise über gefundene Schadsoftware) im Bericht verbleiben.

Wenn dieses Kontrollkästchen deaktiviert ist, bewahrt Kaspersky Endpoint Security alle Informationen über die vorhergehende Ausführung der Aufgabe auf.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Im Abschnitt **Backup** können Sie festlegen, wie lange Objekte im Backup aufbewahrt werden sollen.

Objekte löschen nach Tagen

Mit diesem Kontrollkästchen wird ein Modus aktiviert/deaktiviert, in dem Objekte nach einem festgelegten Zeitraum aus dem Backup gelöscht werden.

Wenn dieses Kontrollkästchen aktiviert ist, werden Objekte nach dem festgelegten Zeitraum aus dem Backup gelöscht. Die standardmäßige Speicherdauer beträgt 30 Tage.

Wenn dieses Kontrollkästchen deaktiviert ist, bewahrt Kaspersky Endpoint Security die Objekte unbefristet im Backup auf.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Interaktion mit dem Benutzer“

Im Abschnitt **Anwendungsoberfläche** können Sie festlegen, ob das Anwendungssymbol in der Menüleiste auf einem Remote-Computer angezeigt werden soll und ob ein Benutzer das Hauptfenster von Kaspersky Endpoint Security öffnen und die Anwendungsoberfläche verwenden darf.

App-Symbol in der Menüleiste anzeigen

Dieses Kontrollkästchen aktiviert/deaktiviert die Anzeige des Anwendungssymbols in der Menüleiste eines Remote-Computers.

Wenn dieses Kontrollkästchen aktiviert ist, wird das Anwendungssymbol in der Menüleiste angezeigt.

Wenn das Kontrollkästchen deaktiviert ist, wird das Anwendungssymbol nicht in der Menüleiste angezeigt.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Benutzer darf die App öffnen

Dieses Kontrollkästchen aktiviert/deaktiviert für einen Benutzer die Möglichkeit, das Hauptfenster von Kaspersky Endpoint Security zu öffnen und die Anwendungsoberfläche auf einem Remote-Computer zu verwenden.

Wenn dieses Kontrollkästchen aktiviert ist, kann ein Benutzer das Hauptfenster von Kaspersky Endpoint Security öffnen und die Anwendungsoberfläche auf einem Remote-Computer verwenden.

Wenn dieses Kontrollkästchen deaktiviert ist, verhindert Kaspersky Endpoint Security, dass ein Benutzer das Hauptfenster öffnet und die Anwendungsoberfläche auf einem Remote-Computer verwendet.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Benachrichtigungen** können Sie Benachrichtigungen über Kaspersky Endpoint Security-Ereignisse aktivieren und die bevorzugte Benachrichtigungsmethode auswählen.

Benachrichtigungen

Der Umschalter **Benachrichtigungen** aktiviert/deaktiviert die Benachrichtigungen über Ereignisse in Kaspersky Endpoint Security.

Wenn der Umschalter **Benachrichtigungen** aktiviert ist, zeigt Kaspersky Endpoint Security Benachrichtigungen über Ereignisse an, die bei der Ausführung der Komponenten von Kaspersky Endpoint Security auftreten.

Wenn der Umschalter **Benachrichtigungen** deaktiviert ist, zeigt Kaspersky Endpoint Security keine Benachrichtigungen über Ereignisse an, die bei der Ausführung der Komponenten von Kaspersky Endpoint Security auftreten.

Der Umschalter ist standardmäßig aktiviert.

Benutzerbenachrichtigungen

Dieser Link öffnet ein Fenster, in dem Sie auswählen können, welche Benachrichtigungstypen für alle Ereignistypen verwendet werden sollen.

Im Abschnitt **Benutzer darf die App beenden** kann festgelegt werden, ob Kaspersky Endpoint Security vom Benutzer auf dem Remote-Computer deaktiviert werden kann.

"Beenden" im Kontextmenü der App anzeigen

Dieses Kontrollkästchen aktiviert/deaktiviert die Verfügbarkeit des Punktes **Beenden** im Kontextmenü des Anwendungssymbols, das sich in der Menüleiste befindet.

Wenn dieses Kontrollkästchen aktiviert ist, ist der Punkt **Beenden** im Kontextmenü des Anwendungssymbols verfügbar. Der Benutzer eines Remote-Computers kann Kaspersky Endpoint Security auf dem Remote-Computer beenden.

Wenn dieses Kontrollkästchen deaktiviert ist, ist der Punkt **Beenden** im Kontextmenü des Anwendungssymbols nicht verfügbar. Der Benutzer eines Remote-Computers kann Kaspersky Endpoint Security auf dem Remote-Computer nicht beenden.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Ereignisse in Kaspersky Security Center** kann ausgewählt werden, in welcher Sprache die Ereignisse für Kaspersky Endpoint Security in Kaspersky Security Center angezeigt werden sollen.

Anzeigesprache

Über die Dropdown-Liste können Sie die Anzeigesprache für Ereignisse von Kaspersky Endpoint Security in Kaspersky Security Center auswählen.

Im Abschnitt **Beschränkungen** können Sie erlauben, dass die Schlüssel und Updates für Kaspersky Endpoint Security auf einem Remote-Computer lokal verwaltet werden dürfen.

Lokale Update-Verwaltung durch den Benutzer erlauben

Mit diesem Kontrollkästchen wird die lokale Verwaltung der Updates für Kaspersky Endpoint Security auf einem Remote-Computer aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, ist die lokale Verwaltung der Updates für Kaspersky Endpoint Security auf einem Remote-Computer aktiviert.

Wenn dieses Kontrollkästchen deaktiviert ist, ist die Verwaltung der Updates für Kaspersky Endpoint Security auf einem Remote-Computer nur mithilfe des Verwaltungs-Plug-ins für Kaspersky Endpoint Security in Kaspersky Security Center möglich.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Lokale Schlüsselverwaltung durch den Benutzer erlauben

Mit diesem Kontrollkästchen wird die lokale Verwaltung von Schlüsseln für Kaspersky Endpoint Security auf einem Remote-Computer aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, können Sie die Schlüssel für Kaspersky Endpoint Security auf dem Remote-Computer lokal verwalten.

Wenn das Kontrollkästchen deaktiviert ist, ist die Verwaltung der Schlüssel für Kaspersky Endpoint Security auf dem Remote-Computer nur mithilfe des Verwaltungs-Plug-ins für Kaspersky Endpoint Security in Kaspersky Security Center möglich.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Kennwortschutz** können Sie ein Kennwort festlegen und konfigurieren, um unerwünschte Aktionen auf den Benutzergeräten einzuschränken.

Kennwortschutz

Der Umschalter **Kennwortschutz** aktiviert/deaktiviert den Kennwortschutz vor unerwünschten Aktionen auf den Benutzergeräten.

Wenn der Umschalter **Kennwortschutz** aktiviert ist, können Sie ein Kennwort festlegen und so konfigurieren, dass die Benutzer in ihren Aktionen auf ihren Geräten eingeschränkt werden.

Wenn der Umschalter **Kennwortschutz** deaktiviert ist, kann ein Benutzer eine unerwünschte Aktion ausführen, ohne ein Kennwort einzugeben.

Der Umschalter ist standardmäßig deaktiviert.

Bei Aktivieren dieses Umschalters wird ein Fenster geöffnet, in dem Sie das Kennwort konfigurieren, um unerwünschte Aktionen auf den Benutzergeräten einzuschränken.

Einstellungen

Bei Klick auf diese Schaltfläche wird ein Fenster geöffnet, in dem Sie das Kennwort konfigurieren, um unerwünschte Aktionen auf dem Benutzergerät einzuschränken.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Benutzerbenachrichtigungen“

Ereignisse

In dieser Spalte werden Ereignisse aufgelistet, die während der Ausführung von Kaspersky Endpoint Security auftreten können:

- **Kritische Ereignisse**. Ereignisse, die vorrangige Priorität für die Computersicherheit besitzen.
- **Funktionsfehler**. Ereignisse, die zur Funktionsuntüchtigkeit des Systems führen.
- **Wichtige Ereignisse**. Ereignisse, die der Benutzer bearbeiten muss.
- **Informative Ereignisse**. Ereignisse mit Informationscharakter.

Benachrichtigungen

Eine Benachrichtigung ist eine Pop-up-Meldung, die den Benutzer über ein Ereignis informiert.

Das Kontrollkästchen in der Spalte **Benachrichtigungen** aktiviert/deaktiviert Pop-up-Benachrichtigungen über die Ereignisse einer bestimmten Kategorie.

Signalton

Tonsignal, das sich auf ein Ereignis bezieht.

Das Kontrollkästchen in der Spalte **Signalton** aktiviert/deaktiviert Tonsignale für die Ereignisse einer bestimmten Kategorie.

Abschnitt „Update“

App-Module aktualisieren

Dieses Kontrollkästchen aktiviert/deaktiviert die Updates für Programm-Module. Die Anwendungsdatenbanken werden immer aktualisiert.

Wenn dieses Kontrollkästchen aktiviert ist, aktualisiert Kaspersky Endpoint Security die Programm-Module.

Wenn dieses Kontrollkästchen deaktiviert ist, aktualisiert Kaspersky Endpoint Security die Anwendungsmodule nicht.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Update-Quellen

Diese Liste enthält die Adressen von Ressourcen, von denen Kaspersky Endpoint Security die Updates für die Datenbanken und Module der Anwendung herunterlädt und installiert. Als Update-Quelle können Sie lokale Ordner oder Netzwerkordner, einen FTP- oder HTTP-Server festlegen.

Die Liste der Update-Quellen enthält standardmäßig die Kaspersky-Update-Server.

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Web Console verwalten, enthält die Liste der Update-Quellen standardmäßig auch die Server von Kaspersky Security Center.

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, enthält die Liste der Update-Quellen standardmäßig auch Verteilungspunkte. Ausführliche Informationen über Verteilungspunkte finden Sie in der Hilfe zu Kaspersky Security Center.

Die standardmäßigen Update-Quellen können nicht aus der Liste gelöscht werden.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie den Pfad eines lokalen Ordners oder eines Netzwerkordners, oder eine Webadresse angeben können, die zur Liste der Update-Quellen hinzugefügt werden sollen.

Löschen

Mit dieser Schaltfläche wird die ausgewähltes Update-Quelle aus der Liste gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Update-Quelle aktiviert ist.

Update-Quelle

Diese Spalte enthält die Update-Quellen für Kaspersky Endpoint Security.

Status

Wenn der Umschalter in dieser Spalte aktiviert ist, verwendet Kaspersky Endpoint Security die entsprechende Update-Quelle aus der Spalte **Update-Quelle**, um Updates zu empfangen.

Wenn der Umschalter in dieser Spalte deaktiviert ist, verwendet Kaspersky Endpoint Security die entsprechende Update-Quelle aus der Spalte **Update-Quelle** nicht, um Updates zu empfangen.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Update-Quelle hinzufügen“

Pfad eines lokalen Ordners oder Netzwerkordners, oder Webadresse eingeben

Adresse der Ressource, von der Kaspersky Endpoint Security Updates kopiert.

Als Adresse der Ressource können Sie den Pfad eines lokalen oder eines Netzwerkordners, die Webadresse oder IP-Adresse eines FTP- oder HTTP-Servers angeben.

Für die Webadresse eines FTP-Servers gilt das Format ftp://<Benutzername>:<Kennwort>@<Host>:<Port>.

Im Abschnitt **Status** können Sie festlegen, ob Kaspersky Endpoint Security die angegebene Webadresse als Update-Quelle verwenden soll.

Deaktiviert

Die Webadresse wird zur Liste der Update-Quellen hinzugefügt, aber Kaspersky Endpoint Security verwendet diese Webadresse nicht als Update-Quelle.

Aktiviert

Die Webadresse wird zur Liste der Update-Quellen hinzugefügt und Kaspersky Endpoint Security verwendet diese Webadresse als Update-Quelle.

Abschnitt „Datenverschlüsselung“

FileVault-Volume-Verschlüsselung

Der Umschalter **FileVault-Volume-Verschlüsselung** aktiviert/deaktiviert die Verwaltung der FileVault-Volume-Verschlüsselung.

Wenn der Umschalter **FileVault-Volume-Verschlüsselung** aktiviert ist, kann die FileVault-Volume-Verschlüsselung auf die Client-Computer von Kaspersky Security Center angewendet werden.

Wenn der Umschalter **FileVault-Volume-Verschlüsselung** deaktiviert ist, kann die FileVault-Volume-Verschlüsselung nicht auf die Client-Computer von Kaspersky Security Center angewendet werden.

Der Umschalter ist standardmäßig deaktiviert.

Hinweis: Wenn der Umschalter **FileVault-Volume-Verschlüsselung** aktivieren deaktiviert ist, können Benutzer mit Administratorrechten ihre Mac-Startvolumes von den Systemeinstellungen aus verschlüsseln und entschlüsseln. Weitere Informationen über FileVault finden Sie in der Apple-Dokumentation.

Volume verschlüsseln

Kaspersky Endpoint Security fragt die Anmeldedaten für die Client-Computer ab, auf welche die Richtlinie angewendet wird. Wenn der Benutzer die Anmeldedaten eingibt, startet Kaspersky Endpoint Security die Verschlüsselung des Startvolumes des Benutzers.

Wenn der Umschalter **FileVault-Volume-Verschlüsselung** aktiviert ist und die Option **Volume verschlüsseln** ausgewählt ist, können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen aus entschlüsseln.

Volume entschlüsseln

Kaspersky Endpoint Security fragt die Anmeldedaten für die Client-Computer ab, auf welche die Richtlinie angewendet wird. Wenn der Benutzer die Anmeldedaten eingibt, startet Kaspersky Endpoint Security die Entschlüsselung des Benutzer-Startvolumes.

Wenn der Umschalter **FileVault-Volume-Verschlüsselung** aktiviert ist und die Option **Volume entschlüsseln** ausgewählt ist, können Benutzer mit Administratorrechten ihr Mac-Startvolume nicht aus den Systemeinstellungen aus verschlüsseln.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Der Abschnitt „Detection and Response“

Managed Detection and Response

Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die Einstellungen für Managed Detection and Response konfigurieren können.

Endpoint Detection and Response

Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die Einstellungen für Endpoint Detection and Response konfigurieren können.

Endpoint Detection and Response (KATA)

Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die Einstellungen für Endpoint Detection and Response (KATA) konfigurieren können.

Das Fenster „Managed Detection and Response“

Managed Detection and Response

Über den Umschalter **Managed Detection and Response** wird die Komponente Managed Detection and Response aktiviert bzw. deaktiviert, die mit dem Dienst Kaspersky Managed Detection and Response interagiert. Dieser Dienst erkennt fortwährend Sicherheitsbedrohungen, die auf Ihr Unternehmen abzielen, und eliminiert sie.

Wenn der Umschalter **Managed Detection and Response** aktiviert und die MDR-Konfigurationsdatei importiert wird, ist die Komponente Managed Detection and Response aktiviert.

Wenn der Umschalter **Managed Detection and Response** deaktiviert wird, wird die Komponente Managed Detection and Response deaktiviert.

Der Umschalter ist standardmäßig deaktiviert.

Importieren

Über diese Schaltfläche öffnen Sie ein Fenster, über das Sie die MDR-Konfigurationsdatei in die Richtlinie für Kaspersky Endpoint Security importieren können.

Konfigurationsdatei löschen

Durch Klick auf diese Schaltfläche wird die MDR-Konfigurationsdatei aus der Kaspersky Endpoint Security-Richtlinie gelöscht.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Das Fenster „Endpoint Detection and Response“

Endpoint Detection and Response

Über den Schalter **Endpoint Detection and Response** wird die Komponente Endpoint Detection and Response aktiviert bzw. deaktiviert, die mit der Lösung Kaspersky Endpoint Detection and Response interagiert. Diese Lösung schützt Computer vor komplexen Bedrohungen, einschließlich neuen Exploits, Ransomware und dateilosen Angriffen.

Wenn der Schalter **Endpoint Detection and Response** aktiviert ist, ist die Komponente Endpoint Detection and Response aktiviert.

Wenn der Schalter **Endpoint Detection and Response** deaktiviert ist, ist die Komponente Endpoint Detection and Response deaktiviert.

Der Umschalter ist standardmäßig deaktiviert.

Im Abschnitt **Netzwerkisolation** können Sie Einstellungen für die Isolation von Computern vom Netzwerk anpassen. Diese Einstellungen gelten beim Fund eines Kompromittierungsindikators.

Einstellungen für das Aufheben der Netzwerkisolation von Computern konfigurieren

Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie eine Verzögerung für die automatische Deaktivierung der Netzwerkisolation festlegen können.

Ausnahmen

Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie Netzwerkverbindungen angeben können, die auf dem Computer nicht blockiert werden sollen, nachdem die Netzwerkisolation automatisch aktiviert wurde.

Im Abschnitt **Ausführungsprävention** können Sie die Einstellungen für das Ausführen von ausführbaren Dateien und Skripten sowie für das Öffnen von Dateien im Office-Format konfigurieren.

Ausführungsprävention

Der Schalter **Ausführungsprävention** aktiviert bzw. deaktiviert die Ausführungsprävention.

Wenn der Schalter **Ausführungsprävention** aktiviert ist, können Sie eine Liste mit Regeln für die Ausführungsprävention erstellen und bearbeiten und eine Aktion auswählen, die ausgeführt werden soll, wenn verbotene Objekte ausgeführt oder geöffnet werden.

Wenn der Schalter **Ausführungsprävention** deaktiviert ist, können Sie die Objekte, die Benutzer auf ihren Geräten ausführen oder öffnen, nicht verwalten.

Der Umschalter ist standardmäßig deaktiviert.

Aktion beim Ausführen oder Öffnen eines verbotenen Objekts

Blockieren und protokollieren

Wenn dieser Modus ausgewählt ist, blockiert das Programm die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Zusätzlich veröffentlicht die Anwendung im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über Versuche, Objekte zu starten oder Dokumente zu öffnen.

Nur Ereignisse protokollieren

Wenn dieser Modus ausgewählt ist, veröffentlicht Kaspersky Endpoint Security im Ereignisprotokoll von Kaspersky Security Center und im vereinheitlichten Protokollsystem ein Ereignis über den Start von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Allerdings wird das Starten oder Öffnen des Objekts nicht blockiert. Diese Variante ist standardmäßig ausgewählt.

Hinzufügen

Wenn Sie auf diese Schaltfläche klicken, wird ein Dialog geöffnet, in dem Sie eine neue Regel für die Ausführungsprävention erstellen können.

Bearbeiten

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie eine vorhandene Präventionsregel für die Ausführung bearbeiten können.

Diese Schaltfläche ist verfügbar, wenn in der Regelliste eine Regel ausgewählt ist.

Löschen

Mit dieser Schaltfläche wird die ausgewählte Ausführungspräventionsregel aus der Regelliste gelöscht.

Diese Schaltfläche ist verfügbar, wenn in der Regelliste eine Regel ausgewählt ist.

Im Abschnitt **Einstellungen der Cloud Sandbox** können Sie die Komponente Cloud Sandbox aktivieren oder deaktivieren.

Cloud Sandbox

Der Schalter **Cloud Sandbox** aktiviert bzw. deaktiviert die Cloud Sandbox-Technologie, die komplexe Bedrohungen auf einem Computer erkennen kann. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox" weiter. „Cloud Sandbox" führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivität zu erkennen, und entscheidet dann über ihre Reputation. Daten über diese Dateien werden an Kaspersky Security Network gesendet. Wenn Cloud Sandbox eine bösartige Datei erkennt, führt Kaspersky Endpoint Security die entsprechende Aktion aus, um die Bedrohung auf allen Computern zu entfernen, auf denen diese Datei gefunden wurde.

Wenn der Schalter **Cloud Sandbox** aktiviert ist, ist die Cloud Sandbox-Technologie aktiviert.

Wenn der Schalter **Cloud Sandbox** deaktiviert ist, ist die Cloud Sandbox-Technologie deaktiviert.

Der Umschalter ist standardmäßig deaktiviert.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Das Fenster mit Einstellungen zum Entsperren von Computern

Isolation des Computers automatisch aufheben nach

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die automatische Deaktivierung der Netzwerkisolation nach einem bestimmten Zeitraum.

Wenn dieses Kontrollkästchen aktiviert ist, können Sie die Verzögerung für die automatische Deaktivierung der Netzwerkisolation eines Computers festlegen.

Wenn das Kontrollkästchen deaktiviert ist, deaktiviert Kaspersky Endpoint Security die Netzwerkisolation 8 Stunden nach Beginn der Isolation.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Stunden

Intervall, nach dem die Netzwerkisolation automatisch deaktiviert wird.

Dieses Feld kann nur bearbeitet werden, wenn das Kontrollkästchen **Isolation des Computers automatisch aufheben nach** aktiviert ist.

Das Fenster Ausnahmen für die Netzwerkisolation

Ausnahmen für die Netzwerkisolation

Diese Liste enthält die Netzwerkverbindungen, die Sie als Ausnahmen für die Netzwerkisolation hinzugefügt haben.

Hinzufügen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Einstellungen der Netzwerkverbindung, die als Ausnahme hinzugefügt werden soll, manuell festlegen können.

Aus Profil hinzufügen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie Standard-Netzwerkprofile für die Konfiguration von Ausnahmen auswählen können.

Löschen

Wenn Sie auf diese Schaltfläche klicken, wird eine Netzwerkverbindung aus der Liste der Ausnahmen für die Netzwerkisolation entfernt.

Diese Schaltfläche ist verfügbar, wenn in der Liste der Ausnahmen für die Netzwerkisolation eine Verbindung ausgewählt ist.

Das Fenster mit den Regeloptionen

Regelname

Name einer Ausnahmeregel für die Netzwerkisolation.

Diese Einstellung ist optional.

Richtung

Richtung des Datenverkehrs.

Protokoll

Protokolltyp.

Nummer

Protokollnummer.

Der Wert muss der IANA-Liste für Internetprotokollnummern entsprechen.

Dieses Feld ist verfügbar, wenn der Protokolltyp **Benutzerdefiniert** ausgewählt ist.

Lokaler Port oder Bereich

Lokaler Port oder Bereich des Computers, für den die Ausnahmen für die Netzwerkisolation konfiguriert werden.

Remote-Port oder -Bereich

Remote-Port oder -Bereich des Computers, für den die Ausnahmen für die Netzwerkisolation konfiguriert werden.

Remote-Adresse

Netzwerkadresse des Computers, für den die Ausnahmen für die Netzwerkisolation konfiguriert werden.

Programme

Mit diesem Kontrollkästchen können Sie ein Programm hinzufügen, das eine Netzwerkverbindung initiieren darf, die zu den Ausnahmen für die Netzwerkisolation auf dem isolierten Computer hinzugefügt wurde.

Wenn dieses Kontrollkästchen aktiviert ist, können Sie ein solches Programm hinzufügen.

Wenn dieses Kontrollkästchen deaktiviert ist, kann eine Netzwerkverbindung, die zu den Ausnahmen der Netzwerkisolation hinzugefügt wurde, von einem beliebigen Programm auf dem isolierten Computer initiiert werden.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Hinzufügen

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet. Dort können Sie den Pfad eines Programms angeben, das eine Netzwerkverbindung aufbauen darf, die zu den Ausnahmen für die Netzwerkisolation hinzugefügt wurde.

Bearbeiten

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet. Dort können Sie den Pfad eines hinzugefügten Programms bearbeiten.

Diese Schaltfläche ist verfügbar, wenn in der Liste ein Programm ausgewählt ist.

Löschen

Mit dieser Schaltfläche wird ein hinzugefügtes Programm gelöscht.

Diese Schaltfläche ist verfügbar, wenn in der Liste ein Programm ausgewählt ist.

Das Fenster „Präventionsregel“

Name

Name der Regel.

Typ

Typ des Objekts, das Sie blockieren möchten.

Im Abschnitt **Pfad des Objekts** können Sie auswählen, ob der vollständige Pfad des zu verbietenden Objekts angegeben werden soll. Wenn Sie den Pfad angeben möchten, geben Sie den Wert in das entsprechende Feld ein.

Im Abschnitt **Objektprüfsumme** können Sie auswählen, ob die Prüfsumme für das zu verbietende Objekt angegeben werden soll. Wenn Sie die Prüfsumme angeben möchten, wählen Sie den Typ aus und geben Sie den Wert in das entsprechende Feld ein.

Das Fenster „Endpoint Detection and Response (KATA)“

Endpoint Detection and Response (KATA)

Der Schalter **Endpoint Detection and Response (KATA)** aktiviert /deaktiviert die Komponente Endpoint Detection and Response (KATA), die mit der Lösung Kaspersky Anti Targeted Attack Platform interagiert. Diese Lösung kann komplexe Bedrohungen sofort erkennen. Dazu zählen beispielsweise gezielte Angriffe, hochentwickelte, hartnäckige Bedrohungen und Zero-Day-Angriffe.

Wenn der Schalter **Endpoint Detection and Response (KATA)** aktiviert ist, ist die Komponente Endpoint Detection and Response (KATA) aktiviert.

Wenn der Schalter **Endpoint Detection and Response (KATA)** deaktiviert ist, ist die Komponente Endpoint Detection and Response (KATA) deaktiviert.

Der Umschalter ist standardmäßig deaktiviert.

Einstellungen der Serververbindung

Dieser Link öffnet einen Dialog, in dem Sie die Einstellungen für die Verbindung mit KATA-Servern konfigurieren können.

KATA-Server

Diese Liste enthält die KATA-Server, die Sie hinzugefügt haben.

Hinzufügen

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie die Verbindung zu einem KATA-Server konfigurieren können.

Bearbeiten

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie eine bestehende Verbindung zu einem KATA-Server bearbeiten können.

Diese Schaltfläche ist verfügbar, wenn ein Server in der Serverliste ausgewählt ist.

Löschen

Mit dieser Schaltfläche wird ein KATA-Server aus der Serverliste entfernt.

Diese Schaltfläche ist verfügbar, wenn ein Server in der Serverliste ausgewählt ist.

Adresse

IP-Adresse eines KATA-Servers.

Port

Portnummer eines KATA-Servers.

Synchronisierungsanfrage an KATA senden alle (Min.)

Das Intervall zwischen Synchronisierungsanfragen, die an einen KATA-Server gesendet werden.

Der Standardwert ist 5 Minuten.

TTL beim Senden von Ereignissen verwenden

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die TTL-Funktion für Pakete, die von Kaspersky Endpoint Security an einen KATA-Server gesendet werden. Der TTL-Mechanismus begrenzt die Lebensdauer von Ereignispaketen auf den Wert, der im Feld TTL (h) angegeben ist.

Wenn dieses Kontrollkästchen aktiviert ist, ist TTL aktiviert.

Wenn dieses Kontrollkästchen deaktiviert ist, ist TTL deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

TTL (h)

Die Lebensdauer von Paketen, die von Kaspersky Endpoint Security an einen KATA-Server gesendet werden.

Der Standardwert ist 24 Stunden.

Im Abschnitt **Einstellungen für die Datenübertragung** können Sie die Einstellungen für das Senden von Daten an die KATA-Server konfigurieren.

Maximale Verzögerung der Ereignisübertragung (s)

Das Intervall, in dem Kaspersky Endpoint Security Ereignisse an einen KATA-Server sendet.

Standardmäßig ist ein Wert von 30 Sekunden eingestellt.

Maximale Anzahl von Ereignissen pro Paket

Die maximale Anzahl von Ereignissen, die Kaspersky Endpoint Security pro Paket an einen KATA-Server sendet.

Der Standardwert ist 1.024 Ereignisse.

Im Abschnitt **Anforderungsbegrenzung** können Sie die Anzahl der übertragenen Ereignisse einschränken.

Anforderungsbegrenzung aktivieren

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Beschränkung für die Anzahl der Ereignisse, die Kaspersky Endpoint Security an einen KATA-Server sendet.

Wenn dieses Kontrollkästchen aktiviert ist, wird die Anzahl der von der App gesendeten Ereignisse beschränkt.

Wenn dieses Kontrollkästchen deaktiviert ist, wird die Anzahl der von der App gesendeten Ereignisse nicht beschränkt.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Maximale Anzahl von Ereignissen pro Stunde

Die maximale Anzahl von Ereignissen, die Kaspersky Endpoint Security pro Stunde an einen KATA-Server sendet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort.

Der Standardwert ist 3.000 Ereignisse pro Stunde.

Prozentsatz für die Überschreitung des Ereignislimits

Der Schwellenwert für Ereignisse des gleichen Typs (in Prozent).

Kaspersky Endpoint Security beschränkt die Übertragung von Ereignissen eines bestimmten Typs, wenn das Verhältnis von Ereignissen dieses Typs zur Gesamtanzahl der Ereignisse den konfigurierten Schwellenwert überschreitet.

Der Standardwert ist 15 Prozent.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Das Fenster „KATA-Server“

Adresse

IP-Adresse eines KATA-Servers.

Port

Portnummer eines KATA-Servers.

Der Standardwert ist 443.

Das Fenster „Einstellungen für die Serververbindung“

Timeout (s)

Das Timeout für die Antwort des KATA-Servers. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, eine Verbindung zu einem anderen KATA-Server herzustellen.

Standardmäßig ist ein Wert von 10 Sekunden eingestellt.

Im Abschnitt **TLS-Serverzertifikat** können Sie ein TLS-Zertifikat hinzufügen oder entfernen und Informationen über das hinzugefügte Zertifikat ansehen.

TLS-Zertifikat hinzufügen

Mit dieser Schaltfläche wird ein Fenster geöffnet. Dort können Sie ein TLS-Zertifikat auswählen, das zum Herstellen einer vertrauenswürdigen Verbindung mit einem KATA-Server verwendet wird.

Entfernen

Mit dieser Schaltfläche wird das aktuelle TLS-Zertifikat entfernt.

Diese Schaltfläche ist verfügbar, wenn ein TLS-Zertifikat hinzugefügt wurde.

Im Abschnitt **Erhöhte Verbindungssicherheit** können Sie den erweiterten Schutz für die Verbindung zwischen Kaspersky Endpoint Security und einem KATA-Server konfigurieren.

Zwei-Wege-Überprüfung verwenden

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Zwei-Wege-Überprüfung, durch die die Sicherheit der Verbindung zwischen Kaspersky Endpoint Security und einem KATA-Server erhöht wird. Um die Zwei-Wege-Überprüfung zu verwenden, müssen Sie einen Krypto-Container laden.

Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security die Zwei-Wege-Überprüfung, um eine Verbindung mit einem KATA-Server herzustellen.

Wenn dieses Kontrollkästchen deaktiviert ist, verwendet Kaspersky Endpoint Security keine Zwei-Wege-Überprüfung für die Verbindung mit einem KATA-Server.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Krypto-Container laden

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet. Dort können Sie einen Krypto-Container auswählen, der für die Zwei-Wege-Überprüfung verwendet werden soll. Die Krypto-Container-Datei hat die Erweiterung .PFX.

> **Hinweis:** Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Kennwort kann nicht hinzugefügt werden.

Kennwort des Krypto-Containers

Das Kennwort für den Krypto-Container, das für die Zwei-Wege-Überprüfung verwendet wird.

Abschnitt „Sicherheitskontrolle“

Web-Kontrolle

Der Umschalter **Web-Kontrolle** aktiviert/deaktiviert die „Web-Kontrolle“.

Wenn der Umschalter **Web-Kontrolle** aktiviert ist, können Sie Regeln erstellen, um die Websites zu verwalten, welche die Benutzer auf den Remote-Computern besuchen.

Wenn der Umschalter **Web-Kontrolle** deaktiviert ist, können Sie die Websites nicht verwalten, welche die Benutzer auf den Remote-Computern besuchen.

Der Umschalter ist standardmäßig deaktiviert.

Regelliste

Diese Liste enthält die von Ihnen erstellten Regeln zur Verwaltung von Websites, welche die Benutzer auf Remote-Computern besuchen.

Die Reihenfolge, in der die Regeln angeordnet sind, entspricht der Priorität, nach welcher die Regeln durch Kaspersky Endpoint Security angewendet werden.

Hinzufügen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie eine neue Regel für die Web-Kontrolle erstellen können.

Löschen

Mit dieser Schaltfläche wird die ausgewählte Regel aus der Regelliste gelöscht.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Regel aktiviert ist.

Nach oben

Mit dieser Schaltfläche wird die ausgewählte Regel in der Regelliste nach oben verschoben und die Priorität der Regel wird für ihre Anwendung durch Kaspersky Endpoint Security erhöht.

Nach unten

Mit dieser Schaltfläche wird die ausgewählte Regel in der Regelliste nach unten verschoben und die Priorität der Regel wird für ihre Anwendung durch Kaspersky Endpoint Security reduziert.

Name

Name der Regel.

Status

Der Umschalter in dieser Spalte bestimmt, ob die Regel aktiv oder inaktiv ist.

Sie können den Umschalter neben einer Regel aktivieren/deaktivieren, um den Status der Regel zu ändern.

Aktion

Eine Aktion, die Kaspersky Endpoint Security ausführt, wenn der Benutzer eine bestimmte Webadresse, eine Gruppe von Webadressen oder eine Website-Kategorie besucht, für welche die Regel gilt.

Sie können die zugewiesene Aktion ändern. Wählen Sie dazu im Kontextmenü in dieser Spalte eine andere Aktion aus.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Regel bearbeiten“

Eingabefeld „Regelname eingeben“

Name der Regel.

Im Abschnitt **Status** können Sie festlegen, ob die Regel aktiv oder inaktiv sein soll.

Aktiv

Wenn diese Option ausgewählt ist, erstellen Sie eine aktive Regel. Sie wird auf den Remote-Computer angewandt, sobald die Richtlinie wirksam wird.

Inaktiv

Wenn diese Option ausgewählt ist, erstellen Sie eine inaktive Regel. Sie wird nicht verwendet, wenn die Richtlinie wirksam wird.

Im Abschnitt **Aktion** können Sie auswählen, welche Aktion Kaspersky Endpoint Security ausführen soll, wenn der Benutzer eine bestimmte Webadresse, Gruppe von Webadressen oder Kategorie von Websites besucht, für welche die Regel gilt.

Erlauben

Wenn diese Option ausgewählt ist, erlaubt Kaspersky Endpoint Security, dass der Benutzer die Webadresse, Gruppe von Webadressen oder Kategorie von Websites besucht, für welche die Regel gilt.

Hinweis: Kaspersky Endpoint Security erlaubt den Besuch von Webressourcen auf dem Remote-Computer, wenn der Schalter **Sichere Verbindungen (HTTPS) untersuchen** im Fenster **Netzwerk** des Assistenten für neue Richtlinien aktiviert ist.

Diese Variante ist standardmäßig ausgewählt.

Blockieren

Wenn diese Option ausgewählt ist, verhindert Kaspersky Endpoint Security, dass der Benutzer die Webadresse, Gruppe von Webadressen oder Kategorie von Websites besucht, für welche die Regel gilt.

Hinweis: Kaspersky Endpoint Security zeigt Benachrichtigungen an, wenn der Benutzer auf Webressourcen zugreift, die von der „Web-Kontrolle“ auf dem Remote-Computer blockiert werden, vorausgesetzt der Schalter **Sichere Verbindungen (HTTPS) untersuchen** im Fenster **Netzwerk** des Assistenten für neue Richtlinien ist aktiviert.

Warnung anzeigen

Wenn diese Option ausgewählt ist, zeigt Kaspersky Endpoint Security eine Warnung an, wenn der Benutzer versucht, die Webadresse, Gruppe von Webadressen oder Website-Kategorie zu besuchen, für welche die Regel gilt.

Im Abschnitt **Bereich der Regel** können Sie festlegen, wofür eine Regel erstellt werden soll: für eine bestimmte Webadresse, eine Gruppe von Webadressen oder Website-Kategorien.

Kategorien

Wenn diese Option ausgewählt ist, erstellen Sie eine Regel für Website-Kategorien.

Kategorien auswählen

Dieser Link öffnet einen Dialog, in dem Sie die Website-Kategorien auswählen können, für welche die Regel gilt.

Individuelle Adressen

Wenn diese Option ausgewählt ist, erstellen Sie eine Regel für eine bestimmte Webadresse oder für eine Gruppe von Webadressen.

Diese Variante ist standardmäßig ausgewählt.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie eine Webadresse oder die Maske einer Webadresse angeben können, für welche die Regel gilt.

Löschen

Durch Klick auf diese Schaltfläche wird die ausgewählte Webadresse oder Maske einer Webadresse aus der Liste der Webadressen gelöscht, für welche die Regel gilt.

Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Webadresse oder der Maske einer Webadresse aktiviert ist.

Adresse

Webadressen oder Masken für Webadressen, für welche die Regel gilt.

Dialog „Webadresse hinzufügen“

Eingabefeld „Webadresse eingeben“

Webadresse oder Maske einer Webadresse, für welche die Regel gilt.

Dialog „Inhaltskategorien“

Liste der Inhaltskategorien

Diese Liste enthält eine Liste mit den Website-Kategorien, die Sie zu der Regel hinzufügen können.

Das Kontrollkästchen neben dem Namen einer Website-Kategorie fügt die Websites, die zu dieser Kategorie gehören, zu der Regel hinzu oder löscht diese Websites aus der Regel.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Der Abschnitt „Basisschutz“

Schutz vor bedrohlichen Dateien

Dieser Link öffnet ein Fenster, in dem Sie die Einstellungen für den „Schutz vor bedrohlichen Dateien“ anpassen können.

Schutz vor Web-Bedrohungen

Dieser Link öffnet ein Fenster, in dem Sie die Einstellungen für den „Schutz vor Web-Bedrohungen“ anpassen können.

Schutz vor Netzwerkbedrohungen

Dieser Link öffnet ein Fenster, in dem Sie die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ anpassen können.

Schutz vor E-Mail-Bedrohungen

Dieser Link öffnet ein Fenster, in dem Sie die Einstellungen für den Schutz vor E-Mail-Bedrohungen anpassen können.

Firewall

Dieser Link öffnet ein Fenster, in dem Sie die Einstellungen für die Firewall anpassen können.

Fenster „Schutz vor bedrohlichen Dateien“

Schutz vor bedrohlichen Dateien

Der Umschalter **Schutz vor bedrohlichen Dateien** aktiviert/deaktiviert den „Schutz vor bedrohlichen Dateien“.

Wenn der Umschalter **Schutz vor bedrohlichen Dateien** aktiviert ist, überwacht Kaspersky Endpoint Security in Echtzeit das Dateisystem der Client-Computer, für welche die Richtlinie gilt.

Wenn der Umschalter **Schutz vor bedrohlichen Dateien** deaktiviert ist, wird das Dateisystem der Client-Computer, für welche die Richtlinie gilt, nicht durch Kaspersky Endpoint Security geschützt.

Der Umschalter ist standardmäßig aktiviert.

Im Abschnitt **Schutzbereich** können Sie einen Schutzbereich festlegen. Dazu können Sie einen der vordefinierten Einträge auswählen oder Dateien und Ordner hinzufügen.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie eine Datei, einen Ordner oder eine Maske angeben können, die zur Liste für die Objekte des Schutzbereichs hinzugefügt werden sollen.

Löschen

Mit dieser Schaltfläche können Sie das Objekt aus dem Schutzbereich entfernen.

Diese Schaltfläche ist verfügbar, wenn in der Liste geschützter Objekte ein Objekt ausgewählt ist.

Sie können die in den Schutzbereich einbezogenen Standardobjekte nicht löschen.

Schutzbereich

Diese Spalte enthält die Objekte, die Kaspersky Endpoint Security untersucht, wenn der „Schutz vor bedrohlichen Dateien“ aktiviert ist.

Kaspersky Endpoint Security untersucht standardmäßig die folgenden Objekte:

- **Alle Wechseldatenträger**. Kaspersky Endpoint Security untersucht alle Wechseldatenträger.
- **Alle internen Datenträger**. Kaspersky Endpoint Security untersucht alle internen Laufwerke.
- **Alle Netzlaufwerke**. Kaspersky Endpoint Security untersucht alle Netzlaufwerke.

Status

Ist der Umschalter in dieser Spalte aktiviert, so untersucht Kaspersky Endpoint Security das entsprechende Objekt in der Spalte **Schutzbereich**, wenn der „Schutz vor bedrohlichen Dateien“ aktiviert ist.

Ist der Umschalter in dieser Spalte deaktiviert, so untersucht Kaspersky Endpoint Security das entsprechende Objekt in der Spalte **Schutzbereich** nicht, wenn der „Schutz vor bedrohlichen Dateien“ aktiviert ist.

Erweitert

Diese Spalte gibt an, ob Kaspersky Endpoint Security die Unterordner des entsprechenden Objekts untersucht.

Im Abschnitt **Beim Erkennen eines schädlichen Objekts** können Sie auswählen, welche Aktion Kaspersky Endpoint Security beim Fund eines schädlichen Objekts ausführen soll.

Aktion erfragen

Kaspersky Endpoint Security zeigt ein Benachrichtigungsfenster an. Es informiert darüber, von welchem schädlichen Objekt die Datei infiziert ist, und bietet entsprechende Aktionen zur Auswahl an. Die Aktionen können je nach Objektstatus variieren.

Diese Variante ist standardmäßig ausgewählt.

Desinfizieren – Löschen, wenn Desinfektion fehlschlägt

Kaspersky Endpoint Security blockiert den Zugriff auf die infizierte Datei und versucht, sie zu desinfizieren, ohne nach Bestätigung durch den Benutzer zu fragen.

Wenn die Datei desinfiziert werden konnte, wird sie am ursprünglichen Ort unter dem ursprünglichen Namen gespeichert. Wenn die Desinfektion fehlschlägt, löscht Kaspersky Endpoint Security die infizierte Datei.

Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt

Kaspersky Endpoint Security blockiert den Zugriff auf die infizierte Datei und versucht, sie zu desinfizieren, ohne nach Bestätigung durch den Benutzer zu fragen.

Wenn die Datei desinfiziert werden konnte, wird sie am ursprünglichen Ort unter dem ursprünglichen Namen gespeichert. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei blockiert und verbleibt am ursprünglichen Ort.

Im Abschnitt **Optimierung** können Sie die Leistungseinstellungen für die Untersuchung anpassen und den Untersuchungsalgorithmus auswählen.

Nur neue und veränderte Dateien untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert einen Untersuchungsmodus, in dem nur jene Dateien untersucht werden, die Kaspersky Endpoint Security als neu oder als seit der letzten Untersuchung verändert einstuft.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security nur jene Dateien, die als neu oder als seit der letzten Untersuchung verändert gelten.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security alle Dateien.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schreibgeschütztes Systemvolume bei der Untersuchung überspringen

Dieses Kontrollkästchen deaktiviert/aktiviert in Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume. Dadurch wird die Untersuchungsdauer erheblich verkürzt.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security das schreibgeschützte Systemvolume.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

iSwift verwenden

Dieses Kontrollkästchen aktiviert/deaktiviert die Verwendung der iSwift-Untersuchungstechnologie. iSwift bietet in Kaspersky Endpoint Security einen speziellen Algorithmus, um bestimmte Objekte von der Untersuchung auszuschließen und dadurch die Untersuchung zu beschleunigen.

Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security iSwift bei der Untersuchung.

Wenn dieses Kontrollkästchen deaktiviert ist, wird iSwift von Kaspersky Endpoint Security nicht bei der Untersuchung verwendet.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Dateitypen** können Sie auswählen, welche Dateien von Kaspersky Endpoint Security untersucht werden, wenn der „Schutz vor bedrohlichen Dateien“ aktiviert ist.

Alle Dateien untersuchen

Kaspersky Endpoint Security untersucht alle Objekte, die im Dateisystem ausgeführt, geöffnet und gespeichert werden.

Anwendungen und Dokumente nach Inhalt untersuchen

Kaspersky Endpoint Security untersucht nur jene Objekte, die aufgrund ihres Inhalts als infizierbar gelten.

Anwendungen und Dokumente nach Erweiterung untersuchen

Kaspersky Endpoint Security untersucht jene Objekte, die aufgrund ihrer Dateierweiterung als infizierbar gelten.

Die Liste der Erweiterungen wird von Kaspersky erstellt und ist Teil der Kaspersky Endpoint Security-Datenbanken.

Dateien ohne Erweiterung werden von Kaspersky Endpoint Security immer untersucht.

Im Abschnitt **Zusammengesetzte Dateien** können Sie die Typen der zusammengesetzten Dateien auswählen, die Kaspersky Endpoint Security untersucht, wenn der „Schutz vor bedrohlichen Dateien“ aktiviert ist.

Archive untersuchen

Mit diesem Kontrollkästchen wird die Untersuchung von Archiven aktiviert/deaktiviert. Eine Liste der Erweiterungen finden Sie in der Hilfe zu Kaspersky Endpoint Security.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security Archive.

Wenn das Kontrollkästchen deaktiviert ist, werden Archive bei der Untersuchung übersprungen.

Installationspakete untersuchen

Mit diesem Kontrollkästchen wird die Untersuchung von Installationspaketen aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, werden Installationspakete durch Kaspersky Endpoint Security untersucht.

Wenn das Kontrollkästchen deaktiviert ist, werden Installationspakete bei der Untersuchung durch Kaspersky Endpoint Security übersprungen.

Eingebettete OLE-Objekte untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Objekten, die in Dateien eingebettet sind (z. B. Excel-Tabellen, Makros oder E-Mail-Anhänge).

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security eingebettete OLE-Objekte.

Wenn dieses Kontrollkästchen deaktiviert ist, werden eingebettete OLE-Objekte bei der Untersuchung übersprungen.

Archive nicht extrahieren, die größer sind als MB

Dieses Kontrollkästchen aktiviert/deaktiviert eine Größenbeschränkung für zu untersuchende Archive.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security Archive, welche die festgelegte Größe überschreiten.

Wenn das Kontrollkästchen deaktiviert ist, extrahiert und untersucht Kaspersky Endpoint Security Archive unabhängig von ihrer Größe.

Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** aktiviert ist.

Extrahieren aufschieben, wenn Archiv größer als MB

Größe für zu untersuchende Archive beschränken.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security alle Archive, deren Größe das festgelegte Limit überschreitet. Die Untersuchung erfolgt allerdings mit einer niedrigeren Priorität und beginnt zwei Minuten, nachdem ein solches Archiv gefunden wurde.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security alle Archive mit der gleichen Priorität.

Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** aktiviert ist.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Schutzbereich hinzufügen“

Eingabefeld „Geben Sie den Dateinamen, den Ordnernamen oder die Maske ein“

Pfad zu einer Datei, einem Ordner oder zur Maske von Datei/Ordner.

Dieses Objekt ist ein Ordner

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung eines Objekts als einen Ordner.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security das Objekt, das Sie im Feld **Dateiname, Ordnername oder Maske eingeben** als Ordner angegeben haben.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security das Objekt, das Sie im Feld **Dateiname, Ordnername oder Maske eingeben** als eine Datei angegeben haben.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Unterordner einschließen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung der Unterordner des Ordners, der im Eingabefeld **Dateiname, Ordnername oder Maske eingeben** angegeben ist.

Ist dieses Kontrollkästchen aktiviert, werden untergeordnete Ordner bei Malware-Untersuchungen von Kaspersky Endpoint Security untersucht.

Ist dieses Kontrollkästchen deaktiviert, scannt Kaspersky Endpoint Security bei Malware-Untersuchungen nur jene Dateien, die sich direkt in dem Ordner befinden, der im Feld **Dateiname, Ordnername oder Maske eingeben** angegeben ist.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Fenster „Schutz vor Web-Bedrohungen“

Schutz vor Web-Bedrohungen

Der Umschalter **Schutz vor Web-Bedrohungen** aktiviert/deaktiviert den „Schutz vor Web-Bedrohungen“.

Wenn der Umschalter **Schutz vor Web-Bedrohungen** aktiviert ist, untersucht der „Schutz vor Web-Bedrohungen“ die Daten, die mit dem HTTP- oder HTTPS-Protokoll in Safari, Google Chrome und Firefox auf Ihren Computer gelangen oder von ihm gesendet werden.

Wenn der Umschalter **Schutz vor Web-Bedrohungen** deaktiviert ist, untersucht der „Schutz vor Web-Bedrohungen“ die Daten nicht, die auf Ihrem Computer über die Webbrowser empfangen und gesendet werden.

Der Umschalter ist standardmäßig aktiviert.

Im Abschnitt **Beim Erkennen eines schädlichen Objekts** können Sie auswählen, welche Aktion Kaspersky Endpoint Security beim Fund eines schädlichen Objekts ausführen soll.

Aktion erfragen

Kaspersky Endpoint Security zeigt ein Benachrichtigungsfenster an, das darüber informiert, von welchem Schadsoftwaretyp das Objekt im Web-Datenverkehr infiziert ist. Sie werden aufgefordert, die Aktion auszuwählen, die von Kaspersky Endpoint Security mit dem Objekt ausgeführt werden soll. Die verfügbaren Aktionen können je nach Objektstatus variieren.

Diese Aktion ist standardmäßig ausgewählt.

Automatisch blockieren

Kaspersky Endpoint Security sperrt die gefährlichen Objekte im Web-Datenverkehr automatisch.

Im Abschnitt **Vertrauenswürdige Webadressen** können Sie eine Liste mit vertrauenswürdigen Webadressen erstellen oder bearbeiten, und die Untersuchung des Datenverkehrs von Webadressen aus dieser Liste aktivieren oder deaktivieren.

Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung des Web-Datenverkehrs von vertrauenswürdigen Webadressen.

Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security den Web-Datenverkehr von vertrauenswürdigen Webadressen nicht.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security den Web-Datenverkehr von vertrauenswürdigen Webadressen.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Liste Webadresse

Diese Liste enthält vertrauenswürdige Webadressen.

Sie können das Kontrollkästchen für eine Webadresse in der Liste deaktivieren. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht der „Schutz vor Web-Bedrohungen“ den Web-Datenverkehr von der vertrauenswürdigen Webadresse.

Die Liste ist verfügbar, wenn das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** aktiviert ist.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie eine Webadresse oder die Maske einer Webadresse eingeben können, die zur Liste der vertrauenswürdigen Webadressen hinzugefügt werden soll.

Löschen

Durch Klick auf diese Schaltfläche wird die ausgewählte Webadresse oder die Maske für eine Webadresse aus der Liste für vertrauenswürdige Webadressen gelöscht.

Die Schaltfläche ist verfügbar, wenn in der Liste für vertrauenswürdige Webadressen eine Webadresse oder die Maske für eine Webadresse ausgewählt ist.

Webadresse

Diese Spalte enthält vertrauenswürdige Webadressen.

Status

Ist der Umschalter in dieser Spalte aktiviert, so untersucht Kaspersky Endpoint Security das entsprechende Objekt aus der Spalte **Webadresse** nicht, wenn der „Schutz vor Web-Bedrohungen“ aktiviert ist und das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** aktiviert ist.

Ist der Umschalter in dieser Spalte deaktiviert, so untersucht Kaspersky Endpoint Security das entsprechende Objekt aus der Spalte **Webadresse**, wenn der „Schutz vor Web-Bedrohungen“ aktiviert ist und das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** aktiviert ist.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Webadresse hinzufügen“

Eingabefeld „Webadresse eingeben“

Webadresse oder Maske für eine Webadresse, deren Datenverkehr vom „Schutz vor Web-Bedrohungen“ nicht untersucht wird.

Im Abschnitt **Status** können Sie festlegen, ob Kaspersky Endpoint Security den Datenverkehr von dieser Webadresse oder Gruppe von Webadressen untersuchen soll.

Deaktivieren

Die Webadresse oder die Maske einer Webadresse wird zur Liste der **Vertrauenswürdige Webadressen** hinzugefügt, aber Kaspersky Endpoint Security untersucht ihren Datenverkehr trotzdem.

Aktivieren

Die Webadresse oder die Maske einer Webadresse wird zur Liste der **Vertrauenswürdige Webadressen** hinzugefügt und Kaspersky Endpoint Security untersucht ihren Datenverkehr nicht.

Fenster „Schutz vor Netzwerkbedrohungen“

Schutz vor Netzwerkbedrohungen

Der Umschalter **Schutz vor Netzwerkbedrohungen** aktiviert/deaktiviert den „Schutz vor Netzwerkbedrohungen“.

Wenn der Umschalter **Schutz vor Netzwerkbedrohungen** aktiviert ist, schützt Kaspersky Endpoint Security den Remote-Computer vor Netzwerkangriffen.

Wenn der Umschalter **Schutz vor Netzwerkbedrohungen** deaktiviert ist, schützt Kaspersky Endpoint Security den Remote-Computer nicht vor Netzwerkangriffen.

Der Umschalter ist standardmäßig aktiviert.

Im Abschnitt **Einstellungen für den Schutz vor Netzwerkbedrohungen** können Sie den Zeitraum ändern, für den Kaspersky Endpoint Security angreifende Computer blockiert.

Angreifenden Computer sperren für Min.

Dieses Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit der angreifende Computer für einen festgelegten Zeitraum auf die Liste der blockierten Computer gesetzt werden.

Wenn dieses Kontrollkästchen aktiviert ist, werden angreifende Computer für einen festgelegten Zeitraum auf die Liste der blockierten Computer gesetzt.

Wenn dieses Kontrollkästchen deaktiviert ist, werden angreifende Computer nicht von Kaspersky Endpoint Security blockiert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Angreifende Computer werden standardmäßig für 60 Minuten blockiert.

Im Abschnitt **Ausnahmen** können Sie eine Liste mit IP-Adressen von Remote-Computern erstellen und bearbeiten, deren Netzwerkaktivität Kaspersky Endpoint Security nie blockiert.

Liste der IP-Adressen

Diese Liste enthält IP-Adressen von Remote-Computern, deren Netzwerkaktivität nie von Kaspersky Endpoint Security blockiert wird.

Hinzufügen

Diese Schaltfläche öffnet einen Dialog, in dem Sie die IP-Adresse eines Remote-Computers eingeben können.

Löschen

Durch Klick auf diese Schaltfläche wird die ausgewählte IP-Adresse aus der Liste für IP-Adressen gelöscht.

Die Schaltfläche ist verfügbar, wenn in der Liste für IP-Adressen die IP-Adresse eines Remote-Computers ausgewählt ist.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Dialog „Ausnahme hinzufügen“

Eingabefeld „IP-Adresse eingeben“

IP-Adresse eines Remote-Computers.

Abschnitt „Erweiterter Schutz“

Im Abschnitt **KSN-Einstellungen** können Sie die Verwendung von Kaspersky Security Network anpassen.

Kaspersky Security Network

Der Umschalter **Kaspersky Security Network** aktiviert/deaktiviert die Teilnahme an Kaspersky Security Network.

Wenn der Umschalter **Kaspersky Security Network** aktiviert ist, nehmen die Client-Computer, für welche die Richtlinie gilt, an Kaspersky Security Network teil.

Wenn der Umschalter **Kaspersky Security Network** deaktiviert ist, nehmen die Client-Computer, für welche die Richtlinie gilt, nicht an Kaspersky Security Network teil.

Der Umschalter ist standardmäßig deaktiviert.

Erweiterter KSN-Modus

Der Umschalter **Erweiterter KSN-Modus** aktiviert/deaktiviert das Senden von zusätzlichen Daten von einem Remote-Computer an Kaspersky. Dabei geht es um Daten, die erforderlich sind, um den Schutz von Client-Computern und die Benutzerfreundlichkeit von Kaspersky Endpoint Security zu verbessern.

Wenn der **Erweiterte KSN-Modus** aktiviert ist, stellen die Client-Computer, die der Richtlinie unterliegen, sowohl die Daten bereit, die für das Funktionieren der Erkennungsdienste erforderlich sind, als auch zusätzliche Daten für Kaspersky Security Network.

Wenn der **Erweiterte KSN-Modus** deaktiviert ist, stellen die Client-Computer, die der Richtlinie unterliegen, nur die Daten bereit, die für das Funktionieren der Erkennungsdienste erforderlich sind, und stellen keine zusätzlichen Daten für Kaspersky Security Network bereit.

Der Umschalter **Erweiterte KSN-Modus** ist standardmäßig deaktiviert.

Der Umschalter ist automatisch aktiviert, wenn Sie den Umschalter **Kaspersky Security Network** aktivieren. Er kann aber deaktiviert werden.

Daten, die an Kaspersky bereitgestellt werden, wenn Kaspersky Security Network in der Global KSN-Infrastruktur verwendet wird

Wenn der Umschalter **Kaspersky Security Network** aktiviert ist und der Umschalter **Erweiterter KSN-Modus** deaktiviert ist, stellt Kaspersky Endpoint Security, das auf Client-Computern läuft, die folgenden Daten an Kaspersky bereit:

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Vollversion der installierten Software;
  Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; einmalige Geräte-ID Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

Wenn die Umschalter **Kaspersky Security Network** und **Erweiterter KSN-Modus** aktiviert sind, stellt Kaspersky Endpoint Security, das auf Client-Computern läuft, die folgenden Daten an Kaspersky bereit:

- Informationen über die Version des Betriebssystems (OS) und die auf dem Computer installierten Service Packs, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems, Parameter des Funktionsmodus des Betriebssystems; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Windows Service Packs; Datum und Uhrzeit des Betriebssystemstarts; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Verhaltensanalyse-Subsystem; Anzahl der verzögerten Aktionsereignisse des Betriebssystems des aktuellen Typs; Verzögerungsdauer bei der Ereignisverarbeitung für Betriebssystemaktionen im Subsystem für den proaktiven Schutz; Anzahl der verarbeiteten Aktionsereignisse des Betriebssystems; Anzahl der verarbeiteten synchronen Aktionsereignisse des Betriebssystems; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems des aktuellen Typs; Verarbeitungsverzögerungszeit des Ereignisses über die Betriebssystemaktion im Subsystem für die persistente Ereignisspeicherung; Gesamtverzögerung aller Aktionsereignisse des Betriebssystems; Anzahl der wartenden synchronen Aktionsereignisse des Betriebssystems; Datum und Uhrzeit des empfangenen Ereignisses über eine Aktion im Betriebssystem.

- Informationen über den fehlgeschlagenen letzten Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.

- Informationen über die installierte Anwendung des Rechtsinhabers und den Status des Antiviren-Schutzes: ID der Software-Installation (PCID) Version des Software-Datenbankeintrags; eindeutige ID der Instanz der Anwendungsinstallation auf dem Computer, Anwendungstyp, Anwendungstyp-ID, die Vollversion der installierten Anwendung, ID der Version der Anwendungseinstellungen, ID des Computertyps, eindeutige ID des Computers, auf dem die Anwendung installiert ist, eindeutige Benutzer-ID beim Dienst des Rechteinhabers, lokale Sprache und Betriebszustand, Version der installierten Softwarekomponenten und ihr Betriebszustand, Version des verwendeten Protokolls zur Verbindungsherstellung zum Dienst des Rechteinhabers; Vollversion der installierten Software; Typ der installierten Software; ID des Software-Updates; ID des Reputationsdienstes; ID des Protokolltyps; ID eines regionalen Aktivierungscenters; Version der Liste für widerrufene Entscheidungen des Softwaredienstes; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; eindeutige ID der Instanz der Programminstallation auf dem Computer; Datum der Lizenzaktivierung; Ablaufdatum der Lizenz; Lizenz-ID; Status der von der Software verwendeten Lizenz; Prüfsummentyp des verarbeiteten Objekts; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Prüfsumme des verarbeiteten Objekts; Prüfsumme des Software-Aktivierungscodes; Vollversion der Software; Software-ID; Prüfsumme der Software-Schlüsseldatei; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; ID des Zertifikats, mit dem die Kopfzeile des Software-Lizenztickets signiert wurde; Erstellungsdatum und -uhrzeit des Software-Lizenztickets; Prüfsumme des Software-Lizenztickets; Version des Software-Lizenztickets; Version des Software-Aktivierungscodes; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aktuelle Lizenzticket-ID; ID der Softwarekomponente; Ergebnis der Software-Aktion; Fehlercode; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Anzahl der Update-Anwendungs-Zyklen für die Antiviren-Datenbanken; Zeitpunkt (Datum und Uhrzeit), an dem die Antiviren-Datenbanken zuletzt aktualisiert und angewendet wurden; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version der Software-Komponente; ID des Software-Updates; Typ der installierten Software; Startdatum und -uhrzeit vom Aktivitätsmonitor; Installationsdatum und -uhrzeit der Software; Wahrscheinlichkeit der Übermittlung von Statistiken durch den Aktivitätsmonitor; Code des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Datenbank-Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; maximal zulässige Zeit für die Verarbeitung eines Ereignisses durch den Aktivitätsmonitor; Verarbeitungsdauer des Ereignisses, das länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert hat; Gesamtzahl der Ereignisse, die länger als die Standard-Verarbeitungsdauer vom Aktivitätsmonitor gedauert haben.

- Informationen über alle verarbeiteten Objekte und Vorgänge: Verdikt der Software für das verarbeitete Objekt; Verzeichniscode; Größe des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Anzahl der erkannten Software im Kontext des „Aktivitätsmonitors“; Zeitpunkt (Datum und Uhrzeit), zu dem der „Aktivitätsmonitor“ die Software erkannt hat; Erkennungscharakteristiken; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Grund, aus dem der „Aktivitätsmonitor“ die Software erkannt hat; Prüfsumme (MD5) des verarbeiteten Objekts; Ergebnis der Modul-Integritätsprüfung; Name des verarbeiteten Objekts; Typ des ausgelösten Eintrags der Antiviren-Datenbanken der Software; Speicherpfad des verarbeiteten Objekts; Name des untersuchten Objekts; Datum und Uhrzeit der Untersuchung; URL-Adresse und Referenzadresse, von denen es heruntergeladen wurde; Größe und Pfade der untersuchten Dateien; Zeichen des Archivs; Datum und Uhrzeit der Dateierstellung; Name, Größe und Prüfsummen (MD5, SHA2-256) des Packers (falls die Datei gepackt wurde); Entropie der Datei; Typ der Datei; Code des Dateityps; Zeichen, ID und Format der ausführbaren Datei; Prüfsumme des Objekts (MD5, SHA2-256); Typ und Wert der zusätzlichen Prüfsumme des Objekts; Daten über die digitale Signatur des Objekts (Zertifikat): Daten über den Herausgeber des Zertifikats, Anzahl der Starts des Objekts seit der letzten Übermittlung von Statistiken, ID der Überprüfungsaufgabe der Anwendung, Mittel zum Erhalt von Informationen über den Ruf des Objekts, Wert des Zielfilters, technische Parameter der anwendbaren Erkennungstechnologien; Speicherpfad des verarbeiteten Objekts; Verzeichniscode.

- Für ausführbare Dateien: Entropie der Dateiabschnitte, Kennzeichen der Reputations-Überprüfung oder Kennzeichen der Dateisignatur, Name, Typ, ID-Typ, Prüfsumme (MD5) und Größe der Anwendung, die vom zu validierenden Objekt geladen wurde, Anwendungspfad und Vorlagenpfade, Attribut, das das Vorhandensein in der Autostart-Liste angibt, Datum des Eintrags, Liste mit Attributen, Name des Packers, Informationen über die digitale Signatur der Anwendung: Herausgeberzertifikat, Name der hochgeladenen Datei im MIME-Format, Datum und Uhrzeit der Dateierstellung.

- Informationen über die gestarteten Anwendungen und deren Module: Prüfsummen (MD5, SHA2-256) von ausgeführten Dateien, Größe, Attribute, Erstellungsdatum, Name des Packers (falls die Datei gepackt wurde), Dateinamen, Informationen über die im System ausgeführten Prozesse (Prozess-ID (PID), Prozessname, Informationen über das Benutzerkonto, aus dem der Prozess gestartet wurde, Anwendung und Befehl, mit dem der Prozess gestartet wurde, vollständiger Pfad der Dateien des Prozesses sowie auszuführende Befehlszeile, Beschreibung der Anwendung, zu dem der Prozess gehört (Name der Anwendung und Informationen über den Herausgeber) sowie die verwendeten digitalen Zertifikate und Informationen, die zur Überprüfung ihrer Authentizität dienen, oder Informationen über das Fehlen einer digitalen Signatur einer Datei) und Informationen über die in die Prozesse geladenen Module: deren Namen, Größen, Typen, Erstellungsdaten, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfade, Header-Informationen der PE-Datei, Namen der Packer (falls die Datei gepackt wurde), Informationen über die Verfügbarkeit und Gültigkeit dieser Statistiken, ID des Modus zur Erstellung von zu sendenden Statistiken.

- Falls Bedrohungen oder Schwachstellen erkannt werden, werden zusätzlich zu den Informationen über das erkannte Objekt auch die folgenden Informationen bereitgestellt: ID, Version und Typ des Eintrags in der Antiviren-Datenbank, Name der Bedrohung, basierend auf der Klassifikation von Kaspersky, Datum und Uhrzeit der letzten Aktualisierung der Antiviren-Datenbank, Name der ausführbaren Datei, Prüfsumme (MD5) der Anwendungsdatei, welche die Webadresse, unter der die Bedrohung erkannt wurde, angefordert hat, IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, ID der Schwachstelle und ihre Gefahrenstufe, URL und Referenz der Webseite, auf der die Schwachstelle gefunden wurde.

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt.

- Informationen über einen Netzwerkangriff: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.

- Informationen zu Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, aus der der Prozess gestartet wurde, der den Port geöffnet hat, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Verbindungsports, Verbindungsstatus, Zeitstempel für das Öffnen des Ports.

- URL- und IP-Adresse der Webseite, auf der schädliche oder verdächtige Inhalte erkannt wurden, Name, Größe und Prüfsumme der Datei, die die URL anforderte, Kennung, Priorität und Grad der Regel, die für die Entscheidung verwendet wurde, Ziel des Angriffs.

- Informationen über Updates der installierten App- und Antiviren-Datenbanken: Bearbeitungsstand der Update-Aufgabe, Art des Fehlers, der möglicherweise während des Update-Vorgangs aufgetreten ist, Anzahl der fehlgeschlagenen Updates, ID der Anwendungskomponente, die die Updates ausführt.

- Informationen über die Nutzung von Kaspersky Security Network (KSN): KSN-ID, Anwendungs-ID, vollständige Version der Anwendung, anonymisierte IP-Adresse des Benutzergerätes, Indikatoren für die Qualität der Ausführung von KSN-Anfragen, Indikatoren für die Qualität der Verarbeitung von KSN-Paketen, Indikatoren für die Anzahl der KSN-Anfragen und Informationen über die Arten von KSN-Anfragen, Datum und Uhrzeit für den Beginn des Sendevorgangs von Statistiken, Datum und Uhrzeit für das Ende des Sendevorgangs von Statistiken, Informationen über die Aktualisierung der KSN-Konfiguration: ID der aktiven Konfiguration, ID der empfangenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen zu Systemprotokoll-Ereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.

- Informationen zur Bestimmung der Reputation von Dateien und URL-Adressen: URL-Adresse, unter der die Reputation angefordert wird, und Referrer, Protokolltyp der Verbindung, interne ID des Anwendungstyps, Nummer des verwendeten Ports, Benutzer-ID, Prüfsumme der untersuchten Datei (MD5), Typ der erkannten Bedrohung, Informationen über den Datensatz, der zum Erkennen der Bedrohung verwendet wurde (ID des Datensatzes für die Antiviren-Datenbanken, Zeitstempel und Typ des Datensatzes); öffentlicher Schlüssel des Zertifikats; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus.

- Daten zur geografischen Verteilung der Anwendung: Datum der Anwendungsinstallation und -aktivierung, ID des Partners, der die Lizenz für die Anwendungsaktivierung bereitstellt, Anwendungs-ID, Lokalisierungs-ID der Anwendungssprache, Lizenz-Seriennummer für die Anwendungsaktivierung, Merkmal für die KSN-Teilnahme.

- Informationen zur verwendeten Lizenz: Typ und Gültigkeitsdauer der Lizenz, Anzahl der Tage bis zum Ablauf der Lizenz, ID des Partners, bei dem die Lizenz erworben wurde, ID des Regionalen Aktivierungscenters, Prüfsumme des Aktivierungscodes, mit dem SHA1-Algorithmus berechneter Hash des Tickettexts, Datum und Uhrzeit der Erstellung des Lizenztickets, ID der Lizenzinformationen, ID des Lizenztickets, Sequenz-ID des Lizenztickets, eindeutige ID des Benutzercomputers, Datum, ab dem das Lizenzticket gültig ist, Datum, bis zu dem das Lizenzticket gültig ist, aktueller Status des Lizenztickets, Version des Ticket-Headers, Lizenzversion, ID des Signaturzertifikats für den Ticket-Header, Prüfsumme der Schlüsseldatei, Seriennummer des Signaturgebers für den Ticket-Header, Authentifizierungstoken.

- Informationen über die auf dem Computer installierte Hardware: Typ, Name, Modellname, Firmware-Version, Parameter der integrierten und angeschlossenen Geräte.

- Informationen über das Gerät: Geräte-ID.

- Informationen zum Betrieb der Komponente Web-Kontrolle:
  Komponentenversion, Kategorisierungsgrund, zusätzliche Informationen zum Kategorisierungsgrund, kategorisierte URL, Host-IP-Adresse des blockierten/kategorisierten Objekts.

Cloud-Modus

Mit dem Schalter **Cloud-Modus** wird der Ausführungsmodus der Anwendung aktiviert bzw. deaktiviert, in dem Kaspersky Endpoint Security eine eingeschränkte Version der Anti-Malware-Datenbanken verwendet. Dieser Modus ist nur verfügbar, wenn die Teilnahme an Kaspersky Security Network aktiviert ist. Wenn Sie die eingeschränkte Version der Anti-Malware-Datenbanken verwenden, wird der Arbeitsspeicher im Vergleich zur Nutzung der vollständigen Datenbanken nur etwa halb so stark belastet. Wenn Sie nicht an Kaspersky Security Network teilnehmen oder der Cloud-Modus deaktiviert ist, lädt Kaspersky Endpoint Security die vollständige Version der Anti-Malware-Datenbanken von den Kaspersky-Servern herunter.

Ist der Schalter aktiviert, verwendet Kaspersky Endpoint Security die eingeschränkte Version der Anti-Malware-Datenbanken. Dadurch werden die Ressourcen des Betriebssystems geschont.

Hinweis: Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die eingeschränkte Version der Anti-Malware-Datenbanken herunter.

Ist der Schalter deaktiviert, verwendet Kaspersky Endpoint Security die vollständige Version der Anti-Malware-Datenbanken.

Hinweis: Nachdem das Kontrollkästchen deaktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Anti-Malware-Datenbanken herunter.

KSN-Erklärung

Mit diesem Link wird ein Fenster geöffnet. Dort können Sie den Text der Erklärung zu Kaspersky Security Network lesen und die Bedingungen für die Teilnahme an Kaspersky Security Network akzeptieren.

Hinweis: Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Web Console verwalten, ist es von den Einstellungen für Kaspersky Security Center abhängig, ob Sie anstelle von Kaspersky Endpoint Security an Kaspersky Private Security Network teilnehmen können. Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, ist eine Teilnahme an Kaspersky Private Security Network nicht möglich. Ausführliche Informationen zur Teilnahme an Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center.

Im Abschnitt **KSN-Proxyeinstellungen** können Sie die Einstellungen für den KSN-Proxy anpassen.

KSN-Proxy verwenden

Dieses Kontrollkästchen aktiviert/deaktiviert die Verwendung eines Proxy-Servers für die Verbindung mit Kaspersky Security Network.

Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security einen Proxy-Server für die Verbindung mit Kaspersky Security Network.

Wenn das Kontrollkästchen deaktiviert ist, stellt Kaspersky Endpoint Security eine direkte Verbindung mit Kaspersky Security Network her.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Kaspersky-Server verwenden, wenn KSN-Proxy nicht verfügbar ist

Dieses Kontrollkästchen aktiviert/deaktiviert die Verwendung der Kaspersky-Dienste, wenn der KSN-Proxy nicht verfügbar ist.

Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security bei Nichtverfügbarkeit des KSN-Proxys die Kaspersky-Server.

Wenn dieses Kontrollkästchen deaktiviert ist, verwendet Kaspersky Endpoint Security bei Nichtverfügbarkeit des KSN-Proxys die Kaspersky-Server nicht.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **KSN-Proxy verwenden** aktiviert ist.

Erzwingen

Wenn der Umschalter **Erzwingen** aktiviert ist, verbietet Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Wenn der Umschalter **Erzwingen** deaktiviert ist, erlaubt Kaspersky Endpoint Security das Ändern von Werten der Aufgabeneinstellungen, der Anwendungseinstellungen und der Richtlinien von Untergruppen und untergeordneten Administrationsservern auf einem lokalen Computer.

Fenster „Teilnahme an Kaspersky Security Network/Kaspersky Private Security Network“

Erfahren Sie mehr

Dieser Link öffnet ein neues Browserfenster. Dort können Sie den Text der Erklärung zu Kaspersky Security Network oder der Erklärung zu Kaspersky Private Security Network lesen.

Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network/Kaspersky Private Security Network.

Die Computer, für welche die Richtlinie gilt, nehmen an Kaspersky Security Network/Kaspersky Private Security Network teil.

Ich lehne die Teilnahmebedingungen für Kaspersky Security Network/Kaspersky Private Security Network ab.

Die Computer, für welche die Richtlinie gilt, nehmen nicht an Kaspersky Security Network/Kaspersky Private Security Network teil.

Hinweis: Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console verwalten, ist eine Teilnahme an Kaspersky Private Security Network nicht möglich. Ausführliche Informationen zur Teilnahme an Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center.

Dialog „Zugriff gewähren“

Wiederherstellungsschlüssel anfordern

Bei Klick auf diese Schaltfläche wird ein Wiederherstellungsschlüssel generiert, der für den Zugriff auf einen verschlüsselten Datenträger auf einem Client-Computer erforderlich ist.

Anwendung über die Befehlszeile verwalten

Sie können das Programm Kaspersky Endpoint Security über die Befehlszeile verwalten.

Hinweis: Nachdem Updates für die Module von Kaspersky Endpoint Security installiert wurden, kann sich die Version des Anwendungs-Clients in der Befehlszeile von der installierten Anwendungsversion unterscheiden.

Syntax der Befehlszeile:

```
kav <Befehl> <Parameter>
```

Jedem Befehl entspricht eine bestimmte Auswahl von unterstützten Parametern.

Hilfe zu Befehlszeilen anzeigen

Mit dem folgenden Befehl können Sie Informationen über die Syntax der Befehlszeile anzeigen:

```
kav -? | help
```

Schadsoftware-Untersuchung ausführen

Syntax des Befehls:

```
kav scan <Untersuchungsbereich> <Aktion> <Dateitypen> <Ausnahmen> <Berichtsparameter>
<erweiterte Parameter>
```

Hinweis: Um eine Schadsoftware-Untersuchung auszuführen, können Sie auch Aufgaben verwenden, die in der Anwendung erstellt wurden. Starten Sie dazu die entsprechende Aufgabe über die Befehlszeile. Die Aufgabe wird mit den Einstellungen ausgeführt, die über die Oberfläche von Kaspersky Endpoint Security festgelegt wurden.

Beschreibungen der Parameter

`<Untersuchungsbereich>` – Dieser Parameter legt eine Liste der Objekte fest, die auf schädlichen Code untersucht werden sollen. Es können mehrere Parameter angegeben werden, die durch Leerzeichen zu trennen sind.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Folgende Werte sind möglich:

- `<Dateien>` – Liste mit den Pfaden der zu untersuchenden Dateien und/oder Ordner. Sie können absolute oder relative Dateipfade verwenden. Die Elemente werden in der Liste durch Leerzeichen getrennt.

  Hinweis: Wenn der Objekt- oder Pfadname ein Leerzeichen oder Sonderzeichen (beispielsweise $, & oder @) enthält, muss entweder der Name in einfache Anführungszeichen (' ') gesetzt werden oder direkt vor jedem Sonderzeichen muss ein Backslash (\) gesetzt werden. Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien und Ordner untersucht.

- `-all` – Vollständige Untersuchung Ihres Computers.
- `-remdrives` – Alle Wechselmedien.
- `-fixdrives` – Alle internen Laufwerke.
- `-netdrives` – Alle Netzlaufwerke.
- `-@:<dateiliste.lst>` – Pfad der Datei mit einer Liste der Objekte und Ordner, die zum Untersuchungsbereich gehören. Die Datei muss das Textformat besitzen und jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Nur ein absoluter Dateipfad ist zulässig.

`<Aktion>` – Dieser Parameter bestimmt die Aktion für schädliche Objekte, die bei der Untersuchung gefunden werden. Wenn dieser Parameter nicht angegeben ist, wird die standardmäßige Aktion ausgeführt, die dem Wert `-i8` entspricht.

Folgende Werte sind möglich:

- `-i0` – Keine Aktion mit dem Objekt ausführen, nur Informationen im Bericht speichern.
- `-i1` – Infizierte Objekte desinfizieren, irreparable Objekte überspringen.
- `-i2` – Infizierte Objekte desinfizieren, irreparable Objekte löschen; Container nicht löschen, außer Containern mit ausführbaren Headern (sfx-Archive).
- `-i3` – Infizierte Objekte desinfizieren, irreparable Objekte löschen; Container vollständig löschen, falls die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
- `-i4` – Infizierte Objekte löschen; Container vollständig löschen, falls die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
- `-i8` – Benutzer nach einer Aktion fragen, wenn ein infiziertes Objekt gefunden wird (Standardwert).
- `-i9` – Benutzer nach einer Aktion fragen, nachdem die Untersuchung abgeschlossen wurde.

`<Dateitypen>` – Dieser Parameter bestimmt die Dateitypen, die bei der Untersuchung untersucht werden. Wenn dieser Parameter nicht angegeben ist, werden nur Dateien untersucht, die potentiell infiziert werden können (basierend auf dem Dateiinhalt).

Folgende Werte sind möglich:

- `-fe` – Nur Dateien untersuchen, die potentiell infiziert werden können (basierend auf dem Dateiinhalt).
- `-fi` – Nur Dateien untersuchen, die potentiell infiziert werden können (basierend auf der Dateierweiterung). Dieser Parameter wird standardmäßig verwendet.
- `-fa` – Alle Dateien untersuchen.

`<Ausnahmen>` – Dieser Parameter bestimmt, welche Objekte von der Untersuchung ausgeschlossen werden sollen. Es können mehrere Parameter angegeben werden, die durch Leerzeichen zu trennen sind.

Folgende Werte sind möglich:

- `-e:a` – Archive nicht untersuchen.
- `-e:b` – E-Mail-Datenbanken nicht untersuchen.
- `-e:m` – E-Mail-Nachrichten im Textformat nicht untersuchen.
- `-e:<Maske>` – Objekte, die der Maske entsprechen, nicht untersuchen.
- `-e:<Sekunden>` – Objekte überspringen, deren Untersuchung länger dauert, als der in Sekunden angegebene Zeitraum.
- `-es:<Größe>` – Objekte überspringen, die größer sind, als der in Megabyte angegebene Wert.

`<Berichtsparameter>` – Diese Parameter bestimmen das Format des Berichts, der die Untersuchungsergebnisse enthält. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn dieser Parameter nicht angegeben ist, werden die Untersuchungsergebnisse angezeigt. Dabei werden alle Ereignisse genannt.

Folgende Werte sind möglich:

- `-r:<Berichtsdatei>` – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- `-ra:<Berichtsdatei>` – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

`<zusätzliche Parameter>` – Parameter für die Verwendung von Untersuchungstechnologien und Konfigurationsdateien:

- `-iSwift=<on|off>` – Verwendung von iSwift aktivieren/deaktivieren.
- `-c:<Konfigurationsdatei>` – Gibt den Pfad der Konfigurationsdatei an, die die Anwendungseinstellungen für Untersuchungsaufgaben enthält. Sie können einen absoluten oder einen relativen Dateipfad angeben. Wenn dieser Parameter nicht angegeben ist, werden neben den Werten, die bereits in der Befehlszeile angegeben sind, jene Werte verwendet, die auf der Anwendungsoberfläche festgelegt sind.

Beispiel:
Die Untersuchung der Ordner ~/Documents, /Applications, und der Datei my test.exe soll gestartet werden:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Die Objekte, die in der Datei objects2scan.txt angegeben sind, sollen untersucht werden. Die Konfigurationsdatei scan_settings.txt soll verwendet werden. Nach der Untersuchung soll ein Bericht für alle Ereignisse erstellt werden:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Beispiel für die Konfigurationsdatei:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Anwendung aktualisieren

Syntax des Befehls:

```
kav update <Update-Quelle> <Berichtsparameter> <erweiterte Parameter
```

Beschreibungen der Parameter

`<Update-Quelle>` – HTTP-Server, Netzwerkordner oder lokaler Ordner, aus dem die Updates heruntergeladen werden. Wenn kein Pfad angegeben ist, wird die Update-Quelle aus den Anwendungseinstellungen für das Update übernommen.

`<Berichtsparameter>` – Diese Parameter bestimmen das Format des Berichts für die Untersuchungsergebnisse. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn dieser Parameter nicht angegeben ist, erscheinen die Update-Ergebnisse auf dem Bildschirm, wobei alle Ereignisse angezeigt werden.

Folgende Werte sind möglich:

- `-r:<Berichtsdatei>` – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- `-ra:<Berichtsdatei>` – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

`<erweiterte Parameter>` – Parameter für die Verwendung einer Konfigurationsdatei

`-c:<Konfigurationsdatei>` – Gibt den Pfad einer Konfigurationsdatei an, welche die Einstellungen für das Update der Anwendung enthält. Sie können einen absoluten oder einen relativen Dateipfad angeben. Wenn der Parameter nicht angegeben ist, werden die Werte verwendet, die auf der Anwendungsoberfläche festgelegt sind.

Beispiel:
Anwendungsdatenbanken aus der standardmäßigen Quelle aktualisieren, alle Ereignisse im Bericht aufzeichnen:

```
kav update -ra:avbases_upd.txt
```

Module von Kaspersky Endpoint Security aktualisieren und dafür die Parameter der Konfigurationsdatei updateapp.ini verwenden:

```
kav update -app=on -c:updateapp.ini
```

Rollback des letzten Updates

Syntax des Befehls:

```
kav rollback <Berichtsparameter>
```

Wichtig: Dieser Befehl erfordert Administratorrechte.

Beschreibungen der Parameter

`<Berichtsparameter>` – Dieser Parameter bestimmt das Format des Berichts, der die Ergebnisse des Update-Rollbacks enthält. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn dieser Parameter nicht angegeben ist, erscheinen die Rollback-Ergebnisse auf dem Bildschirm, wobei alle Ereignisse angezeigt werden.

Folgende Werte sind möglich:

- `-r:<Berichtsdatei>` – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- `-ra:<Berichtsdatei>` – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

Beispiel:
```
kav rollback -ra:rollback.txt
```

Komponente oder Aufgabe starten/beenden

Syntax des Befehls start:

```
kav start <Name der Aufgabe oder Komponente> <Berichtsparameter>>
```

Syntax des Befehls stop:

```
kav stop <Name der Aufgabe oder Komponente>
```

Wichtig: Für den Befehl stop sind Administratorrechte erforderlich.

Beschreibungen der Parameter

`<Name der Aufgabe oder Komponente>` – Geben Sie einen der folgenden Werte an:

- `fm` oder `file_monitoring` – Schutz vor bedrohlichen Dateien
- `wm` oder `web_monitoring` – Schutz vor Web-Bedrohungen
- `ids` – Schutz vor Netzwerkbedrohungen
- `full` oder `scan_my_computer` – Aufgabe „Vollständige Untersuchung“

- `scan_objects` – Aufgabe „Benutzerdefinierte Untersuchung“
- `quick` oder `scan_critical_areas` – Aufgabe „Schnelle Untersuchung“
- `updater` – Update-Aufgabe
- `rollback` – Rollback-Aufgabe

`<Berichtsparameter>` – Diese Parameter bestimmen das Format des Berichts mit den Ergebnissen einer Komponente oder Aufgabe. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn dieser Parameter nicht angegeben ist, richtet sich Kaspersky Endpoint Security bei der Ergebnisanzeige nach den Einstellungen, die auf der grafischen Benutzeroberfläche festgelegt sind.

Hinweis: `<Berichtseinstellungen>` ist nur für die Werte `scan_objects`, `updater` und `rollback` verfügbar.

Folgende Werte sind möglich:

- `-r:<Berichtsdatei>` – Kaspersky Endpoint Security protokolliert nur wichtige Ereignisse in der angegebenen Berichtsdatei.
- `-ra:<Berichtsdatei>` – Kaspersky Endpoint Security protokolliert alle Ereignisse in der angegebenen Berichtsdatei.

Hinweis: Komponenten und Aufgaben, die aus der Befehlszeile gestartet wurden, werden mit den Parametern ausgeführt, die auf der grafischen Benutzeroberfläche festgelegt wurden.

Beispiel:
Um die Komponente „Schutz vor bedrohlichen Dateien“ zu aktivieren, geben Sie in der Befehlszeile folgenden Befehl ein:

```
kav start fm
```

Um die Aufgabe Vollständige Untersuchung über die Befehlszeile abzubrechen, geben Sie folgenden Befehl ein:

```
kav stop scan_my_computer
```

Status und Statistik für eine Komponente oder Aufgabe anzeigen

Syntax des Befehls status:

```
kav status <Name der Aufgabe oder Komponente>
```

Syntax des Befehls statistics:

```
kav statistics <Name der Aufgabe oder Komponente>
```

Beschreibungen der Parameter

`<Name der Aufgabe oder Komponente>` – Geben Sie einen der folgenden Werte an:

- `fm` oder `file_monitoring` – Schutz vor bedrohlichen Dateien
- `wm` oder `web_monitoring` – Schutz vor Web-Bedrohungen
- `Mail_monitoring` – Schutz vor E-Mail-Bedrohungen
- `ids` – Schutz vor Netzwerkbedrohungen
- `firewall` – Firewall
- `behaviordetection` – Verhaltensanalyse
- `exploitprevention` – Exploit-Prävention
- `remediationengine` – Rollback von schädlichen Aktionen
- `devicecontrol` – Gerätekontrolle
- `webcontrol` – Web-Kontrolle
- `full` oder `scan_my_computer` – Aufgabe „Vollständige Untersuchung“
- `scan_objects` – Aufgabe „Benutzerdefinierte Untersuchung“
- `quick` oder `scan_critical_areas` – Aufgabe „Schnelle Untersuchung“
- `externalstoragesscanner` – Aufgabe „Untersuchung von Wechseldatenträgern“
- `updater` – Update-Aufgabe
- `rollback` – Rollback-Aufgabe
- `diskencryption` – FileVault-Volume-Verschlüsselung
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response (KATA)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

Hinweis: Wenn der Befehl status ohne eine Wertangabe für den Parameter `<Name der Aufgabe oder Komponente>` ausgeführt wird, wird der Status aller Aufgaben und Anwendungskomponenten angezeigt. Für den Befehl statistics ist die Angabe eines Werts für den Parameter `<Name der Aufgabe oder Komponente>` obligatorisch.

Schutzeinstellungen exportieren

Syntax des Befehls:

```
kav export <Name der Aufgabe oder Komponente> <Exportdatei>
```

Beschreibungen der Parameter

`<Name der Aufgabe oder Komponente>` – Geben Sie einen der folgenden Werte an:

- `fm` oder `file_monitoring` – Schutz vor bedrohlichen Dateien
- `wm` oder `web_monitoring` – Schutz vor Web-Bedrohungen
- `ids` – Schutz vor Netzwerkbedrohungen
- `full` oder `scan_my_computer` – Aufgabe „Vollständige Untersuchung“
- `scan_objects` – Aufgabe „Benutzerdefinierte Untersuchung“
- `quick` oder `scan_critical_areas` – Aufgabe „Schnelle Untersuchung“
- `updater` – Update-Aufgabe
- `rollback` – Rollback-Aufgabe

`<Exportdatei>` – Pfad der Datei, in welche die Anwendungseinstellungen exportiert werden. Sie können einen absoluten oder einen relativen Dateipfad angeben.

Beispiel:
```
kav export fm fm_settings.txt
```

Anwendung aktivieren

Sie können Kaspersky Endpoint Security durch Verwenden einer Schlüsseldatei aktivieren.

Syntax des Befehls:

```
kav license /add <Schlüsseldatei oder Schlüsselaktivierungscode>
```

Beschreibungen der Parameter

`<Schlüsseldatei>` – Schlüsseldatei für das Programm. Die Schlüsseldatei besitzt die Erweiterung .key.

`<Schlüsselaktivierungscode>` - Aktivierungscode im Format XXXX-XXXX-XXXX-XXXX

Beispiel:

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Systemerweiterung installieren

Syntax des Befehls:

```
kav activatesystemextension /sysext
```

Hinweis: Sie müssen Kaspersky Endpoint Security in der Systemeinstellung **Datenschutz & Sicherheit** Berechtigungen gewähren, um die Installation der Erweiterung abzuschließen.

Netzwerkverbindungen konfigurieren

Sie können Netzwerkverbindungen für die Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“ konfigurieren.

Syntax des Befehls:

```
kav activatesystemextension /webav
```

Hinweis: Sie müssen Kaspersky Endpoint Security Berechtigungen für die Filterung von Netzwerkinhalten gewähren, um die Konfiguration abzuschließen.

Lizenzschlüssel löschen

Sie können alle Lizenzschlüssel löschen, die momentan in der Anwendung vorhanden sind.

Syntax des Befehls:

```
kav license /del
```

Wichtig: Dieser Befehl erfordert Administratorrechte.

Rückgabecodes der Befehlszeile

Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Die Rückgabecodes umfassen sowohl allgemeine Codes als auch spezifische Codes für eine konkrete Aufgabe.

Syntax des Befehls zum Anfordern eines Rückgabecodes:

```
echo $?
```

Allgemeine Rückgabecodes:

- `0` – Der Vorgang wurde erfolgreich ausgeführt.
- `1` – Ungültiger Parameterwert.
- `2` – Unbekannter Fehler.
- `3` – Fehler bei Ausgabenausführung.
- `4` – Die Aufgabe wurde abgebrochen.

Rückgabecodes für Untersuchungsaufgaben:

- `101` – Alle schädlichen Objekte wurden verarbeitet.
- `102` – Es wurden schädliche Objekte erkannt.

Anwendung beenden

Syntax des Befehls:

```
kav exit
```

Wichtig: Dieser Befehl erfordert Administratorrechte.

Anwendung deinstallieren

Um Kaspersky Endpoint Security über die Befehlszeile zu deinstallieren, verwenden Sie die folgende Reihenfolge von Befehlen:

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
```

```
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

Wichtig: Zum Ausführen der Deinstallation der Anwendung sind Administratorrechte erforderlich.

Befehle zur Verwaltung von Detection and Response

Sie können die Befehlszeile verwenden, um die integrierten Funktionen der Lösung „Detection and Response“ zu verwalten. Sie können die „Detection and Response“-Lösungen verwalten, wenn die Verwaltung über die Kaspersky Security Center-Konsole nicht möglich ist.

Ausführungsprävention verwalten

Sie können die Einstellungen für die Ausführungsprävention des Client-PCs anzeigen und die Ausführungsprävention auf dem Client-PC deaktivieren.

Syntax des Befehls:

```
kav prevention </disable | /show>
```

Befehlsbeschreibungen

`/disable` - Befehl zum Deaktivieren der Ausführungsprävention auf dem Client-PC

`/show` – Befehl zum Anzeigen der aktuellen Einstellungen der Ausführungsprävention, einschließlich ihres Modus und der Liste mit den Regeln der Ausführungsprävention

Netzwerkisolation verwalten

Sie können die Einstellungen für die Netzwerkisolation des Hosts anzeigen und die Netzwerkisolation auf dem Host deaktivieren.

Syntax des Befehls:

```
kav isolation </off | /status>
```

Befehlsbeschreibungen

`/off` – Befehl zum Deaktivieren der Netzwerkisolation

Wichtig: Dieser Befehl erfordert Administratorrechte.

`/status` – Befehl zum Anzeigen des Status der Netzwerkisolation und ihrer Ausnahmen

Hinweis: Diese Befehle müssen gleichzeitig ausgeführt werden.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können, und nennt die dafür notwendigen Voraussetzungen.

So erhalten Sie technische Unterstützung

Wenn Sie in der Dokumentation oder in den Informationsquellen zu Kaspersky Endpoint Security keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky. Die Mitarbeiter des Technischen Supports beantworten alle Ihre Fragen zur Installation und zur Verwendung von Kaspersky Endpoint Security.

Hinweis: Kaspersky bietet Support für Kaspersky Endpoint Security während des Lebenszyklus dieser App (siehe Seite zum Produktsupport-Lebenszyklus). Bitte beachten Sie die Support-Regeln, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Durch Besuch der Website des Technischen Supports
- Durch Senden einer Anfrage an den Technischen Support über das Portal Kaspersky CompanyAccount

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Programme von Kaspersky verwenden. Im Portal Kaspersky CompanyAccount können sich Benutzer über Online-Anfragen mit den Kaspersky-Experten austauschen. Mit dem Kaspersky CompanyAccount können Sie den Status Ihrer Online-Anfragen überprüfen und ihren Verlauf speichern.

Sie können alle Mitarbeiter Ihres Unternehmens unter einem Universalkonto bei Kaspersky CompanyAccount registrieren. Mithilfe eines Universalkontos können Sie die Online-Anfragen der bei Kaspersky registrierten Mitarbeiter zentral bearbeiten und die Berechtigungen dieser Mitarbeiter über Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch

- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Details zu Kaspersky CompanyAccount finden Sie auf der Website des Technischen Supports.

Informationen für den Technischen Support abrufen

Es kann es sein, dass Sie von den Support-Experten dazu aufgefordert werden, die Anwendungseinstellungen vorübergehend zu ändern. Diese Maßnahme ermöglicht es, den Support effektiver zu gestalten und eine Fehlerdiagnose vorzunehmen. Dafür können folgende Aktionen erforderlich sein:

- Aktivierung der Funktion zur Extraktion erweiterter Diagnoseinformationen.
- Anpassen spezieller Einstellungen für bestimmte Anwendungskomponenten, die über die standardmäßige Anwendungsoberfläche nicht verfügbar sind.
- Änderung der Einstellungen für die Übertragung von extrahierten Diagnoseinformationen.

Alle Informationen, die für die oben genannten Aktionen erforderlich sind, sowie Informationen über den Umfang der im Rahmen der Fehlersuche zu erfassenden Daten werden Ihnen von den Support-Experten mitgeteilt. Die zusätzlich extrahierten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Die Daten werden nicht automatisch an Kaspersky gesendet.

Protokolldatei verwenden

Wenn Sie sich mit einem Problem an den Technischen Support von Kaspersky wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über Kaspersky Endpoint Security zu erstellen und diesen an den Support zu schicken. Außerdem können die Kaspersky-Experten für Technischen Support eine *Protokolldatei* von Ihnen anfordern. Die Protokolldatei ermöglicht eine schrittweise Analyse der ausgeführten Anwendungsbefehle und der Fehlerursachen.

Protokolldatei erstellen

Die Protokollierung ist eine effektive Methode, um ausführliche Informationen über die Anwendungsaktivität aufzuzeichnen. Die Experten des Technischen Supports verwenden die Protokolldateien, um aufgetretene Probleme zu beheben.

Protokolldatei erstellen

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Protokollierung** das Kontrollkästchen **Protokollierung aktivieren**.

Wichtig: Es wird empfohlen, die Protokollierung nur auf Anfrage eines Kaspersky-Support-Experten zu aktivieren.

Protokolldateien können viel Festplattenplatz beanspruchen. Wenn Sie keine Protokolldateien mehr benötigen, deaktivieren Sie die Protokollierung.

Protokollierung deaktivieren

1. Klicken Sie in der Menüleiste auf das App-Symbol und wählen Sie **Einstellungen** aus.

   Das Fenster mit Anwendungseinstellungen wird geöffnet.

2. Deaktivieren Sie auf der Registerkarte **Benutzeroberfläche** im Abschnitt **Protokollierung** das Kontrollkästchen **Protokollierung aktivieren**.

In einer Protokolldatei für Kaspersky Endpoint Security werden folgende Informationen gespeichert:

- Informationen über das Gerät und das Betriebssystem (einmalige Geräte-ID, Gerätetyp, MAC-Adresse der Netzwerkgeräte, Typ des Betriebssystems, Version des Betriebssystems).
- Informationen über die Funktion der Anwendung und ihrer Module.
- Informationen über das Abonnement (Abonnementtyp, Region).
- Informationen über die Sprache (Gebietsschema), Anwendungs-ID, Anpassung der Anwendung, Anwendungsversion, einmalige Installations-ID der Anwendung, einmalige Computer-ID.
- Informationen über den Status des Anti-Malware-Schutzes auf dem Computer, sowie über alle verarbeiteten und erkannten Objekte (Name des erkannten Objekts, Datum und Uhrzeit des Fundes, Webadresse, von der das Objekt heruntergeladen wurde, Namen, Größen und Pfade von infizierten Dateien, IP-Adresse des angreifenden Computers und Nummer des angegriffenen Ports des Computers, Liste der Schadsoftware-Aktivitäten und unerwünschte Webadressen), und relevante Aktionen und Entscheidungen, die von der Anwendung und vom Benutzer getroffen wurden.
- Informationen über Anwendungen, die vom Benutzer heruntergeladen wurden (Webadresse, Attribute, Dateigröße, und Informationen zum Prozess, der den Download initiiert hat).
- Informationen zu laufenden Anwendungen und Anwendungsmodulen (Größe, Attribute, Erstellungsdatum, Informationen zum PE-Header, Region, Name, Ort und Packprogramme).
- Informationen über Schnittstellenfehler und über die Nutzung der Schnittstelle der installierten Kaspersky-Anwendung.
- Informationen über Netzwerkverbindungen: IP-Adresse des Remote-Computers und des Computers des Endbenutzers, Nummern der Ports, mit denen die Verbindung hergestellt wurde, und Netzwerkprotokoll der Verbindung.

- Informationen über Netzwerkpakete, die der Computer über IT-Netzwerke und Telekommunikationsnetze empfangen und gesendet hat.
- Informationen über gesendete und empfangene E-Mail-Nachrichten und IM-Nachrichten.
- Informationen über besuchte Webadressen: Zeitpunkt, zu dem die Verbindung unter Verwendung eines offenen Protokolls hergestellt wurde, Daten über den Benutzernamen und das Kennwort für die Website, und Inhalt von Cookies.
- Öffentliches Serverzertifikat.

Protokolldateien enthalten nur die Informationen, die erforderlich sind, um Beschädigungen in der Anwendung zu reparieren. Kaspersky verwendet Ablaufverfolgungsdateien, um Ereignisse zu untersuchen, die mit Funktionsfehlern des Programms Kaspersky Endpoint Security zusammenhängen.

Die Erstellung von Protokolldateien ist standardmäßig deaktiviert. Sie können die Erstellung von Protokolldateien in den Anwendungseinstellungen aktivieren.

Ablaufverfolgungsdateien können nur manuell an Kaspersky geschickt werden. Das Programm sendet Ablaufverfolgungsdateien nicht automatisch an Kaspersky.

Sie können auswählen, auf welche Weise Ablaufverfolgungsdateien an Kaspersky geschickt werden sollen.

Bitte überprüfen Sie die Daten, die in Ablaufverfolgungsdateien enthalten sind, bevor Sie solche Dateien an Kaspersky senden.

Wichtig: Protokolldateien können persönliche oder sensible Informationen enthalten. Wenn Sie Ablaufverfolgungsdateien an Kaspersky senden, erklären Sie sich damit einverstanden, Kaspersky alle in den Protokolldateien enthaltenen Daten bereitzustellen, und Sie akzeptieren die entsprechende Versandmethode.

Informationsquellen für die Anwendung

Seite für Kaspersky Endpoint Security auf der Kaspersky-Website

Auf der Seite für Kaspersky Endpoint Security auf der Kaspersky-Website finden Sie allgemeine Informationen über das Programm sowie über seine Funktionen und Besonderheiten.

Seite für Kaspersky Endpoint Security in der Wissensdatenbank

Die *Wissensdatenbank* ist ein spezieller Bereich auf der Website des Technischen Supports von Kaspersky.

Auf der Seite des Programms finden Sie in der Wissensdatenbank Artikel mit nützlichen Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Die Artikel der Wissensdatenbank behandeln Fragen zu Kaspersky Endpoint Security und anderen Kaspersky-Anwendungen. Die Artikel in der Wissensdatenbank können auch Neuigkeiten über den Technischen Support von Kaspersky enthalten.

Über das Pulldown-Menü „Hilfe“ zur Wissensdatenbank wechseln

1. Wählen Sie den Punkt **Hilfe** > **Support** aus.
2. Klicken Sie auf **Technischer Support**.

Im Kaspersky-Support-Forum über Kaspersky-Anwendungen diskutieren

Wenn Ihre Frage nicht dringend ist, können Sie mit Kaspersky-Experten und anderen Benutzern in unserem Forum darüber diskutieren.

Im Forum können Sie Diskussionsthemen nachlesen, Kommentare schreiben und neue Themen zur Diskussion stellen.

Über das Pulldown-Menü 'Hilfe' zum Forum wechseln

1. Wählen Sie **Hilfe** > **Support**.
2. Klicken Sie auf **Community**.

Hinweis: Für den Zugriff auf die Online-Ressourcen ist eine Internetverbindung erforderlich.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky.

Hilfematerialien, die in Anwendung enthalten sind

Die Anwendung enthält eine vollständige Hilfe sowie Kontexthilfe.

Die vollständige Hilfe bietet Informationen zur Konfiguration und Verwendung von Kaspersky Endpoint Security.

Die Kontexthilfe bietet Informationen über die Fenster von Kaspersky Endpoint Security, beschreibt die Einstellungen von Kaspersky Endpoint Security und enthält Links zu Beschreibungen der Aufgaben, in denen diese Einstellungen verwendet werden.

Die Hilfe kann im Installationspaket enthalten sein oder befindet sich auf der Kaspersky-Website. Zum Anzeigen der Online-Hilfe ist eine Internetverbindung erforderlich.

Online-Hilfe (diese Hilfe)

In dieser Hilfe finden Sie Informationen zu folgenden Themen:

- Installation der Anwendung vorbereiten, Anwendung installieren und aktivieren.
- Anwendung konfigurieren und verwenden.
- Anwendung per Remote-Zugriff über Kaspersky Security Center verwalten.

Anhänge

Dieser Abschnitt bietet zusätzliche Informationen.

Bekannte Probleme und Beschränkungen

Kaspersky Endpoint Security weist folgende bekannte Probleme und Einschränkungen auf:

- Wenn auf Ihrem Computer eine Anwendung installiert ist, die Informationen sammelt und zur Verarbeitung sendet, klassifiziert das Programm Kaspersky Endpoint Security diese Anwendung möglicherweise als schädlich. Um dies zu vermeiden, können Sie die Anwendung von der Untersuchung ausschließen, indem Sie das Programm Kaspersky Endpoint Security so konfigurieren, wie es in diesem Dokument beschrieben wird.
- Funktionale Einstellungen der Anwendung lassen sich durch Bearbeiten der Konfigurationsdateien modifizieren.
- In Kaspersky Security Center können lokale Aufgaben doppelt in den Eigenschaften von verwalteten Geräten erscheinen.
- Wenn die Update-Quelle für eine lokale Update-Aufgabe geändert wird, wird die automatische Ausführung der Update-Aufgabe deaktiviert.
- Wenn Sie eine Aufgabe zum Neustart des Computers über die Verwaltungskonsole mit einer Nachricht an den Benutzer starten, die ein Semikolon (;) enthält, wird die Aufgabe als abgeschlossen angezeigt, der Benutzer wird jedoch nicht aufgefordert, den Mac neu zu starten.
- Um den Safari-Netzwerkverkehr von der Untersuchung durch Kaspersky Endpoint Security auszuschließen, müssen Sie die folgenden Pfade zur Ausnahmeliste hinzufügen:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- Um den Google Chrome-Netzwerkverkehr von der Untersuchung durch Kaspersky Endpoint Security auszuschließen, müssen Sie den folgenden Pfad zur Ausnahmeliste hinzufügen:
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- Nachdem Sie mithilfe von Kaspersky Security Center Web Console und Cloud Console ein Richtlinienprofil für eine Kaspersky Endpoint Security-Richtlinie erstellt haben, müssen Sie überprüfen, ob die Einstellungen auf den Client-Computern korrekt angewendet wurden.
- Wenn die FileVault-Volume-Verschlüsselung in den Richtlinieneinstellungen aktiviert ist, können Benutzer mit Administratorrechten ihr Mac-Startvolume über die Systemeinstellungen entschlüsseln.

- Änderungen in den Proxy-Server-Optionen werden erst nach einem Neustart von Kaspersky Endpoint Security übernommen.
- Zu einer Website mit einem nicht vertrauenswürdigen Zertifikat stellt Safari möglicherweise keine Verbindung her. Sie können eine solche Website entweder zu den Ausnahmen hinzufügen oder einen anderen Browser verwenden.
- Nachdem Kaspersky Endpoint Security 11.2 oder höher per Fernzugriff über Kaspersky Security Center deinstalliert wurde, verbleibt unter Umständen eine der Systemerweiterungen der Anwendung im Arbeitsspeicher des Computers. Danach kann es bei der Installation von Kaspersky Endpoint Security in seltenen Fällen zu einem Problem mit der Berechtigung für den Festplattenvollzugriff kommen. In diesem Fall empfehlen wir, die Deinstallation der Anwendung lokal durchzuführen und es anschließend erneut zu installieren.
- Anwendungen, für die Rosetta eine Voraussetzung ist, können möglicherweise nicht installiert werden, wenn gleichzeitig Kaspersky Endpoint Security ausgeführt wird. Um das Problem zu beheben, versuchen Sie Kaspersky Endpoint Security zu beenden und die Installation erneut auszuführen.
- Alarmdetails für Bedrohungen, die in zusammengesetzten Objekten erkannt wurden, enthalten nur Informationen über das erkannte Objekt selbst und kein Diagramm der Entwicklungskette der Bedrohung.
- Beim Speichern eines Kennworts für den Kennwortschutz kann ein Fehler auftreten. In diesem Fall wird es empfohlen, die Anwendung zu deinstallieren und erneut zu installieren.
- Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.
- Sie können kein Objekt untersuchen, das durch die Aufgabe „Datei in die Quarantäne verschieben“ in die Quarantäne verschoben wurde.
- In Kaspersky Security Center wird der Gerätename nur dann korrekt angezeigt, wenn NetBIOS-Name, Computername und Hostname übereinstimmen.

Liste der Objekte, die nach Erweiterung untersucht werden

Wenn Sie in Kaspersky Security Center eine Untersuchungsaufgabe erstellt und dabei in den Untersuchungseinstellungen die Option **Anwendungen und Dokumente nach Erweiterung untersuchen** ausgewählt haben, untersucht Kaspersky Endpoint Security sowohl Objekte ohne Dateierweiterungen als auch Objekte mit den folgenden Erweiterungen:

Allgemeine Formate:

- txt
- csv

- htm
- html

Multimediadateien (Audio/Video):

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3

- mpeg3
- flac
- ape
- ogg
- aac
- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

Grafikdateien:

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff

- emf
- wmf
- eps
- psd
- cdr
- swf

Ausführbare Dateien und Systemdateien:

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm

- sh
- pl
- dylib

Dokumente und Vorlagen:

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx

- ppsm
- rtf
- pdf
- msg
- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

Archive:

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

Hinweis: Das tatsächliche Format einer Datei kann sich von der Dateinamenserweiterung unterscheiden.

Masken für die Pfade von Dateien und Ordnern

Der Name einer Dateimaske oder *der Name einer Namensmaske* stellt mithilfe von Platzhaltern den Namen und die Erweiterung einer Datei oder den Namen eines Ordners dar.

Diese Zeichen können Sie zur Angabe des Schutzbereichs, des Untersuchungsbereichs und der vertrauenswürdigen Zone verwenden:

- Das Tilde-Symbol (`~`) steht für `/Users/<Benutzername>` in einem Datei- oder Ordnerpfad. Beispielsweise bedeutet der Pfad `~/Desktop` dass der Schutzbereich Desktop-Ordner aller Benutzer auf den zu schützenden Computern umfasst.

- Das Sternchensymbol (`*`) steht für eine beliebige Zeichenkombination in einem Datei- oder Ordnernamen. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `/*/*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich in Ordnern auf dem internen Datenträger befinden, allerdings nicht in untergeordneten Ordnern.

- Zwei aufeinanderfolgende Sternchensymbole (`**`) stehen für eine beliebige Zeichenkombination (auch eine leere Zeichenfolge) in einem Datei- oder Ordnernamen, einschließlich der Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `/Folder/**/*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich im Ordner „Folder“ und in dessen Unterordnern befinden. Die Maske muss mindestens eine Verschachtelungsebene enthalten. Die Maske `/**/*.txt` ist ungültig.

- Das Fragezeichen (`?`) steht für ein beliebiges Einzelzeichen in einem Datei- oder Ordnernamen. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `/Folder/???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen „Folder“ enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

Anforderungen an IOC-Dateien

Beachten Sie beim Erstellen von IOC-Untersuchungsaufgaben die folgenden Anforderungen und Einschränkungen für IOC-Dateien.

- Für die Beschreibung von Kompromittierungsindikatoren unterstützt das Programm IOC-Dateien mit IOC-, XLM- und JSON-Erweiterungen im offenen Standard OpenIOC Version 1.0 und 1.1 oder STIX Version 2.0 und 2.1.

- Wenn Sie beim Erstellen einer IOC-Untersuchungsaufgabe über die Befehlszeile IOC-Dateien hochladen, von denen einige nicht unterstützt werden, verwendet die Anwendung beim Ausführen der Aufgabe nur die unterstützten IOC-Dateien. Wenn sich beim Erstellen einer IOC-Untersuchungsaufgabe über die Befehlszeile herausstellt, dass keine der hochgeladenen IOC-Dateien unterstützt wird, kann die Aufgabe trotzdem ausgeführt werden. in diesem Fall werden jedoch keine Kompromittierungsindikatoren gefunden. Es ist nicht möglich, nicht unterstützte IOC-Dateien über die Web Console oder Cloud Console hochzuladen.

- Semantische Fehler sowie nicht unterstützte IOC-Ausdrücke und Tags in den IOC-Dateien führen nicht dazu, dass die Ausführung der Aufgabe fehlschlägt. Für solche Abschnitten in den IOC-Dateien erkennt die Anwendung keine Übereinstimmung.

- Die IDs aller IOC-Dateien, die innerhalb einer IOC-Untersuchungsaufgabe verwendet werden, müssen eindeutig sein. Sollten IOC-Dateien mit derselben ID vorhanden sind, kann sich dies auf die Ergebnisse der Aufgabenausführung auswirken.

- Eine IOC-Datei darf maximal 2 MB groß sein. Größere Dateien führen zu einem Fehlerabbruch von IOC-Untersuchungsaufgaben. Die Gesamtgröße aller zur IOC-Sammlung hinzugefügten Dateien sollte maximal 10 MB betragen. Wenn die Gesamtgröße aller Dateien 10 MB überschreitet, müssen Sie die IOC-Sammlung aufteilen und mehrere IOC-Untersuchungsaufgaben erstellen.

- Es wird empfohlen, pro Bedrohung eine IOC-Datei zu erstellen. Dies erleichtert die Ergebnisanalyse der IOC-Untersuchungsaufgabe.

Die folgenden Tabelle nennt die Funktionen, die die Anwendung für IOC-Dateien unterstützt, sowie entsprechende Einschränkungen.

Funktionen und Einschränkungen der Unterstützung für IOC-Dokumente.

Unterstützte Bedingungen	OpenIOC 1.0:
	
	`is`
	`isnot` (als Ausnahme der Menge)
	`contains`
	`containsnot` (als Ausnahme der Menge)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	STIX 2.0 and 2.1:
	
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`matches`

Unterstützte Attribute der Bedingungen	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Unterstützte Operatoren	`AND` `OR`
Unterstützte Datentypen	`"date"`: Datum (anwendbare Bedingungen: `is`, `greater-than`, `less-than`) `"int"`: Integer (anwendbare Bedingungen: `is`, `greater-than`, `less-than`) `"string"`: String (anwendbare Bedingungen: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: Dauer in Sekunden (anwendbare Bedingungen: `is`, `greater-than`, `less-than`)

Besonderheiten der Datentypinterpretation	Die folgenden Datentypen werden String interpretiert: `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` und `"base64Binary"`.
	
	Das Programm unterstützt die Interpretation der Einstellung `Content` für die Datentypen `int` und `date`, wenn Intervalle angegeben werden:
	
	OpenIOC 1.0:
	Verwendung des Operators `TO` im Feld `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Verwendung der Bedingungen `greater-than` und `less-than`
	Verwendung des Operators `TO` im Feld `Content`
	Das Programm unterstützt die Interpretation der Datentypen `date` und `duration`, wenn die Indikatoren im Format `ISO 8601`, `Zulu Time Zone`, `UTC format` angegeben werden.

Unterstützte Skriptinterpreter der Ausführungsprävention

Die Ausführungsprävention unterstützt die folgenden Skriptinterpreter:

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Wichtig: Wenn die Skriptinterpreter PkgUtil oder PkgInstaller bereits geöffnet sind und ein in den Regeln der Ausführungsprävention angegebenes Skript öffnen, wird die Ausführung des Skriptes nicht blockiert.

Zertifikat von Kaspersky Endpoint Security dem Zertifikatspeicher von Mozilla Firefox hinzufügen

Wenn der Browser den Zertifikatspeicher von Mozilla Firefox verwendet, müssen Sie das Kaspersky-Zertifikat exportieren und manuell zu diesem Zertifikatspeicher hinzufügen. Andernfalls kann der Browser keine HTTPS-Seiten öffnen.

Exportieren Sie das Kaspersky Zertifikat

1. Öffnen Sie auf Ihrem Mac **Launchpad** > **Andere** > **Schlüsselbundverwaltung**.
2. Klicken Sie im linken Bereich des Fensters auf **System** und öffnen Sie die Registerkarte **Zertifikate**.
3. Suchen Sie in der Liste der Zertifikate nach der **Zertifizierungsstelle für Kaspersky Web Anti-Virus**.
4. Klicken Sie mit der rechten Maustaste auf dieses Zertifikat und wählen Sie **Zertifizierungsstelle für Kaspersky Web Anti-Virus exportieren** aus.
5. Wählen Sie einen Speicherort für das Zertifikat aus und klicken Sie auf **Speichern**.

Das Kaspersky-Zertifikat wird gespeichert.

Kaspersky-Zertifikat zum Zertifikatspeicher von Mozilla Firefox hinzufügen

1. Öffnen Sie Mozilla Firefox.
2. Klicken Sie oben rechts auf die Menüschaltfläche und wählen Sie **Einstellungen** aus.
3. Wählen Sie im linken Fensterbereich **Datenschutz & Sicherheit** aus.
4. Scrollen Sie nach unten zum Abschnitt **Zertifikate**.
5. Klicken Sie auf **Zertifikate anzeigen**.
6. Klicken Sie im folgenden Fenster auf **Importieren**.
7. Wählen Sie die Kaspersky-Zertifikatsdatei aus und klicken Sie auf **Öffnen**.
8. Aktivieren Sie die Kontrollkästchen **Dieser Zertifizierungsstelle vertrauen, um Websites zu identifizieren** und **Dieser Zertifizierungsstelle vertrauen, um E-Mail-Benutzer zu identifizieren**. Klicken Sie auf **OK**.

   Das Kaspersky-Zertifikat wird in den Zertifikatspeicher von Mozilla Firefox importiert. Es wird in der Liste der Zertifikate im Fenster **Zertifikatsverwaltung** angezeigt.

Wichtig: Bei jeder Neuinstallation von Kaspersky Endpoint Security wird ein neues Kaspersky-Stammzertifikat erstellt. Das bedeutet, dass Sie diesen Vorgang nach jeder Neuinstallation von Kaspersky Endpoint Security ausführen müssen.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt im Installationsordner der Anwendung enthalten.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

App Store, Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, Mac Pro, macOS, Rosetta, Safari und Xcode sind Markenzeichen von Apple Inc.

IOS ist eine in den USA und in anderen Ländern eingetragene Marke oder ein Dienstleistungszeichen von Cisco Systems, Inc. und/oder ihrer verbundenen Unternehmen.

Android, Chrome, Chromium, Google und Google Chrome sind Markenzeichen von Google LLC.

Intel ist ein Markenzeichen der Intel Corporation oder ihrer Tochtergesellschaften.

Linux ist die eingetragene Marke von Linus Torvalds in den USA und anderen Ländern.

Excel, IIS, Internet Explorer, Microsoft, Microsoft Edge, Windows, Windows Installer, Windows Phone und WMI sind Markenzeichen der Microsoft-Unternehmensgruppe.

Firefox und Mozilla sind Markenzeichen der Mozilla Foundation in den USA und anderen Ländern.

Java und JavaScript sind eingetragene Marken von Oracle und/oder deren Tochtergesellschaften.

Parallels, das Parallels-Logo und Coherence sind Markenzeichen oder eingetragene Markenzeichen der Parallels International GmbH.

VMware und VMware Fusion sind eingetragene Markenzeichen und/oder Markenzeichen von VMware, Inc. in den USA und anderen Ländern.

JAMF und Composer sind in den USA und anderen Ländern eingetragene Markenzeichen oder nicht eingetragene Marken von JAMF SOFTWARE, LLC.

Fenster „Kennwortgeschütztes Archiv wurde erkannt“

Wenn Kaspersky Endpoint Security ein kennwortgeschütztes Archiv untersuchen muss, während der „Schutz vor bedrohlichen Dateien“ oder eine Untersuchungsaufgabe ausgeführt wird, erscheint ein Benachrichtigungsfenster.

Archiv

Pfad zum Archiv.

Kennwort

Eingabefeld für das Kennwort

Wenn Sie das Kennwort eingeben, untersucht Kaspersky Endpoint Security das Archiv auf Malware und andere Sicherheitsbedrohungen.

Geschützte Archive überspringen

Bei Klick auf diese Schaltfläche werden das Objekt und alle Objekte des gleichen Typs übersprungen.

Überspringen

Bei Klick auf diese Schaltfläche wird das Objekt übersprungen.

Der Dialog „Proxyserver-Authentifizierung erforderlich“

Benutzername

Eingabefeld für den Benutzernamen für eine Verbindung mit dem Proxy-Server.

Kennwort

Eingabefeld für das Kennwort

Kennwort merken

Dieses Kontrollkästchen aktiviert/deaktiviert die künftige Verwendung des angegebenen Benutzernamens und des Kennworts für die Authentifizierung auf dem Proxy-Server.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Dialog „Objekt wurde gefunden“

Wenn Kaspersky Endpoint Security einen Virus oder eine andere Sicherheitsbedrohung findet, wird auf dem Bildschirm ein Meldungsfenster angezeigt.

Erkannt

Name des Objekts gemäß der Klassifizierung der Viren-Enzyklopädie von Kaspersky.

Details

Diese Schaltfläche öffnet eine Seite in der Viren-Enzyklopädie von Kaspersky. Dort finden Sie Informationen über das gefundene Objekt.

Objekt

Pfad des Ordners mit dem gefundenen Objekt oder die Webadresse, unter der das Objekt gefunden wurde.

Aktion auf alle anwenden

Mit diesem Kontrollkästchen wird die ausgewählte Aktion für alle Objekte des gleichen Typs aktiviert bzw. deaktiviert. Diese Auswahl gilt für die laufende Sitzung des „Schutzes vor bedrohlichen Dateien“, des „Schutzes vor Web-Bedrohungen“ oder einer Untersuchungsaufgabe.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Als laufende Sitzung für den „Schutz vor bedrohlichen Dateien“ oder den „Schutz vor Web-Bedrohungen“ gilt der Zeitraum vom Start bis zum Beenden der Komponente oder bis zum Beenden oder dem Neustart der Anwendung. Als laufende Sitzung für eine Untersuchungsaufgabe gilt der Zeitraum vom Start bis zum Abschluss der Aufgabe.

Die Schaltflächen mit den Aktionen, die mit gefundenen Objekten ausgeführt werden können, variieren je nach dem Typ des gefundenen Objekts.

Sie können eine der folgenden Aktionen auswählen:

- **Desinfizieren**. Objekt desinfizieren. Vor der Desinfektion legt Kaspersky Endpoint Security eine Backup-Kopie der Datei an, damit Sie die Originaldatei gegebenenfalls wiederherstellen können.
- **Löschen**. Objekt löschen. Vor dem Löschen legt Kaspersky Endpoint Security eine Backup-Kopie der Datei an, damit Sie die Originaldatei gegebenenfalls wiederherstellen können.
- **Nicht blockieren**. Zugriff auf eine Website erlauben, die als gefährliches Objekt im Web-Datenverkehr gilt.
- **Blockieren**. Zugriff auf eine Website verbieten, die als gefährliches Objekt im Web-Datenverkehr gilt.
- **Archiv löschen**. Archiv löschen, in dem sich das gefundene Objekt befindet.
- **Geschützte Archive überspringen**. Kennwortgeschützte Archive bei der Untersuchung auf Malware überspringen.
- **Überspringen**. Zugriff auf das Objekt blockieren, aber keine Aktionen mit dem Objekt vornehmen.

Fenster „Untersuchung“



Bei Klick auf diese Schaltfläche kehrt Kaspersky Endpoint Security zum vorherigen Fenster zurück.



Bei Klick auf diese Schaltfläche wechselt Kaspersky Endpoint Security zum nächsten Fenster.



Bei Klick auf diese Schaltfläche werden im Fenster **Untersuchung** alle Einträge für alle Aufgaben zur Malware-Untersuchung gelöscht.

Untersuchungszeitplan

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie einen Zeitplan für die Vollständige Untersuchung und für die Schnelle Untersuchung festlegen können.

Schnelle Untersuchung

Wenn Sie in diesem Abschnitt auf die Starten-Schaltfläche ( ) klicken, wird die Aufgabe „Schnelle Untersuchung“ ausgeführt.

Vollständige Untersuchung

Wenn Sie in diesem Abschnitt auf die Starten-Schaltfläche ( ) klicken, wird die Aufgabe „Vollständige Untersuchung“ ausgeführt.

Durch Klick auf diese Schaltfläche wird die ausgewählte Untersuchungsaufgabe abgebrochen.

Diese Schaltfläche wird angezeigt, wenn eine Untersuchungsaufgabe ausgeführt wird.

Einstellungen

Wenn Sie auf diese Schaltfläche klicken, wird die Registerkarte **Untersuchung** geöffnet, auf der Sie die Einstellungen für Untersuchungsaufgaben anpassen können.

Auswählen

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie eine Datei oder einen Ordner für die Untersuchung wählen können.

Im unteren Bereich des Abschnitts **Dateien und Ordner** sehen Sie die Einträge aller Aufgaben zur Untersuchung auf Malware, die für die ausgewählten Dateien oder Ordner ausgeführt wurden.

Details

Durch Klick auf diese Schaltfläche wird ein Berichtsfenster für die Untersuchungsaufgabe geöffnet.

Diese Schaltfläche erscheint, wenn Sie mit dem Mauszeiger auf eine Untersuchungsaufgabe zeigen.

Untersuchungsverlauf leeren

Wenn Sie auf diese Schaltfläche klicken, werden alle Einträge aller Aufgaben zur Schadsoftware-Untersuchung gelöscht.

Alle einblenden

Mit dieser Schaltfläche wird das Fenster **Erkannte Objekte** geöffnet, in dem alle gefundenen Objekte angezeigt werden.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Das Fenster „Gefundene Objekte“

Der Abschnitt **Erkannte Objekte** enthält schädliche Objekte, die vom Programm gefunden wurden.

Alle desinfizieren

Mit dieser Schaltfläche wird die Desinfektion für alle gefundenen infizierten Objekte gestartet.

Alle ignorieren

Mit dieser Schaltfläche werden alle schädlichen Objekte aus der Liste der schädlichen Objekte im Abschnitt **Erkannte Objekte** gelöscht.

•••

Durch Klick auf diese Schaltfläche wird ein Pop-up-Menü geöffnet, in dem Sie eine der folgenden Aktionen für ein schädliches Objekt auswählen können:

- **Desinfizieren**. Objekt desinfizieren. Vor der Desinfektion legt das Programm Kaspersky Endpoint Security eine Backup-Kopie der Datei an, damit die Datei später gegebenenfalls wiederhergestellt oder desinfiziert werden kann, ohne einen Datenverlust zu riskieren.
- **Ignorieren**. Objekt aus der Liste der gefundenen Objekte löschen.

Der Abschnitt **Andere Objekte** enthält gefundene Objekte, die zwar nicht schädlich sind, mit denen Hacker aber trotzdem Ihren Computer oder Ihre Daten beschädigen können.

Alle löschen

Bei Klick auf diese Schaltfläche werden alle gefundenen Objekte von Ihrem Computer gelöscht.

Alle ignorieren

Mit dieser Schaltfläche werden alle gefundenen Objekte aus der Liste der gefundenen Objekte im Abschnitt **Andere Objekte** gelöscht.

•••

Mit dieser Schaltfläche wird ein Pop-up-Menü geöffnet, in dem Sie eine der folgenden Aktionen für ein gefundenes Objekt auswählen können:

- **Löschen**. Gefundenes Objekt von Ihrem Computer löschen.
- **Ignorieren**. Objekt aus der Liste der gefundenen Objekte löschen.

Der Abschnitt **Backup** enthält Backup-Kopien von gefundenen Objekten.

Alle löschen

Bei Klick auf diese Schaltfläche werden alle Backup-Kopien der gefundenen Objekte von Ihrem Computer gelöscht.

•••

Mit dieser Schaltfläche wird ein Pop-up-Menü geöffnet, in dem Sie eine der folgenden Aktionen für ein Backup-Objekt auswählen können:

- **Gesicherte Kopie löschen**. Backup-Kopie des gefundenen Objekts von Ihrem Computer löschen.
- **Datei wiederherstellen**. Backup-Kopie der in der Liste ausgewählten Datei am ursprünglichen Speicherort unter jenem Namen wiederherstellen, den die Quelldatei vor der Desinfektion oder dem Löschen trug. Wenn sich am ursprünglichen Speicherort bereits ein Objekt mit dem gleichen Namen befindet (dies kann vorkommen, wenn Kaspersky Endpoint Security eine Kopie der Originaldatei erstellt hat, bevor die Originaldatei desinfiziert oder gelöscht wurde), wird eine Warnung angezeigt. Sie können entweder den Speicherort für das wiederherzustellende Objekt ändern oder das Objekt umbenennen.

Das Fenster Lizenz



Bei Klick auf diese Schaltfläche kehrt Kaspersky Endpoint Security zum vorherigen Fenster zurück.



Bei Klick auf diese Schaltfläche wechselt Kaspersky Endpoint Security zum nächsten Fenster.

Hinweis: Das Aussehen dieses Fenster ist davon abhängig, ob Kaspersky Endpoint Security aktiviert ist und welcher Lizenz- oder Abonnementtyp verwendet wird.

Das Fenster kann die folgenden Informationen enthalten:

- Status der Lizenz oder des Abonnements
- Aktive Schlüssel
- Reserveschlüssel (falls vorhanden)
- Lizenztyp und Anzahl der Computer, auf denen Sie die App im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verwenden können
- App-Funktionen, die im Rahmen der aktuellen Lizenz oder des aktuellen Abonnements verfügbar sind
- Zeitpunkt (Datum und Uhrzeit), zu dem die Lizenz abläuft
- Anzahl der Tage bis zum Ablauf der Lizenz

In diesem Fenster können Sie die folgenden Aktionen ausführen:

- Anwendung durch die Eingabe eines Aktivierungscodes aktivieren
- Zu einer Website wechseln, die darüber informiert, wie Sie im Kaspersky-Online-Shop eine Lizenz kaufen können
- Website des Händlers von Kaspersky Endpoint Security mit Informationen zur Verlängerung des Abonnements öffnen
- Status Ihres Abonnements aktualisieren

Um weitere Informationen über die Lizenzverwaltung von Kaspersky Endpoint Security zu erhalten, wenden Sie sich an den Systemadministrator Ihres Unternehmens.

Registerkarte „Basis“

Im Abschnitt **Allgemein** können Sie den Computerschutz vor Malware und anderen Sicherheitsbedrohungen aktivieren oder deaktivieren.

Schutz aktivieren

Mit diesem Kontrollkästchen wird der Echtzeitschutz vor Malware und anderen Sicherheitsbedrohungen aktiviert bzw. deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Sichere Verbindungen (HTTPS) untersuchen

Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von verschlüsselten Verbindungen (HTTPS) durch Kaspersky Endpoint Security, sowie die Anzeige von Benachrichtigungen, wenn die Web-Kontrolle den Zugriff des Benutzers auf gefährliche Webressourcen blockiert.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Vertrauenswürdige Zone

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet, in dem Sie die „Vertrauenswürdige Zone“ anpassen können, indem Sie eine Liste mit Objekten erstellen, denen Sie vertrauen und die nicht auf Schadsoftware untersucht werden sollen.

Einstellungen

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet, in dem Sie die Liste der vertrauenswürdigen Stammzertifikate verwalten können und den Zertifikatspeicher für die Untersuchung des verschlüsselten HTTPS-Datenverkehrs im Mozilla Firefox-Browser auswählen.

Im Abschnitt **Schutz vor bedrohlichen Dateien** können Sie den „Schutz vor bedrohlichen Dateien“ aktivieren oder deaktivieren. Außerdem können Sie hier festlegen, welche Aktion Kaspersky Endpoint Security beim Fund einer infizierten Datei ausführen soll.

Schutz vor bedrohlichen Dateien aktivieren

Mit diesem Kontrollkästchen wird der „Schutz vor bedrohlichen Dateien“ aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schutzbereich

Diese Schaltfläche öffnet ein Fenster, in dem Sie den Schutzbereich erstellen können.

Schädliche Objekte automatisch desinfizieren oder löschen

Kaspersky Endpoint Security blockiert den Zugriff auf die infizierte Datei und versucht, sie zu desinfizieren, ohne nach Bestätigung zu fragen. Vor der Desinfektion speichert Kaspersky Endpoint Security eine Backup-Kopie der Datei im Backup. Wenn die Datei desinfiziert werden konnte, wird sie am ursprünglichen Ort unter dem ursprünglichen Namen gespeichert. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei blockiert und verbleibt am ursprünglichen Ort. Informationen über den Fund des infizierten Objekts werden im Bericht Verarbeitete Objekte protokolliert.

Aktion erfragen

Kaspersky Endpoint Security zeigt ein Benachrichtigungsfenster an. Das Fenster informiert darüber, von welchem schädlichen Objekt die Datei vermutlich infiziert ist, und bietet entsprechende Aktionen zur Auswahl an. Diese Aktionen können je nach Status des Objekts variieren.

Diese Aktion ist standardmäßig ausgewählt.

Im Abschnitt **Schutz vor Web-Bedrohungen** können Sie den „Schutz vor Web-Bedrohungen“ aktivieren oder deaktivieren. Außerdem können Sie hier festlegen, welche Aktion Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr gefährliche Objekte gefunden werden.

Schutz vor Web-Bedrohungen aktivieren

Mit diesem Kontrollkästchen wird der „Schutz vor Web-Bedrohungen“ aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Gefährliche Objekte im Web-Datenverkehr automatisch blockieren

Kaspersky Endpoint Security blockiert den Zugriff auf die Website, auf der ein gefährliches Objekt im Web-Datenverkehr gefunden wurde. Der Benutzer wird nicht nach Bestätigung gefragt.

Aktion erfragen

Kaspersky Endpoint Security zeigt ein Warnfenster an, das über das gefundene gefährliche Objekt im Web-Datenverkehr informiert, und fordert Sie auf, eine Aktion auszuwählen. Diese Aktionen können je nach Status des Objekts variieren.

Diese Aktion ist standardmäßig ausgewählt.

Im Abschnitt **Schutz vor E-Mail-Bedrohungen** können Sie den Schutz vor E-Mail-Bedrohungen aktivieren oder deaktivieren. Außerdem können Sie hier festlegen, welche Aktion Kaspersky Endpoint Security beim Fund eines schädlichen Objekts ausführen soll.

Schutz vor E-Mail-Bedrohungen aktivieren

Mit diesem Kontrollkästchen wird der Schutz vor E-Mail-Bedrohungen aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schädliche Objekte automatisch löschen

Wenn Kaspersky Endpoint Security ein infiziertes Objekt in einer E-Mail-Nachricht findet, löscht es das infizierte Objekt und ersetzt den Inhalt des Objekts durch den Text „The requested file infected with <Virusname> has been deleted“.

Schädliche Objekte automatisch blockieren

Wenn Kaspersky Endpoint Security ein infiziertes Objekt in einer E-Mail-Nachricht findet, ersetzt es den Betreff der E-Mail-Nachricht durch „Message is infected: <ursprünglicher Betreff>“ (<ursprünglicher Betreff> steht für den Betreff der ursprünglichen Nachricht). Der Betreff einer E-Mail-Nachricht wird nur im POP3-Protokoll ersetzt.

Im Abschnitt **Schutz vor Netzwerk- bedrohungen** können Sie den „Schutz gegen Netzwerkangriffe“ aktivieren oder deaktivieren.

Schutz vor Netzwerkbedrohungen aktivieren

Mit diesem Kontrollkästchen wird der „Schutz vor Netzwerkbedrohungen“ aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Einstellungen

Wenn Sie auf diese Schaltfläche klicken, wird ein Fenster geöffnet, in dem Sie eine Liste mit vertrauenswürdigen Computern anlegen oder die Liste der blockierten Computer anzeigen und bearbeiten können.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Fenster „Schutzbereich“

Im Abschnitt **Schutzbereich** können Sie den Schutzbereich anzeigen und bearbeiten.

Alle Wechseldatenträger

Mit diesem Kontrollkästchen wird der Echtzeitschutz für alle Wechseldatenträger aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Alle internen Datenträger

Mit diesem Kontrollkästchen wird der Echtzeitschutz für alle internen Datenträger aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Alle Netzlaufwerke

Mit diesem Kontrollkästchen wird der Echtzeitschutz für alle Netzlaufwerke aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

+

Diese Schaltfläche öffnet ein Fenster, in dem Sie Elemente für den Schutzbereich auswählen können:

- **Dateien und Ordner**. Bei Auswahl dieses Elements wird ein Dialog geöffnet, in dem eine Datei oder ein Ordner zum Schutzbereich hinzugefügt werden kann.
- **Alle Datenträger**. Bei Auswahl dieses Elements werden alle Wechseldatenträger, internen Laufwerke und Netzlaufwerke des Computers zum Schutzbereich hinzugefügt.
- **Alle Wechseldatenträger**. Bei Auswahl dieses Elements werden alle Wechseldatenträger des Computers zum Schutzbereich hinzugefügt.
- **Alle internen Datenträger**. Bei Auswahl dieses Elements werden alle internen Datenträger des Computers zum Schutzbereich hinzugefügt.
- **Alle Netzlaufwerke**. Bei Auswahl dieses Elements werden alle Netzlaufwerke des Computers zum Schutzbereich hinzugefügt.
- **Arbeitsspeicher**. Bei Auswahl dieses Elements wird der Arbeitsspeicher des Computers zum Schutzbereich hinzugefügt.
- **Autostart-Objekte**. Bei Auswahl dieses Elements werden alle ausführbaren Dateien, die beim Hochfahren des Betriebssystems gestartet werden, zum Schutzbereich hinzugefügt. Durch die Untersuchung der Autostart-Objekte können Rootkits erkannt werden.

Das Kontrollkästchen neben einem Listenelement aktiviert/deaktiviert den Echtzeitschutz für die Objekte, die zu diesem Element gehören.

–

Mit dieser Schaltfläche wird das ausgewählte Element aus der Liste für den Schutzbereich gelöscht.

Elemente, die standardmäßig auf der Liste für den Schutzbereich stehen, können nicht gelöscht werden.

Im Abschnitt **Optimierung** können Sie festlegen, ob Kaspersky Endpoint Security das schreibgeschützte Systemvolume untersuchen soll.

Schreibgeschütztes Systemvolume bei der Untersuchung überspringen

Dieses Kontrollkästchen deaktiviert/aktiviert in Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

Das Fenster „Einstellungen“

Auf der Registerkarte **Vertrauenswürdige Computer** können Sie eine Liste für vertrauenswürdige Computer erstellen. Die IP-Adressen dieser Computer werden vom Programm Kaspersky Endpoint Security auch dann nicht automatisch blockiert, wenn eine gefährliche Netzwerkaktivität dieses Computers erkannt wurde.

Die Liste für vertrauenswürdige Computer ist standardmäßig leer.

+

Mit dieser Schaltfläche wird ein Eingabefeld für die IP-Adresse eines vertrauenswürdigen Computers hinzugefügt.

–

Mit dieser Schaltfläche wird die ausgewählte IP-Adresse aus der Liste für vertrauenswürdige Computer gelöscht.

Bearbeiten

Nach Klick auf diese Schaltfläche kann die ausgewählte IP-Adresse geändert werden.

Auf der Registerkarte **Blockierte Computer** können Sie die Liste der blockierten Computer anzeigen und ändern.

Das Programm Kaspersky Endpoint Security blockiert den Computer mit dieser IP-Adresse für eine Stunde, nachdem eine gefährliche Netzwerkaktivität dieses Computers erkannt wurde.

IP-Adresse

Diese Spalte nennt die IP-Adresse des blockierten Computers.

Ereigniszeitpunkt

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit), zu welchem die gefährliche Netzwerkaktivität auf dem Computer erkannt wurde.

Freigeben

Mit dieser Schaltfläche wird die ausgewählte IP-Adresse aus der Liste der blockierten Computer gelöscht.

Die Registerkarte „Untersuchung“

Liste der Untersuchungsaufgaben

Diese Liste enthält die vordefinierten Untersuchungsaufgaben:

- **Vollständige Untersuchung**. Arbeitsspeicher des Computers, Autostart-Objekte und alle internen Datenträger auf Malware untersuchen.
- **Schnelle Untersuchung**. Schadsoftware-Untersuchung, die nur wichtige Computerbereiche umfasst: Arbeitsspeicher, Autostart-Objekte und Systemordner.
- **Benutzerdefinierte Untersuchung**. Schadsoftware-Untersuchung eines bestimmten Objekts (Datei, Ordner, interner Datenträger oder Wechseldatenträger).
- **Untersuchung externer Datenträger**. Eine Malware-Untersuchung für externe Datenträger, die gestartet wird, sobald ein externer Datenträger mit dem Computer verbunden wird.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Im Abschnitt **Bereich** können Sie den Untersuchungsbereich für die Aufgabe „Schnelle Untersuchung“ anzeigen und anpassen.

Bearbeiten

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Untersuchungsbereich anzeigen oder ändern können.

Diese Schaltfläche wird nur angezeigt, wenn in der Liste die Aufgabe Schnelle Untersuchung ausgewählt ist.

Im Abschnitt **Aktion** können Sie auswählen, welche Aktion Kaspersky Endpoint Security beim Fund einer infizierten Datei ausführen soll, und Sie können einen Aufgabenzeitplan erstellen.

Schädliche Objekte automatisch desinfizieren oder löschen

Kaspersky Endpoint Security blockiert den Zugriff auf die infizierte Datei und versucht, sie zu desinfizieren, ohne nach Bestätigung zu fragen. Vor der Desinfektion speichert Kaspersky Endpoint Security eine Backup-Kopie der Datei im Backup. Wenn die Datei desinfiziert werden konnte, wird sie am ursprünglichen Ort unter dem ursprünglichen Namen gespeichert. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei blockiert und verbleibt am ursprünglichen Ort. Informationen über den Fund des infizierten Objekts werden im Bericht Verarbeitete Objekte protokolliert.

Nach Abschluss der Untersuchung erfragen

Kaspersky Endpoint Security schiebt die Verarbeitung von gefundenen infizierten Dateien bis zum Ende der Untersuchung auf. Nach Abschluss der Untersuchung zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster mit Informationen zu jedem gefundenen infizierten Objekt an und bietet Aktionen zur Auswahl an. Diese Aktionen können je nach Status des Objekts variieren.

Diese Aktion ist standardmäßig ausgewählt.

Im Abschnitt **Wenn ein externer Datenträger angeschlossen wird** der Registerkarte **Untersuchung externer Datenträger** können Sie die Aktion auswählen, die Kaspersky Endpoint Security ausführen soll, wenn ein externer Datenträger verbunden wird.

Untersuchung

Wenn diese Option ausgewählt ist, startet Kaspersky Endpoint Security für den angeschlossenen externen Datenträger eine Aufgabe zur Untersuchung auf Malware.

Diese Variante ist standardmäßig ausgewählt.

Nichts tun

Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security den angeschlossenen externen Datenträger nicht.

Im Abschnitt **Optimierung** können Sie festlegen, ob Kaspersky Endpoint Security das schreibgeschützte Systemvolume untersuchen soll, wenn die Aufgabe „Schnelle Untersuchung“ oder „Vollständige Untersuchung“ ausgeführt wird.

Schreibgeschütztes Systemvolume bei der Untersuchung überspringen

Dieses Kontrollkästchen deaktiviert/aktiviert in Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume.

Dieses Kontrollkästchen ist für die Aufgabe „Schnelle Untersuchung“ standardmäßig aktiviert und für die Aufgabe „Vollständige Untersuchung“ standardmäßig deaktiviert.

Wichtig: Es kann sein, dass die Optimierung aus Sicherheitsgründen deaktiviert ist.

CPU-Auslastung

Wenn Sie auf diese Schaltfläche klicken, wird ein Dialog geöffnet. Dort können Sie festlegen, ob für Untersuchungsaufgaben die CPU-Nutzung des geschützten Geräts durch die Anwendung beschränkt werden soll oder nicht. Wenn die Option **Maximale CPU-Last für Untersuchungen** ausgewählt ist, können Sie im entsprechenden Feld die maximal zulässige CPU-Auslastung angeben.

Hinweis: Dies ist ein kumulativer Grenzwert über alle CPU-Kerne. Die im Aktivitätsmonitor angezeigte CPU-Auslastung ist die Summe der Auslastung jedes CPU-Kerns und kann daher 100 Prozent überschreiten.

Die Aktivierung dieser Option kann sich negativ auf die Leistung von Kaspersky Endpoint Security auswirken.

Diese Option ist standardmäßig deaktiviert.

Zeitplan

Mit dieser Schaltfläche wird ein Dialog geöffnet, in dem Sie einen Zeitplan für die Vollständige Untersuchung und für die Schnelle Untersuchung festlegen können.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Fenster „Untersuchungsbereich“

In diesem Fenster können Sie den Untersuchungsbereich für die Aufgabe Schnelle Untersuchung anzeigen und ändern.

Das Kontrollkästchen, das sich in der Liste neben einem Objekt befindet, aktiviert/deaktiviert die Untersuchung für das entsprechende Objekt.

+

Mit dieser Schaltfläche wird eine Liste geöffnet, in welcher der Untersuchungsbereich angepasst werden kann:

- **Dateien und Ordner**. Bei Auswahl dieses Elements wird ein Dialog geöffnet, in dem eine Datei oder ein Ordner zum Untersuchungsbereich hinzugefügt werden kann.
- **Alle Datenträger**. Bei Auswahl dieses Elements werden alle Wechseldatenträger, internen Laufwerke und Netzlaufwerke des Computers zum Untersuchungsbereich hinzugefügt.
- **Alle externen Datenträger**. Bei Auswahl dieses Elements werden alle Wechseldatenträger des Computers zum Untersuchungsbereich hinzugefügt.
- **Alle internen Datenträger**. Bei Auswahl dieses Elements werden alle internen Datenträger des Computers zum Untersuchungsbereich hinzugefügt.
- **Alle Netzlaufwerke**. Bei Auswahl dieses Elements werden alle Netzlaufwerke des Computers zum Untersuchungsbereich hinzugefügt.
- **Arbeitsspeicher**. Bei Auswahl dieses Elements wird der Arbeitsspeicher des Computers zum Untersuchungsbereich hinzugefügt.
- **Autostart-Objekte**. Bei Auswahl dieses Elements werden alle ausführbaren Dateien, die beim Hochfahren des Betriebssystems gestartet werden, zum Untersuchungsbereich hinzugefügt. Durch die Untersuchung der Autostart-Objekte können Rootkits erkannt werden.

–

Mit dieser Schaltfläche wird das ausgewählte Element aus der Liste für den Untersuchungsbereich gelöscht.

Elemente, die standardmäßig auf der Liste für den Untersuchungsbereich stehen, können nicht gelöscht werden.

Im Abschnitt **Optimierung** können Sie festlegen, ob Kaspersky Endpoint Security das schreibgeschützte Systemvolume untersucht, wenn eine Untersuchungsaufgabe ausgeführt wird.

Schreibgeschütztes Systemvolume bei der Untersuchung überspringen

Dieses Kontrollkästchen deaktiviert/aktiviert in Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Endpoint Security die Untersuchung des schreibgeschützten Systemvolume. Dadurch wird die Untersuchungsdauer erheblich verkürzt.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security das schreibgeschützte Systemvolume.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Hinweis: Kaspersky Endpoint Security untersucht keine Dateien, die sich in OneDrive, in der iCloud oder in anderen Cloud-Speichern befinden. Bitte schließen Sie diese Dateien aus dem Untersuchungsbereich aus. Andernfalls werden Untersuchungsaufgaben möglicherweise mit dem Fehler *Infizierte Datei wurde nicht gelöscht* abgeschlossen.

Registerkarte „Bedrohungen“

Im Abschnitt **Zu erkennende Objekte** können Sie die Liste der zu erkennenden Objekte anpassen.

Viren, Würmer, Trojaner, schädliche Tools, Adware und Dialer

Diese Kategorie umfasst folgende Programmtypen:

- Alle Typen von Schadsoftware
- Anwendungen, die auf Ihrem Computer Werbung (z. B. Banner) anzeigen oder die Suchergebnisse in Ihrem Browser durch Websites mit Werbung ersetzen
- Anwendungen, die heimlich Telefonverbindungen über ein Computermodem herstellen

Programme aus dieser Kategorie wird immer von Kaspersky Endpoint Security überwacht.

Das Kontrollkästchen ist immer aktiviert und kann nicht deaktiviert werden.

Legale Software, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können

Mit diesem Kontrollkästchen wird die Überwachung legaler Anwendungen aktiviert/deaktiviert, mit denen Angreifer den Computer oder die Benutzerdaten beschädigen können. Dazu zählen beispielsweise Tools zur Fernverwaltung.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Im Abschnitt **Backup** können Sie die maximale Speicherdauer für Objekte im Backup festlegen.

Gesicherte Objekte löschen nach <Anzahl> Tagen

Dieses Kontrollkästchen aktiviert/deaktiviert das Löschen von Objekten aus dem Backup nach Ablauf der festgelegten Speicherdauer.

Wenn das Kontrollkästchen aktiviert ist, werden Objekte aus dem Backup gelöscht, wenn der im Zahlenfeld neben dem Kontrollkästchen festgelegte Zeitraum abläuft. Wenn das Kontrollkästchen deaktiviert ist, werden Objekte unbefristet im Backup aufbewahrt.

Standardmäßig ist dieses Kontrollkästchen aktiviert und Objekte werden für 30 Tage im Backup aufbewahrt.

Im Abschnitt **Ausnahmen** können Sie eine Liste der Dateien, Ordner, Websites und Programme anlegen, denen Sie vertrauen und die nicht auf Malware untersucht werden sollen.

Vertrauenswürdige Zone

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Vertrauenswürdige Zone ändern können.

Hinweis: Wenn ein Administrator die Richtlinie so konfiguriert, dass die Bearbeitung der „Vertrauenswürdigen Zone“ verboten ist, können die Benutzer nicht auf Einstellungen der „Vertrauenswürdigen Zone“ zugreifen.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Das Fenster „Administratorkennwort einrichten“

Kennwort

Feld zur Eingabe eines Kennworts, um unerwünschte Aktionen auf dem Gerät einzuschränken.

Kennwort bestätigen

Feld, in dem das Kennwort durch erneute Eingabe bestätigt wird.

Optionen

Liste der Aktionen, die durch das Kennwort geschützt werden können. Aktivieren Sie die erforderlichen Kontrollkästchen, um die entsprechenden Aktionen auf dem Gerät zu schützen. Sie müssen mindestens ein Kontrollkästchen aktivieren.

Abbrechen

Bei Klick auf diese Schaltfläche wird das Fenster geschlossen, ohne die Änderungen zu speichern.

OK

Dieser Schaltfläche speichert die Einstellungen des Administratorkennworts und schließt das Fenster. Nach dem Speichern der Änderungen werden Sie zur Eingabe des Kennworts aufgefordert, wenn Sie versuchen, eine unerwünschte Aktion auf dem Gerät auszuführen.

Das Fenster „Einstellungen des Kennwortschutzes“

Kennwort

Feld zur Eingabe eines Kennworts, um unerwünschte Aktionen auf den Benutzergeräten einzuschränken.

Klicken Sie auf Anzeigen, um die eingegebenen Zeichen anzuzeigen.

Kennwort bestätigen

Feld, in dem das Kennwort durch erneute Eingabe bestätigt wird.

Klicken Sie auf Anzeigen, um die eingegebenen Zeichen anzuzeigen.

Kennwort erforderlich für

Liste der Aktionen, die durch das Kennwort geschützt werden können. Aktivieren Sie die erforderlichen Kontrollkästchen, um die entsprechenden Aktionen auf dem Benutzergerät zu schützen.

Registerkarte „Vertrauenswürdige Anwendungen“

Auf der Registerkarte **Vertrauenswürdige Anwendungen** können Sie eine Liste mit Anwendungen erstellen, die nicht von der Anwendung Kaspersky Endpoint Security überwacht werden sollen.

Die Objektliste für die vertrauenswürdige Zone ist standardmäßig leer.

+

Wenn Sie auf diese Schaltfläche klicken, öffnet sich ein Fenster, in dem Sie den Pfad zu einer Anwendung angeben, die erforderliche Code-Signatur festlegen und die Arten der Aktivitäten auswählen können, die Kaspersky Endpoint Security nicht überwacht soll.

–

Bei Klick auf diese Schaltfläche wird das ausgewählte Programm aus der vertrauenswürdigen Zone entfernt.

Bearbeiten

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Einstellungen der vertrauenswürdigen Anwendung ändern können.

Fenster „Vertrauenswürdige Anwendung hinzufügen“

Pfad

Pfad einer Anwendung, deren Aktivität nicht von Kaspersky Endpoint Security überwacht werden soll.

Hinweis: Für Pfadangaben in diesem Feld können keine symbolischen Links verwendet werden.

Auswählen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie eine Anwendung auswählen können, deren Aktivität nicht von Kaspersky Endpoint Security überwacht werden soll. In diesem Fall werden die Werte der Felder **Pfad** und **Anforderung an die Codesignatur** automatisch eingefügt.

Anforderung an die Codesignatur

Anforderungen an die Codesignatur des Programms, dessen Aktivität nicht von Kaspersky Endpoint Security überwacht wird.

Dieser Parameter ist optional.

Wählen Sie im Abschnitt **Optionen** den Aktivitätstyp aus, den Kaspersky Endpoint Security nicht überwachen soll.

Dateiaktivität nicht überwachen

Dieses Kontrollkästchen aktiviert/deaktiviert die Überwachung der Vorgänge einer Anwendung mit Dateien auf einem Client-Computer.

Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security die Dateiaktivität der Anwendung nicht.

Wenn dieses Kontrollkästchen deaktiviert ist, überwacht Kaspersky Endpoint Security die Dateiaktivität der Anwendung.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Netzwerkaktivität nicht überwachen

Dieses Kontrollkästchen aktiviert/deaktiviert die Überwachung des ein- und ausgehenden Internet-Datenverkehrs der Anwendung einem Client-Computer.

Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security die Netzwerkaktivität der Anwendung nicht.

Wenn dieses Kontrollkästchen deaktiviert ist, überwacht Kaspersky Endpoint Security die Netzwerkaktivität der Anwendung.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Abbrechen

Bei Klick auf diese Schaltfläche wird das Fenster geschlossen, ohne die Änderungen zu speichern.

OK

Diese Schaltfläche speichert die Parameter der vertrauenswürdigen Anwendung schließt das Fenster.

Registerkarte „Vertrauenswürdige Dateien und Ordner“

Auf der Registerkarte **Dateien und Ordner** können Sie eine Liste mit Dateien und Ordnern erstellen, die Kaspersky Endpoint Security nicht überwachen soll.

Die Liste der Objekte für die „Vertrauenswürdige Zone“ ist standardmäßig leer.

+

Wenn Sie auf diese Schaltfläche klicken, wird ein Dialog zur Auswahl einer Datei oder eines Ordners geöffnet.

–

Mit dieser Schaltfläche wird das ausgewählte Objekt aus der „Vertrauenswürdigen Zone“ gelöscht.

Die Registerkarte Vertrauenswürdige Webadressen

Auf der Registerkarte **Webadressen** können Sie eine Liste mit Webadressen erstellen, die Kaspersky Endpoint Security nicht überwachen soll.

Die Liste der Objekte für die „Vertrauenswürdige Zone“ ist standardmäßig leer.

+

Wenn Sie auf diese Schaltfläche klicken, wird ein Feld zur Eingabe einer Webadresse hinzugefügt.

Zur Angabe der Website-Adresse können Sie die folgenden Zeichen verwenden:

- Das Sternchen (`*`) steht für eine beliebige Zeichenfolge, unter Ausnahme der Zeichen `\` und `/`.
- Zwei aufeinanderfolgende Sternchen (`**`) stehen für eine beliebige Zeichenfolge (einschließlich einer leeren Zeichenfolge), einschließlich der Zeichen `\` und `/`.
- Das Fragezeichen (`?`) steht für ein beliebiges einzelnes Zeichen im Datei- oder Ordnernamen, unter Ausnahme der Zeichen `\` und `/`.

–

Mit dieser Schaltfläche wird die ausgewählte Webadresse aus der „Vertrauenswürdigen Zone“ gelöscht.

Registerkarte „Erweitert“

Im Abschnitt **KSN** können Sie die Bedingungen der Erklärung zu Kaspersky Security Network lesen und die Teilnahme an Kaspersky Security Network aktivieren oder deaktivieren.

KSN-Erklärung anzeigen

Mit dieser Schaltfläche wird ein Fenster mit dem Text der Erklärung zu Kaspersky Security Network geöffnet.

Kaspersky Endpoint Security kann die Infrastruktur Global KSN oder Private KSN verwenden. Wenn Sie an Kaspersky Security Network teilnehmen, verwendet Kaspersky Endpoint Security Informationen über die Reputation von Dateien, Webressourcen und Anwendungen, die von Kaspersky Security Network stammen, und stellt an Kaspersky Security Network Daten bereit, die für das Funktionieren der Erkennungsdienste notwendig sind.

An Kaspersky Security Network teilnehmen

Mit diesem Kontrollkästchen wird die Teilnahme an Kaspersky Security Network aktiviert/deaktiviert.

An Kaspersky Private Security Network teilnehmen

Dieses Kontrollkästchen aktiviert/deaktiviert die Teilnahme an Kaspersky Private Security Network. Weitere Informationen über die Teilnahme an Kaspersky Private Security Network erhalten Sie vom Systemadministrator Ihres Unternehmens.

Erweiterten KSN-Modus aktivieren

Dieses Kontrollkästchen aktiviert/deaktiviert die Bereitstellung zusätzlicher Daten an Kaspersky Security Network. Dabei geht es um Daten, die erforderlich sind, um den Schutz Ihres Computers und die Benutzerfreundlichkeit von Kaspersky Endpoint Security zu verbessern. Die Liste der Daten finden Sie in der Erklärung zu Kaspersky Security Network und in der Hilfe zu Kaspersky Endpoint Security.

Dieses Kontrollkästchen ist automatisch aktiviert, wenn das Kontrollkästchen **An Kaspersky Security Network teilnehmen** aktiviert ist.

Cloud-Modus aktivieren

Der Cloud-Modus bezieht sich auf den App-Betriebsmodus, in dem Kaspersky Endpoint Security eine eingeschränkte Version der Anti-Malware-Datenbanken verwendet. Dieser Modus ist nur verfügbar, wenn die Teilnahme an Kaspersky Security Network aktiviert ist. Wenn Sie die eingeschränkte Version der Anti-Malware-Datenbanken verwenden, wird der Arbeitsspeicher im Vergleich zur Nutzung der vollständigen Datenbanken nur etwa halb so stark belastet. Wenn Sie nicht an Kaspersky Security Network teilnehmen oder der Cloud-Modus deaktiviert ist, lädt Kaspersky Endpoint Security die vollständige Version der Anti-Malware-Datenbanken von den Kaspersky-Servern herunter.

Ist der Schalter aktiviert, verwendet Kaspersky Endpoint Security die eingeschränkte Version der Anti-Malware-Datenbanken. Dadurch werden die Ressourcen des Betriebssystems geschont.

Hinweis: Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die eingeschränkte Version der Anti-Malware-Datenbanken herunter.

Ist der Schalter deaktiviert, verwendet Kaspersky Endpoint Security die vollständige Version der Anti-Malware-Datenbanken.

Hinweis: Nachdem das Kontrollkästchen deaktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Anti-Malware-Datenbanken herunter.

Im Abschnitt **Verhaltensanalyse** können Sie die Komponente Verhaltensanalyse aktivieren bzw. deaktivieren und eine Aktion auswählen, die beim Erkennen von Malware-Aktivität ausgeführt werden soll.

Verhaltensanalyse aktivieren

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Komponente Verhaltensanalyse. Diese Komponente empfängt Informationen über die Aktionen von auf Ihrem Computer installierten Programmen und stellt diese Informationen anderen Schutzkomponenten zur Verfügung, um deren Leistung zu verbessern.

Malware-Aktivitäten blockieren

Wenn diese Option ausgewählt ist, beendet Kaspersky Endpoint Security ein Programm, sobald eine bösartige Aktivität erkannt wird.

Erkanntes gefährliches Objekt löschen

Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security die ausführbare Datei eines schädlichen Programms und legt im Backup eine Backup-Kopie der Datei an, wenn eine schädliche Aktivität erkannt wird.

Aktion erfragen

Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security eine schädliche Aktivität erkennt, zeigt Kaspersky Endpoint Security ein Benachrichtigungsfenster mit Informationen über das schädliche Objekt an und fragt den Benutzer, welche Aktion ausgeführt werden soll. Die verfügbaren Aktionen können je nach Objektstatus variieren.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Registerkarte „Update“

Im Abschnitt **Datenbanken** können Sie den Update-Modus für die Datenbanken von Kaspersky Endpoint Security anpassen.

Updates automatisch herunterladen

Mit diesem Kontrollkästchen wird das automatische Update für die Anwendungsdatenbanken aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **Proxy** können Sie festlegen, dass beim Update von Kaspersky Endpoint Security ein Proxyserver verwendet werden soll.

Proxyserver verwenden

Mit diesem Kontrollkästchen wird für das Update der Anti-Malware-Datenbanken und Anwendungsmodule die Verwendung eines Proxyservers für die Internetverbindung aktiviert bzw. deaktiviert.

Das Kontrollkästchen ist standardmäßig aktiviert.

Einstellungen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Verbindungseinstellungen für den Proxyserver anpassen können.

Im Abschnitt **Rollback** können Sie zur Verwendung der vorherigen Version der Anwendungsdatenbanken zurückkehren. Sie müssen eventuell ein Update zurücksetzen, wenn die neue Version der Anwendungsdatenbanken einen ungültigen Eintrag enthält, der dazu führt, dass Kaspersky Endpoint Security eine sichere Anwendung blockiert.

Update zurücksetzen

Bei Klick auf diese Schaltfläche wird ein Rollback der Anwendungsdatenbanken durchgeführt.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Fenster „Proxy-Server-Einstellungen“

Proxy-Einstellungen des Systems verwenden

Kaspersky Endpoint Security verwendet die Proxy-Server-Einstellungen, die in den Systemeinstellungen des Mac festgelegt sind.

Diese Aktion ist standardmäßig ausgewählt.

Folgende Proxy-Einstellungen verwenden

Kaspersky Endpoint Security verwendet die Proxy-Server-Einstellungen, die in diesem Fenster angegeben sind.

Adresse

Eingabefeld für die IP-Adresse oder den Domänennamen des Proxy-Servers.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Port

Eingabefeld für die Nummer des Proxy-Server-Ports, der für Updates von Kaspersky Endpoint Security verwendet werden soll.

Dieses Feld ist verfügbar, wenn die Option **Folgende Proxy-Einstellungen verwenden** ausgewählt ist.

Der Standardwert ist 8080.

Authentifizierung verwenden

Bei der *Authentifizierung* werden Benutzername und Kennwort für die Verbindung mit dem Proxy-Server überprüft.

Dieses Kontrollkästchen aktiviert/deaktiviert die Authentifizierung bei der Verbindung mit dem Proxy-Server.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Benutzername

Eingabefeld für den Benutzernamen zur Authentifizierung bei der Verbindung mit dem Proxy-Server

Dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung verwenden** aktiviert ist.

Kennwort

Eingabefeld für das Kennwort zur Authentifizierung bei der Verbindung mit dem Proxy-Server

Dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung verwenden** aktiviert ist.

Wenn Sie den Benutzernamen und das Kennwort nicht angegeben haben oder der Proxy-Server die angegebenen Anmeldedaten nicht akzeptiert hat, öffnet sich ein Fenster, in dem Benutzername und Kennwort für die Authentifizierung auf dem Proxy-Server angegeben werden müssen. Wenn die Authentifizierung erfolgreich war und im Abfragefenster das Kontrollkästchen **Kennwort merken** aktiviert ist, werden in Zukunft der eingegebene Benutzername und das Kennwort verwendet. Wenn das Kontrollkästchen **Kennwort merken** im Eingabefenster für die Anmeldedaten deaktiviert ist, werden Benutzername und Kennwort bei der nächsten Verbindung mit dem Proxy-Server erneut abgefragt.

Für lokale Adressen keinen Proxyserver verwenden

Dieses Kontrollkästchen aktiviert/deaktiviert die Verwendung eines Proxy-Servers bei einem Update aus einem lokalen Ordner oder einem Netzwerkordner.

Das Kontrollkästchen ist standardmäßig aktiviert.

Registerkarte „Benutzeroberfläche“

Im Abschnitt **Benachrichtigungen** können Sie die Benachrichtigungen anpassen, die Kaspersky Endpoint Security anzeigt, um Sie über unterschiedliche Ereignisse zu informieren.

Benachrichtigungen aktivieren

Mit diesem Kontrollkästchen werden Benachrichtigungen über die Ereignisse in der Anwendung aktiviert/deaktiviert.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Alarmton beim Fund von Malware abspielen

Dieses Kontrollkästchen aktiviert/deaktiviert Tonsignale, die ertönen, wenn Kaspersky Endpoint Security ein schädliches Objekt findet.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Abschnitt **App-Symbol** können Sie anpassen, wie das Anwendungssymbol in der Menüleiste angezeigt werden soll.

In Menüleiste anzeigen

Dieses Kontrollkästchen aktiviert/deaktiviert die Anzeige des Anwendungssymbols in der Menüleiste.

Im Abschnitt **Berichte** können Sie die Aufzeichnung von nicht-kritischen Ereignissen in den Berichten von Kaspersky Endpoint Security aktivieren/deaktivieren.

Nicht-kritische Ereignisse protokollieren

Mit diesem Kontrollkästchen wird die Protokollierung von informativen Ereignissen in Berichten aktiviert/deaktiviert. Solche Ereignisse sind für die Sicherheit des Computers in der Regel zweitrangig.

Im Abschnitt **Protokollierung** können Sie die Protokollierung aktivieren oder deaktivieren.

Mit der Protokollierung können ausführliche Informationen über die Anwendungsaktivitäten aufgezeichnet werden. Die Kaspersky-Support-Experten verwenden die Ablaufverfolgungsdateien, um aufgetretene Probleme zu lösen. Sie können die Protokollierung von Anwendungsereignissen aktivieren, um Protokolldateien zu erstellen und diese auf Anfrage an den Technischen Support zu senden. Die Protokollierung von Anwendungsereignissen ist standardmäßig deaktiviert.

Wichtig: Aktivieren Sie die Ablaufverfolgung nur, wenn ein Experte des Technischen Supports Sie dazu auffordert.

Protokollierung aktivieren

Dieses Kontrollkästchen aktiviert/deaktiviert die Erstellung von Protokolldateien.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Im Abschnitt **Kennwortschutz** können Sie den Kennwortschutz für unerwünschte Aktionen auf Ihrem Computer aktivieren.

Kennwortschutz aktivieren

Dieses Kontrollkästchen aktiviert/deaktiviert den Kennwortschutz für unerwünschte Aktionen.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Wenn Sie dieses Kontrollkästchen aktivieren, wird ein Fenster geöffnet, in dem Sie das Administratorkennwort festlegen und konfigurieren können.

Einstellungen

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Einstellungen des Administratorkennworts ändern können.



Mithilfe dieser Schaltfläche können Sie verhindern, dass die Einstellungen der Anwendung Kaspersky Endpoint Security von Benutzern ohne Administratorrechte geändert werden.



Bei Klick auf diese Schaltfläche werden Sie aufgefordert, die Anmeldedaten des Administrators einzugeben. Nachdem Sie die Anmeldedaten des Administrators eingegeben haben, können Sie die Anwendungseinstellungen bearbeiten.

Das Fenster „Einstellungen des Schutzes vor E-Mail-Bedrohungen“

Archive überspringen, wenn größer als n MB

Wenn dieses Kontrollkästchen aktiviert ist, berücksichtigt der Schutz vor E-Mail-Bedrohungen die Größe von Archiven, die an E-Mail-Nachrichten angehängt sind. Archive werden von der Untersuchung ausgeschlossen, wenn ihre Größe den angegebenen Wert überschreitet.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht der Schutz vor E-Mail-Bedrohungen alle Archive, wobei die Größe der E-Mail-Anhänge keine Rolle spielt.

Der Standardwert ist 8 MB.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Maximale Untersuchungsdauer für Archive n Sek.

Wenn dieses Kontrollkästchen aktiviert ist, gilt eine maximale Untersuchungsdauer für Archive, die an E-Mail-Nachrichten angehängt sind.

Wenn dieses Kontrollkästchen deaktiviert ist, wird die Untersuchungsdauer von Archiven nicht begrenzt.

Standardmäßig ist ein Wert von 5 Sekunden eingestellt.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Das Fenster „Netzwerkpaketregel“

Regelname

Name der Netzwerkpaketregel.

Im Abschnitt **Aktion** können Sie die Aktion auswählen, die Kaspersky Endpoint Security beim Erkennen einer Netzwerkaktivität ausführen soll.

Im Abschnitt **Protokoll** können Sie das Protokoll angeben, für das die Netzwerkregel gelten soll.

Im Abschnitt **Richtung** können Sie die Richtung der überwachten Netzwerkaktivität angeben.

Im Abschnitt **TTL** können Sie die Lebensdauer der überwachten Netzwerkpakete angeben.

Im Abschnitt **Netzwerkadapter** können Sie die Netzwerkadapter angeben, für die die Netzwerkregel gelten soll.

Im Abschnitt **Remote-Adresse** können Sie die Netzwerkadressen der Remote-Geräte angeben, die Netzwerkpakete senden und empfangen dürfen.

Im Abschnitt **Lokale Adresse** können Sie die lokalen Netzwerkadressen der Geräte angeben, die Netzwerkpakete senden und empfangen dürfen.

Protokollieren

Mit diesem Kontrollkästchen wird die Protokollierung von Firewall-Ereignissen aktiviert/deaktiviert.

Wenn dieses Kontrollkästchen aktiviert ist, werden Firewall-Ereignisse protokolliert.

Wenn dieses Kontrollkästchen deaktiviert ist, werden Firewall-Ereignisse nicht protokolliert.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Das Fenster „Netzwerkadapter“

Name des Adapters

Name des Netzwerkadapters.

Schnittstellentyp

Aus dieser Dropdown-Liste können Sie den Schnittstellentyp des Netzwerkadapters auswählen.

IP-Adressen

Die Liste der IP-Adressen.

MAC-Adressen

Die Liste der MAC-Adressen.

Das Fenster „Netzwerkadapter“

Name

Diese Spalte enthält den Namen des Netzwerkadapters.

Schnittstellentyp

Diese Spalte enthält den Schnittstellentyp des Netzwerkadapters.

IP-Adressen

Diese Spalte enthält die IP-Adressen des Netzwerkadapters.

MAC-Adressen

Diese Spalte zeigt die MAC-Adresse des Netzwerkadapters.

Das Fenster „Lokale Adressen“

Lokale Adressen

Diese Spalte enthält die lokalen Adressen.

Das Fenster „Lokal Adresse“

Typ

In dieser Dropdown-Liste können Sie den Typ des lokalen IP-Eintrags angeben, für den die Netzwerkregel gelten soll.

IP-Adresse

IP-Adresse des Remote-Computers. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **IP-Adresse** ausgewählt haben.

Anfang des Bereichs

Eingabefeld für den Anfang des Bereichs der IP-Adresse. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich der IP-Adressen** ausgewählt haben.

Ende des Bereichs

Eingabefeld für das Ende des IP-Adressbereichs. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich der IP-Adressen** ausgewählt haben.

Das Fenster „Remote-Adressen“

Remote-Adressen

Diese Spalte enthält die Remote-Adressen.

Das Fenster „Remote-Adresse“

Typ

In dieser Dropdown-Liste können Sie den Typ des Eintrags für die Remote-Adresse angeben, für den die Netzwerkregel gelten soll.

Adresse

Eingabefeld für die IP-Adresse oder den DNS-Namen. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **IP-Adresse oder DNS-Name** ausgewählt haben.

Anfang des Bereichs

Eingabefeld für den Anfang des Bereichs der IP-Adresse. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich der IP-Adressen** ausgewählt haben.

Ende des Bereichs

Eingabefeld für das Ende des IP-Adressbereichs. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich der IP-Adressen** ausgewählt haben.

Das Fenster „Vorlagen“

Vorlagen für Netzwerkregeln

Diese Spalte enthält Vorlagen für Netzwerkregeln.

Die Registerkarte „Regeln für Netzwerkpakete“

Netzwerkdienst

Name der Netzwerkregel.

Aktion

Aktion, die von der Firewall ausgeführt werden soll, wenn eine Netzwerkaktivität dieses Typs erkannt wird.

Adresse

Netzwerkadressen, auf die die Netzwerkregel angewendet wird.

Die Registerkarte „Verfügbare Netzwerke“

Name

Diese Spalte enthält den Namen des Netzwerks.

Netzwerkstatus

Diese Spalte enthält den Netzwerkstatus des Netzwerks.

IP-Adresse

Diese Spalte enthält Netzwerk-IP-Adressen.

Das Fenster „Verfügbares Netzwerk“

Netzwerkname

Name des Netzwerks.

Netzwerkstatus

Die Dropdown-Liste für den Netzwerkstatus.

IP-Adresse

Die IP-Adresse des Netzwerks.

Das Fenster „MAC-Adresse“

Typ

In dieser Dropdown-Liste können Sie den Typ des Eintrags für die MAC-Adresse angeben, für den die Netzwerkregel gelten soll.

MAC-Adresse

MAC-Adresse des Remote-Computers. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **MAC-Adresse** ausgewählt haben.

Maske

Eingabefeld für die Maske der MAC-Adresse. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Maske der MAC-Adresse** ausgewählt haben.

Anfang des Bereichs

Eingabefeld für den Anfang des Bereichs der MAC-Adresse. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich für MAC-Adressen** ausgewählt haben.

Ende des Bereichs

Eingabefeld für das Ende des MAC-Adressbereichs. Dieses Feld ist nur verfügbar, wenn Sie in der Dropdown-Liste **Typ** den Punkt **Bereich für MAC-Adressen** ausgewählt haben.

Der Bericht „Systemereignisse“

Der rechte Fensterbereich enthält einen Bericht über die Verwendung von Kaspersky Endpoint Security.

Zeitpunkt

Diese Spalte nennt Datum und Uhrzeit des Ereignisses.

Ereignis

Diese Spalte nennt den Status des Ereignisses.

Programmname

In dieser Spalte wird der Name des Programms angezeigt, in dem das Ereignis aufgetreten ist.

Benutzer

Diese Spalte nennt den Namen des Benutzers angezeigt, der dieses Ereignis ausgelöst hat.

Benutzertyp

In dieser Spalte wird der Typ des Benutzers angezeigt, der dieses Ereignis initiiert hat.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Bericht über Verarbeitete Objekte

Im rechten Fensterbereich befindet sich die Liste mit allen infizierten Objekte und gefährlichen Objekten, welche die Anwendung Kaspersky Endpoint Security im Web-Datenverkehr gefunden hat.

Uhrzeit

Diese Spalte zeigt den Zeitpunkt, zu dem das Objekt gefunden wurde.

Objekt

Diese Spalte zeigt entweder den Pfad des Speicherorts, an dem das Objekt gefunden wurde, oder die Webadresse des Objekts.

Status

Diese Spalte zeigt die Aktion, die das Programm Kaspersky Internet Security nach dem Fund des Objekts ausgeführt hat.

Erkannt

Diese Spalte zeigt den Typ des gefundenen Objekts. Die Klassifikation entspricht der Viren-Enzyklopädie von Kaspersky.

Name

Diese Spalte zeigt den Namen des gefundenen Objekts. Die Klassifikation entspricht der Viren-Enzyklopädie von Kaspersky.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Datenbanken-Update“

Der rechte Fensterbereich enthält Berichte über die Update-Aufgaben, die von der Anwendung ausgeführt wurden.

Start

Diese Spalte zeigt den Startzeitpunkt (Datum und Uhrzeit) für die einzelnen Update-Aufgaben. Wenn die Liste der Vorgänge erweitert ist, enthält diese Spalte auch die Vorgänge, die während des Programm-Updates ausgeführt wurden, sowie den jeweiligen Zeitpunkt, zu dem sie ausgeführt wurden.

Status

In dieser Spalte wird der Status einer Update-Aufgabe angezeigt.

Größe

Diese Spalte zeigt die Größe der heruntergeladenen Update-Dateien.

Durchschnittsgeschwindigkeit

Diese Spalte zeigt die Übertragungsrate für den Download der Update-Dateien an.

Ende

Diese Spalte zeigt den Zeitpunkt an, zu dem eine Update-Aufgabe abgeschlossen wurde.

Mit dieser Schaltfläche wird die Liste der Vorgänge, die zur Update-Aufgabe gehören, erweitert.

Mit dieser Schaltfläche wird die Liste der Vorgänge, die zur Update-Aufgabe gehören, reduziert.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Bericht über die Untersuchung

Der rechte Fensterbereich enthält Berichte über die Untersuchungsaufgaben, die von Kaspersky Endpoint Security ausgeführt wurden.

Aufgabe

Diese Spalte zeigt den Namen der Untersuchungsaufgabe an.

Status

Diese Spalte zeigt den Status einer Untersuchungsaufgabe oder den Status der untersuchten Objekte an.

Datum

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit) der Aufgabe zur Virensuche an.

Initiator

In dieser Spalte wird der Benutzer, die Anwendung oder der Prozess angezeigt, der bzw. die eine Untersuchungsaufgabe initiiert hat.

Wenn Sie auf diese Schaltfläche klicken, wird die Liste der untersuchten Objekte erweitert.

Wenn Sie auf diese Schaltfläche klicken, wird die Liste der untersuchten Objekte reduziert.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Bericht über den „Schutz vor bedrohlichen Dateien“

Der rechte Fensterbereich enthält einen Bericht über den „Schutz vor bedrohlichen Dateien“.

Datum

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit) an, zu dem die Anwendung auf ein untersuchtes Objekt zugegriffen hat.

Pfad

Diese Spalte zeigt den Pfad des ursprünglichen Speicherorts eines untersuchten Objekts an.

Status

In dieser Spalte wird der Status eines untersuchten Objekts angezeigt.

Programmname

Diese Spalte zeigt die Anwendung an, die auf ein untersuchtes Objekt zugegriffen hat.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Bericht über den „Schutz vor Web-Bedrohungen“

Der rechte Fensterbereich enthält einen Bericht über den „Schutz vor Web-Bedrohungen“.

Datum

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit), zu welchem die Objekte des Web-Datenverkehrs gefunden wurden.

Webadresse

Diese Spalte zeigt die Objekte des Web-Datenverkehrs, die vom „Schutz vor Web-Bedrohungen“ gefunden wurden. Für jedes im Web-Datenverkehr gefundene Objekt wird in dieser Spalte die Webadresse genannt, unter der das Objekt gefunden wurde.

Status

Diese Spalte zeigt den Status der im Web-Datenverkehr gefundenen Objekte.

Programmname

Diese Spalte zeigt das Programm, welches auf die gefundenen Objekte des Web-Datenverkehrs zugegriffen hat.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Schutz vor E-Mail-Bedrohungen“

Der rechte Fensterbereich enthält einen Bericht über den Schutz vor E-Mail-Bedrohungen.

Datum

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem ein infiziertes Objekt in einer E-Mail-Nachricht gefunden wurde.

Pfad

Diese Spalte zeigt Informationen über die E-Mail-Nachricht, in der das infizierte Objekt gefunden wurde.

Status

Diese Spalte zeigt die Aktion, die Kaspersky Endpoint Security ausführt, wenn ein infiziertes Objekt gefunden wird.

Programmname

Diese Spalte zeigt den Namen des E-Mail-Clients.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Bericht über den „Schutz vor Netzwerkbedrohungen“

Der rechte Fensterbereich enthält einen Bericht über den „Schutz vor Netzwerkbedrohungen“.

Datum

Diese Spalte zeigt den Zeitpunkt (Datum und Uhrzeit), zu welchem die gefährliche Netzwerkaktivität auf dem Computer erkannt wurde.

IP-Adresse

Diese Spalte zeigt die IP-Adresse des Computers an, für den Kaspersky Endpoint Security eine gefährliche Netzwerkaktivität erkannt hat.

Status

In dieser Spalte wird die Aktion angezeigt, die Kaspersky Endpoint Security ausführt, wenn eine gefährliche Netzwerkaktivität erkannt wird.

Angriffstyp

Diese Spalte zeigt den Typ des erkannten Netzwerkangriffs.

Lokaler Port

Diese Spalte zeigt die Nummer des lokalen Ports, über den ein Angriffsversuch erfolgt ist.

Protokoll

Diese Spalte zeigt den Typ des Protokolls an, welches für die Durchführung des Angriffs verwendet wurde.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht Endpoint Detection and Response

Der rechte Fensterbereich enthält einen Bericht über die Komponente Endpoint Detection and Response.

Datum

Diese Spalte zeigt Datum und Uhrzeit von Ereignissen.

Ereignis

Diese Spalte zeigt den Status von Ereignissen.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Firewall“

Der rechte Fensterbereich enthält einen Bericht über die Firewall.

Datum

Diese Spalte zeigt Datum und Uhrzeit von Ereignissen.

Ereignis

Diese Spalte zeigt den Status von Ereignissen.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Exploit-Prävention“

Der rechte Fensterbereich enthält einen Bericht über die Exploit-Prävention.

Datum

Diese Spalte zeigt Datum und Uhrzeit von Ereignissen.

Ereignis

Diese Spalte zeigt den Status von Ereignissen.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Gerätekontrolle“

Der rechte Fensterbereich enthält einen Bericht über die Gerätekontrolle.

Datum

Diese Spalte zeigt Datum und Uhrzeit von Ereignissen.

Ereignis

Diese Spalte zeigt den Status von Ereignissen.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Der Bericht „Aktivitätsmonitor“

Der rechte Fensterbereich enthält einen Bericht über die Komponente Aktivitätsmonitor.

Datum

Diese Spalte zeigt Datum und Uhrzeit von Ereignissen.

Ereignis

Diese Spalte zeigt den Status von Ereignissen.



Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie den Bericht als TXT-Datei speichern können.

Fenster „Kundensupport“

Dieses Fenster bietet folgende Informationen:

- Version von Kaspersky Endpoint Security
- Veröffentlichungsdatum der Datenbanken, die Kaspersky Endpoint Security momentan verwendet
- Version des auf dem Computer installierten Betriebssystems

Technischer Support

Diese Schaltfläche öffnet die Wissensdatenbank des Technischen Supports von Kaspersky. Dort finden Sie Artikel zu Kaspersky Endpoint Security, die von den Kaspersky-Experten veröffentlicht wurden.

Community

Diese Schaltfläche öffnet die Community, in der Sie mit Kaspersky-Experten und anderen Nutzern über Kaspersky Endpoint Security diskutieren können.

Schließen

Mit dieser Schaltfläche wird das Kundensupport-Fenster geschlossen.

Das Fenster „Einstellungen für Zertifikate“

Auf der Registerkarte **Allgemein** können Sie den Zertifikatspeicher für die Untersuchung des verschlüsselten HTTPS-Datenverkehrs im Browser Mozilla Firefox auswählen:

- **Schlüsselbund "System Roots" (empfohlen)**
- **Zertifikatspeicher aus den Mozilla Firefox-Einstellungen**

  In diesem Fall müssen Sie das Kaspersky Endpoint Security-Zertifikat manuell zum Zertifikatspeicher des Browsers Mozilla Firefox hinzufügen. Weitere Informationen finden Sie unter So fügen Sie das Zertifikat von Kaspersky Endpoint Security zum Zertifikatspeicher von Mozilla Firefox hinzu.

Im Fenster **Vertrauenswürdige Zertifikate** können Sie eine Liste mit vertrauenswürdigen Stammzertifikaten erstellen, um eine Verbindung zu den entsprechenden Servern herzustellen, ohne dabei Benachrichtigungen zu erhalten.

Die Liste der vertrauenswürdigen Stammzertifikate ist standardmäßig leer.

+

Ein Klick auf diese Schaltfläche öffnet einen Dialog. Dort können Sie Zertifikate hinzufügen, die als vertrauenswürdig gelten sollen.

–

Bei Klick auf diese Schaltfläche wird das ausgewählte Zertifikat aus der Liste für vertrauenswürdige Zertifikate gelöscht.

Name des Zertifikats

Diese Spalte enthält die Namen der vertrauenswürdigen Stammzertifikate.

Abbrechen

Bei Klick auf diese Schaltfläche wird das Fenster geschlossen, ohne die Änderungen zu speichern.

Speichern

Bei Klick auf diese Schaltfläche wird die aktuelle Liste der vertrauenswürdigen Stammzertifikate gespeichert und das Fenster wird geschlossen.

Das Fenster „Zertifikat überprüfen“

Zertifikat anzeigen

Mit dieser Schaltfläche wird ein Systemfenster mit Informationen über das Zertifikat geöffnet.

Abbrechen

Mit dieser Schaltfläche wird das Fenster geschlossen.

Zu „Vertrauenswürdig“ hinzufügen

Bei Klick auf diese Schaltfläche wird das Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzugefügt. Dann können Sie künftig ohne Benachrichtigungen eine Verbindung zum entsprechenden Server herzustellen.

Verbinden

Bei Klick auf diese Schaltfläche wird eine Verbindung mit dem Server hergestellt.

Hinweis: Die verfügbaren Schaltflächen können je nach Zertifikatstyp variieren.

Das Fenster „Zertifikat auswählen“

Liste der verfügbaren Zertifikate

Aktivieren Sie das Kontrollkästchen neben einem Zertifikat, um für die Verbindung mit dem Server zu verwenden.

Zertifikat anzeigen

Mit dieser Schaltfläche wird ein Systemfenster mit Informationen über das Zertifikat geöffnet.

Abbrechen

Mit dieser Schaltfläche wird das Fenster geschlossen.

Weiter

Wenn Sie auf diese Schaltfläche klicken, wird die Verbindung mit dem Server mithilfe des ausgewählten Zertifikats fortgesetzt.