

ESET Endpoint Security for macOS

Benutzerhandbuch

[Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen](#)



Copyright ©2023 by ESET, spol. s r.o.

ESET Endpoint Security for macOS wurde entwickelt von ESET, spol. s r.o.

Weitere Informationen finden Sie unter <https://www.eset.com>.

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnahmen, Scannen oder auf andere Art.

ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung Änderungen an allen hier beschriebenen Software-Anwendungen vorzunehmen.

Technischer Support: <https://support.eset.com>

REV. 19.03.2023

1 ESET Endpoint Security for macOS	1
1.1 Neuerungen in Version 6	1
1.2 Systemanforderungen	2
2 Einführung in ESET PROTECT	2
3 Einführung in ESET PROTECT CLOUD	4
4 Remoteinstallation	4
4.1 Remote-Installationspaket erstellen	7
5 Lokale Installation	9
5.1 Standardinstallation	11
5.2 Benutzerdefinierte Installation	12
5.3 Systemerweiterungen lokal erlauben	13
5.4 Vollständigen Laufwerkszugriff lokal erlauben	14
6 Produktaktivierung	15
7 Deinstallation	16
8 Übersicht	16
8.1 Tastaturbefehle	17
8.2 Überprüfen der Funktionsfähigkeit des Systems	17
8.3 Vorgehensweise bei fehlerhafter Ausführung des Programms	18
9 Computerschutz	18
9.1 Viren- und Spyware-Schutz	19
9.1 Allgemein	19
9.1 Ausschlussfilter	19
9.1 Systemstart-Schutz	20
9.1 Echtzeit-Dateischutz	20
9.1 Erweiterte Einstellungen	21
9.1 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?	21
9.1 Echtzeit-Dateischutz prüfen	21
9.1 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz	22
9.1 On-Demand-Prüfung	22
9.1 Prüfungstyp	23
9.1 Smart-Prüfung	23
9.1 Prüfen mit speziellen Einstellungen	23
9.1 Zu prüfende Objekte	24
9.1 Prüfprofile	24
9.1 ThreatSense Einstellungen für	25
9.1 Objekte	26
9.1 Optionen	26
9.1 Säubern	26
9.1 Ausschlussfilter	27
9.1 Grenzen	27
9.1 Sonstige	28
9.1 Eingedrungene Schadsoftware wurde erkannt	28
9.2 Web- und E-Mail-Schutz	29
9.2 Web-Schutz	29
9.2 Ports	30
9.2 URL-Listen	30
9.2 E-Mail-Schutz	30
9.2 Prüfen von E-Mails per POP3-Protokoll	31
9.2 Prüfen des IMAP-Protokolls	31
9.3 Phishing-Schutz	32

10 Firewall	32
10.1 Filtermodi	32
10.2 Firewall-Regeln	33
10.2 Erstellen neuer Regeln	34
10.3 Firewall-Zonen	35
10.4 Firewall-Profile	35
10.5 Firewall-Logs	35
11 Medienkontrolle	36
11.1 Regel-Editor	36
12 Web-Kontrolle	38
13 Tools	39
13.1 Log-Dateien	39
13.1 Log-Wartung	40
13.1 Log-Filter	41
13.2 Taskplaner	41
13.2 Erstellen von Tasks	42
13.2 Erstellen eines benutzerdefinierten Tasks	44
13.3 LiveGrid®	44
13.3 Verdächtige Dateien	45
13.4 Quarantäne	46
13.4 Quarantäne für Dateien	46
13.4 Wiederherstellen einer Datei aus der Quarantäne	46
13.4 Einreichen von Dateien aus der Quarantäne	46
13.5 Berechtigungen	47
13.6 Präsentationsmodus	47
13.7 Ausgeführte Prozesse	48
14 Benutzeroberfläche	49
14.1 Warnungen und Hinweise	49
14.1 Warnungen anzeigen	50
14.1 Schutzstatus	50
14.2 Kontextmenü	51
15 Update	51
15.1 Einstellungen für Updates	51
15.1 Erweiterte Einstellungen	53
15.2 So erstellen Sie Update-Tasks	53
15.3 Systemupdates	54
15.4 Einstellungen importieren/exportieren	55
15.5 Einstellungen für den Proxyserver	55
15.6 Freigegebener lokaler Cache	56
16 Endbenutzer-Lizenzvereinbarung	56
17 Privacy Policy	63

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS 6 ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des Scanmoduls ThreatSense® bietet in Verbindung mit unserer Firewall eine schnelle und sichere Lösung, die Sicherheit Ihres Computers zu gewährleisten. Das Ergebnis ist ein intelligentes System, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden können.

ESET Endpoint Security for macOS 6 ist eine umfassende Sicherheitslösung und das Produkt unserer langfristigen Bemühung, maximalen Schutz bei minimaler Systembelastung zu bieten. Mithilfe der auf künstlicher Intelligenz basierenden Spitzentechnologien kann das Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderer durch das Internet übertragener Angriffe aktiv verhindert werden, ohne dass die Systemleistung beeinträchtigt oder Ihr Computer vom Netz getrennt würde.

Dieses Produkt wurde speziell für die Nutzung auf Workstations in kleineren Unternehmen entwickelt. In Verbindung mit ESET PROTECT (ehemals ESET Security Management Center) können Sie damit eine beliebige Anzahl von Client-Workstations verwalten, Policies und Regeln anwenden, Ereignisse überwachen und Änderungen auf beliebigen Computern im Netzwerk verwalten.

Neuerungen in Version 6

Die grafische Benutzeroberfläche von ESET Endpoint Security for macOS wurde komplett neu gestaltet, um eine verbesserte Sichtbarkeit und eine intuitivere Bedienung zu ermöglichen. Zu den zahlreichen Verbesserungen in Version 6 gehören:

- Unterstützung für ESET Enterprise Inspector - Ab ESET Endpoint Security for macOS Version 6.9 kann ESET Endpoint Security for macOS mit ESET Enterprise Inspector verbunden werden. ESET Enterprise Inspector (EEI) ist ein umfassendes Erkennungs- und Reaktionssystem für Endpunkte mit diesen Funktionen: Erkennung, Verwaltung und Auflösung von Vorfällen, Datensammlung und Indikatoren für die Erkennung von Angriffen, Anomalien, Verhaltensweisen und Policyverletzungen. Weitere Informationen zur Installation und zur Funktionsweise von ESET Enterprise Inspector finden Sie in der [ESET Enterprise Inspector-Hilfe](#).
- **Unterstützung für 64-Bit-Architekturen**
- **Firewall** – Sie können Firewall-Regeln jetzt direkt im Log oder im IDS (Intrusion detection system)-Benachrichtigungsfenster erstellen und Profile zu Netzwerkschnittstellen zuweisen.
- **Web-Kontrolle** – Sperrt Webseiten, die möglicherweise unerlaubte oder ungeeignete Inhalte enthalten.
- **Web-Schutz** – Der Web-Schutz überwacht die Kommunikation zwischen Webbrowsern und Remoteservern.
- **E-Mail-Schutz** – Überwacht eingehende E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden.
- **Phishing-Schutz** – Schützt Sie vor Versuchen betrügerischer Webseiten, an Passwörter und andere sicherheitsrelevante Informationen zu gelangen, indem sie sich als seriöse Webseiten ausgeben.
- **Medienkontrolle** – Mit dieser Funktion können Sie Medien bzw. Geräte scannen oder sperren oder erweiterte Filter- und/oder Berechtigungseinstellungen anpassen und definieren, wie Benutzer auf externe Geräte zugreifen und mit ihnen arbeiten können. Diese Funktion ist ab Produktversion 6.1 verfügbar.

- **Präsentationsmodus** – Mit dieser Option können Sie ESET Endpoint Security for macOS im Hintergrund ausführen und Pop-up-Fenster und geplante Tasks unterdrücken.
- **Freigegebener lokaler Cache** – Ermöglicht schnellere Prüfungen in virtuellen Umgebungen.

Systemanforderungen

Für den optimalen Betrieb von ESET Endpoint Security for macOS sollte Ihr System die folgenden Hardware- und Softwareanforderungen erfüllen:

	Systemanforderungen:
Prozessorarchitektur	Intel 64-bit, Apple ARM 64-Bit
Betriebssystem	macOS 10.12 und höher
Arbeitsspeicher	300 MB
Freier Speicherplatz auf dem Datenträger	200 MB

 Zusätzlich zu den bereits unterstützten Intel-Versionen unterstützen ESET Endpoint Security for macOS Version 6.10.900.0 und neuere Versionen auch den Apple ARM-Chip mit Rosetta 2.

Einführung in ESET PROTECT

Mit ESET PROTECT können Sie ESET-Produkte auf Arbeitsstationen, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Standort aus verwalten.

Mit der ESET PROTECT-Web-Konsole können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies anwenden, den Systemstatus überwachen und schnell auf Probleme oder Ereignisse auf Remotecomputern reagieren. Siehe auch [Übersicht über die ESET PROTECT-Architektur und -Infrastruktur](#), [Erste Schritte mit der ESET PROTECT-Web-Konsole](#) und [Unterstützte Umgebungen für die Desktopbereitstellung](#).

ESET PROTECT besteht aus den folgenden Komponenten:

- [ESET PROTECT Server](#) – Der ESET PROTECT Server kann auf Windows- und Linux-Servern installiert werden und ist ebenfalls als virtuelle Appliance erhältlich. Diese Komponente ist für die Kommunikation mit Agenten zuständig und sammelt und speichert Anwendungsdaten in der Datenbank.
- [ESET PROTECT-Web-Konsole](#) – Die ESET PROTECT-Web-Konsole ist die wichtigste Oberfläche für die Verwaltung von Clientcomputern in Ihrer Umgebung. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf nicht verwalteten Computern verwendet werden. Nach der Installation des ESET PROTECT Servers (Server) können Sie die Web-Konsole in Ihrem Webbrowser öffnen. Wenn der Webserver über das Internet erreichbar ist, können Sie ESET PROTECT von jedem beliebigen Standort und Gerät mit Internetverbindung verwenden.
- [ESET Management Agent](#) – Der ESET Management Agent erleichtert die Kommunikation zwischen ESET PROTECT Server und den Clientcomputern und muss auf allen Clientcomputern installiert werden, um die Kommunikation zwischen dem Computer und dem ESET PROTECT Server zu ermöglichen. Da der ESET Management Agent auf dem Clientcomputer installiert wird und mehrere Sicherheitsszenarien speichern kann,

wird mit dessen Einsatz die Reaktionszeit für neue Ereignisse deutlich reduziert. Mit der ESET PROTECT-Web-Konsole können Sie den [ESET Management Agenten auf nicht verwalteten Computern bereitstellen](#), die Sie über Active Directory oder mit dem ESET [RD Sensor](#) gefunden haben. Bei Bedarf können Sie den [ESET Management Agenten](#) auch manuell auf Clientcomputern installieren.

- [Rogue Detection Sensor](#) – Der ESET PROTECT Rogue Detection (RD) Sensor erkennt nicht verwaltete Computer in Ihrem Netzwerk und übermittelt deren Daten an den ESET PROTECT Server. Auf diese Weise können Sie neue Clientcomputer schnell und einfach zu Ihrem gesicherten Netzwerk hinzufügen. Der RD Sensor merkt sich bereits erkannte Computer und sendet nicht zweimal die gleichen Informationen.

- [Apache HTTP Proxy](#) – Dieser Dienst kann zusammen mit ESET PROTECT verwendet werden und erfüllt die folgenden Aufgaben:

 - Verteilen von Updates an Clientcomputer und von Installationspaketen an den ESET Management Agenten.

 - Weiterleiten der Kommunikation von ESET Management Agenten zum ESET PROTECT Server.

- [Mobile Device Connector](#) – Mit dieser ESET PROTECT-Komponente können Sie Mobilgeräte (Android und iOS) verwalten und ESET Endpoint Security für Android administrieren.

- [Virtuelle ESET PROTECT-Appliance](#) – Die ESET PROTECT-VA steht für Benutzer zur Verfügung, die ESET PROTECT in einer virtualisierten Umgebung ausführen möchten.

- [ESET PROTECT Virtual Agent Host](#) – Diese ESET PROTECT-Komponente virtualisiert Agenten-Entitäten, um virtuelle Computer ohne Agenten verwalten zu können. Diese Lösung ermöglicht die Automatisierung und die Nutzung dynamischer Gruppen und denselben Funktionsumfang für die Taskverwaltung wie mit dem ESET Management Agenten auf physischen Computern. Der virtuelle Agent erfasst Informationen von virtuellen Computern und sendet diese an den ESET PROTECT Server.

- [Mirror-Tool](#) – Das Mirror-Tool wird für Offline-Updates von Modulen benötigt. Falls Ihre Clientcomputer nicht mit dem Internet verbunden sind, können Sie die Update-Dateien mit dem Mirror-Tool von den ESET-Updateservern herunterladen und lokal speichern.

- [ESET Remote Deployment Tool](#) – Dieses Tool dient zur Bereitstellung von All-in-One-Paketen, die in der <%PRODUCT%-Web-Konsole erstellt wurden. Dies ist ein praktischer Weg, um den ESET Management Agenten mit einem ESET-Produkt auf Computern in einem Netzwerk zu verteilen.

- [ESET Business Account](#) – Mit dem neuen Lizenzierungsportal für ESET-Unternehmensprodukte können Sie Lizenzen verwalten. Im Bereich [ESET Business Account](#) in diesem Dokument finden Sie eine Anleitung zur Produktaktivierung. Weitere Informationen zur Nutzung von ESET Business Account finden Sie im [Benutzerhandbuch](#) für den ESET Business Account. Falls Sie bereits einen Benutzernamen und ein Passwort von ESET erhalten haben und diese Daten in einen Lizenzschlüssel konvertieren möchten, lesen Sie den Abschnitt [Veraltete Lizenzdaten konvertieren](#).

- [ESET Enterprise Inspector](#) – Ein umfassendes Erkennungs- und Reaktionssystem für Endpunkte mit den folgenden Funktionen: Erkennung, Verwaltung und Auflösung von Vorfällen, Datensammlung und Indikatoren für die Erkennung von Angriffen, Anomalien, Verhaltensweisen und Policyverletzungen.

Mit der ESET PROTECT-Web-Konsole können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies erzwingen, den Systemstatus überwachen und schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren.

 Weitere Informationen finden Sie online im [ESET PROTECT-Benutzerhandbuch](#).

Einführung in ESET PROTECT CLOUD

mit ESET PROTECT CLOUD können Sie ESET-Produkte auf Arbeitsstationen und Servern in einer Netzwerkumgebung von einem zentralen Standort aus verwalten, ohne physische oder virtuelle Server zu benötigen wie für ESET PROTECT oder ESET Security Management Center. Mit der ESET PROTECT CLOUD-Web-Konsole können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies umsetzen, den Systemstatus überwachen und schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren.

- [Weitere Informationen finde Sie online im ESET PROTECT CLOUD-Benutzerhandbuch](#)

Remoteinstallation

Vor der Installation

^ [macOS 10.15 und älter](#)

Bevor Sie ESET Endpoint Security for macOS auf macOS 10.13 und neueren Versionen installieren, sollten Sie ESET-Kernelerweiterungen erlauben. Auf macOS 10.14 und neueren Versionen sollten Sie außerdem vollständigen Laufwerkszugriff auf Zielcomputern erlauben. Wenn Sie diese Optionen vor der Installation nicht erlauben, erhalten die Benutzer die Benachrichtigungen **Systemerweiterung blockiert** und **Ihr Computer ist teilweise geschützt**, bis Sie die ESET-Kernelerweiterungen und den vollständigen Laufwerkszugriff erlauben.

Um die ESET-Kernelerweiterungen und den vollständigen Laufwerkszugriff remote zu erlauben, muss Ihr Computer bei einem [MDM-Server \(Mobile Device Management\)](#) registriert sein, beispielsweise Jamf.

ESET-Systemerweiterungen erlauben

So können Sie Kernelerweiterungen auf Ihrem Gerät remote erlauben:

o Falls Sie Jamf als MDM verwenden, lesen Sie dazu unseren [Knowledgebase-Artikel](#).

o Falls Sie ein anderes MDM verwenden, [laden Sie das .plist-Konfigurationsprofil herunter](#). Generieren Sie zwei UUIDs mit einem UUID-Generator Ihrer Wahl und verwenden Sie einen Texteditor, um die Zeichenfolgen [UUID 1 hier einfügen](#) und [UUID 2 hier einfügen](#) im heruntergeladenen Konfigurationsprofil zu ersetzen. Stellen Sie das .plist-Konfigurationsprofil mit dem MDM-Server bereit. Ihr Computer muss im MDM-Server registriert sein, um ein Konfigurationsprofil empfangen zu können.

Vollständigen Laufwerkszugriff erlauben

Auf macOS 10.14 wird nach der Installation die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Endpoint Security for macOS angezeigt. Um alle Funktionen von ESET Endpoint Security for macOS nutzen zu können und zu verhindern, dass diese Meldung angezeigt wird, müssen Sie ESET Endpoint Security for macOS vor der Produktinstallation **vollständigen Laufwerkszugriff erlauben**. So können Sie den **vollständigen Laufwerkszugriff remote erlauben**:

o Falls Sie Jamf als MDM verwenden, lesen Sie dazu unseren [Knowledgebase-Artikel](#).

o Um den **vollständigen Laufwerkszugriff remote zu erlauben**, [laden Sie die .plist-Konfigurationsdatei herunter](#). Generieren Sie zwei UUIDs mit einem UUID-Generator Ihrer Wahl und verwenden Sie einen

Texteditor, um die Zeichenfolgen `UUID 1` hier einfügen und `UUID 2` hier einfügen im heruntergeladenen Konfigurationsprofil. Stellen Sie das .plist-Konfigurationsprofil mit dem MDM-Server bereit. Ihr Computer muss im MDM-Server registriert sein, um ein Konfigurationsprofil empfangen zu können.

[^ macOS Big Sur \(11\)](#)

Bevor Sie ESET Endpoint Security for macOS auf macOS Big Sur installieren, müssen Sie ESET-Systemerweiterungen und vollständigen Laufwerkszugriff auf den Zielcomputern erlauben. Wenn Sie diese Optionen vor der Installation nicht erlauben, erhalten die Benutzer die Benachrichtigungen **Systemerweiterungen blockiert** und **Ihr Computer ist teilweise geschützt**, bis Sie die ESET-Systemerweiterungen erlauben und den vollständigen Laufwerkszugriff erlaubt haben. Die Systemerweiterungen können remote nur vor der Installation von ESET Endpoint Security for macOS erlaubt werden.

Um die ESET-Systemerweiterungen und den vollständigen Laufwerkszugriff remote zu erlauben, muss Ihr Computer bei einem [MDM-Server \(Mobile Device Management\)](#) registriert sein, beispielsweise Jamf.

ESET-Systemerweiterungen erlauben

So können Sie Systemerweiterungen auf Ihrem Gerät remote erlauben:

o Falls Sie Jamf als MDM verwenden, lesen Sie dazu unseren [Knowledgebase-Artikel](#).

o Falls Sie ein anderes MDM verwenden, [laden Sie das .plist-Konfigurationsprofil herunter](#). Stellen Sie das .plist-Konfigurationsprofil mit dem MDM-Server bereit. Ihr Computer muss beim MDM-Server registriert sein, um ein Konfigurationsprofil empfangen zu können. Verwenden Sie die folgenden Einstellungen, um ein eigenes Konfigurationsprofil zu erstellen:

Teambezeichner (TeamID)	P8DQRXPVLP
Paketbezeichner (BundleID)	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

Vollständigen Laufwerkszugriff erlauben

So können Sie den **vollständigen Laufwerkszugriff** remote erlauben:

o Falls Sie Jamf als MDM verwenden, lesen Sie dazu unseren [Knowledgebase-Artikel](#).

o Um den **vollständigen Laufwerkszugriff remote zu erlauben**, [laden Sie die .plist-Konfigurationsdatei](#) herunter. Stellen Sie die .plist-Konfigurationsprofildatei mit Ihrem MDM Server bereit. Ihr Computer muss beim MDM-Server registriert sein, um ein Konfigurationsprofil empfangen zu können. Verwenden Sie die folgenden Einstellungen, um ein eigenes Konfigurationsprofil zu erstellen:

ESET Endpoint Security	
Bezeichner	com.eset.ees.6
Bezeichnertyp	bundleID
Codeanforderung	identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP

App oder Dienst	SystemPolicyAllFiles
Zugriff	Allow

ESET Endpoint Antivirus & ESET Endpoint Security	
Bezeichner	com.eset.devices
Bezeichnertyp	bundleID
Codeanforderung	identifizier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
App oder Dienst	SystemPolicyAllFiles
Zugriff	Allow

ESET Endpoint Antivirus & ESET Endpoint Security	
Bezeichner	com.eset.endpoint
Bezeichnertyp	bundleID
Codeanforderung	identifizier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
App oder Dienst	SystemPolicyAllFiles
Zugriff	Allow

Installation

Vor der Installation können Sie ein Remote-Installationspaket mit einer voreingestellten ESET Endpoint Security for macOS-Konfiguration erstellen, das Sie später mit ESET PROTECT oder einer MDM-Lösung Ihrer Wahl bereitstellen können.

- [Erstellen Sie ein Remote-Installationspaket.](#)

Installieren Sie ESET Endpoint Security for macOS remote, indem Sie einen **Task „Software-Installation“** mit dem ESET-Verwaltungssystem erstellen:

- [Task „Software-Installation“ für ESET PROTECT](#)
- [Task „Software-Installation“ für ESET Security Management Center](#)

Nach Installation

Die Benutzer erhalten die folgende Benachrichtigung: „ESET Endpoint Security for macOS“ **möchte Netzwerkinhalte filtern**. Wenn diese Benachrichtigung angezeigt wird, klicken Sie auf **Zulassen**. Wenn Sie auf **Nicht zulassen** klicken, können Sie den Web-Schutz nicht verwenden.

Remote-Installationspaket erstellen

Installationspaket für die Apple Remote Desktop-Installation erstellen

1. Laden Sie das Standardinstallationspaket von der ESET-Website herunter:

[ESET Endpoint Security for macOS](#)

2. Klicken Sie auf die heruntergeladene Datei, um das Installationsprogramm für ESET Endpoint Security for macOS zu starten.



1. Klicken Sie auf **Installieren** ESET Endpoint Security for macOS.

2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Zulassen**, um festzustellen, ob die Software installiert werden kann.

3. Klicken Sie auf **Weiter**. Falls Sie ein Remote-Installationspaket erstellen, wird ESET Endpoint Security for macOS nicht installiert.

4. Überprüfen Sie die Systemanforderungen und klicken Sie auf **Weiter**.

5. Lesen Sie die ESET-Softwarelizenzvereinbarung und klicken Sie auf **Weiter** → **Zustimmen**, falls Sie zustimmen.

6. Wählen Sie unter **Installationsmodus** die Option **Remote** aus.

7. Wählen Sie aus, welche Produktkomponenten Sie installieren möchten. Standardmäßig sind alle Komponenten ausgewählt. Klicken Sie auf **Weiter**.

8. Wählen Sie im Schritt **Proxyserver** die passende Option für Ihre Internetverbindung aus. Verwenden Sie die

Standardsystemeinstellungen, falls Sie sich nicht sicher sind. Klicken Sie auf **Weiter**. Falls Sie einen Proxyserver verwenden, werden Sie im nächsten Schritt aufgefordert, die Proxyadresse, Ihren Benutzernamen und Ihr Passwort einzugeben.

9. Wählen Sie aus, wer die Programmkonfiguration ändern kann. Nur privilegierte Benutzer und Gruppen können diese Konfiguration ändern. Die Admin-Gruppe ist standardmäßig als privilegiert ausgewählt. Aktivieren Sie das Kontrollkästchen **Alle Benutzer anzeigen** oder **alle Gruppen anzeigen**, um alle virtuellen Benutzer und Gruppen anzuzeigen, z. B. Programme und Prozesse.

10. Aktivieren Sie ESET LiveGrid bei Bedarf auf dem Zielcomputer.

11. Aktivieren Sie bei Bedarf die Erkennung potenziell unerwünschter Anwendungen auf dem Zielcomputer.

12. Wählen Sie einen Firewall-Modus aus:

Automatischer Modus – Dies ist der Standardmodus. Dieser Modus eignet sich für Anwender, die eine möglichst einfache und praktische Nutzung der Firewall wünschen, bei der keine Regeln erstellt werden müssen. Im Automatikmodus ist der ausgehende Standarddatenverkehr für das System zugelassen und nicht initiierte Verbindungen aus dem Netzwerk werden blockiert. Sie haben auch die Möglichkeit, benutzerdefinierte Regeln hinzuzufügen.

Interaktiver Modus – Mit diesem Modus können Sie eine benutzerdefinierte Konfiguration für Ihre Firewall erstellen. Wenn eine Verbindung erkannt wird und keine Regel dafür existiert oder gilt, wird in einem Dialogfenster eine unbekannte Verbindung gemeldet. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll, und diese Auswahl kann als neue Regel für die Firewall übernommen werden. Wenn eine neue Regel erstellt wurde, werden Verbindungen dieser Art beim nächsten Verbindungsversuch entsprechend der Regel automatisch zugelassen oder blockiert.

13. Speichern Sie die Installationsdatei auf Ihrem Computer. Falls Sie zuvor eine Installationsdatei am Standardspeicherort erstellt haben, müssen Sie den Speicherort des Zielordners ändern oder die vorherigen Dateien löschen, bevor Sie fortfahren können. Damit ist die erste Phase der Remoteinstallation abgeschlossen. Das lokale Installationsprogramm wird beendet und erstellt Remoteinstallationsdateien im ausgewählten Zielordner.

Remoteinstallationsdateien:

- *esets_setup.dat* – Einrichtungsdaten, die Sie im Setupbereich des Installationsprogramms eingegeben haben
- *program_components.dat* – Einrichtungsdaten für die ausgewählten Programmkomponenten. Diese Datei ist optional und wird erstellt, wenn Sie bestimmte ESET Endpoint Security for macOS-Komponenten nicht installieren.
- *esets_remote_install.pkg* – Remote-Installationspaket
- *esets_remote_uninstall.sh* – Remote-Deinstallationskript

Apple Remote Desktop installieren

1. Öffnen Sie Apple Remote Desktop und verbinden Sie sich mit dem Zielcomputer. Weitere Informationen finden Sie in der [Apple Remote Desktop-Dokumentation](#).

2. Kopieren Sie die folgenden Dateien mit der Option **Datei oder Ordner kopieren** in Apple Remote Desktop in den Ordner */tmp* auf dem Zielcomputer:

Falls Sie alle Komponenten installieren, kopieren Sie:

– *esets_setup.dat*

Falls Sie nicht alle Produktkomponenten installieren, kopieren Sie:

– *esets_setup.dat*

– *product_components.dat*

3. Mit dem Befehl **Pakete installieren** können Sie die Datei *esets_remote_install.pkg* auf dem Zielcomputer installieren.

Apple Remote Desktop remote deinstallieren

1. Öffnen Sie Apple Remote Desktop und verbinden Sie sich mit dem Zielcomputer. Weitere Informationen finden Sie in der [Apple Remote Desktop-Dokumentation](#).

2. Kopieren Sie die das Skript *esets_remote_uninstall.sh* mit der Option **Datei oder Ordner kopieren** in Apple Remote Desktop in den Ordner */tmp* auf dem Zielcomputer.

3. Senden Sie in Apple Remote Desktop den folgenden **UNIX-Shellbefehl** an den Zielcomputer und führen Sie ihn aus:

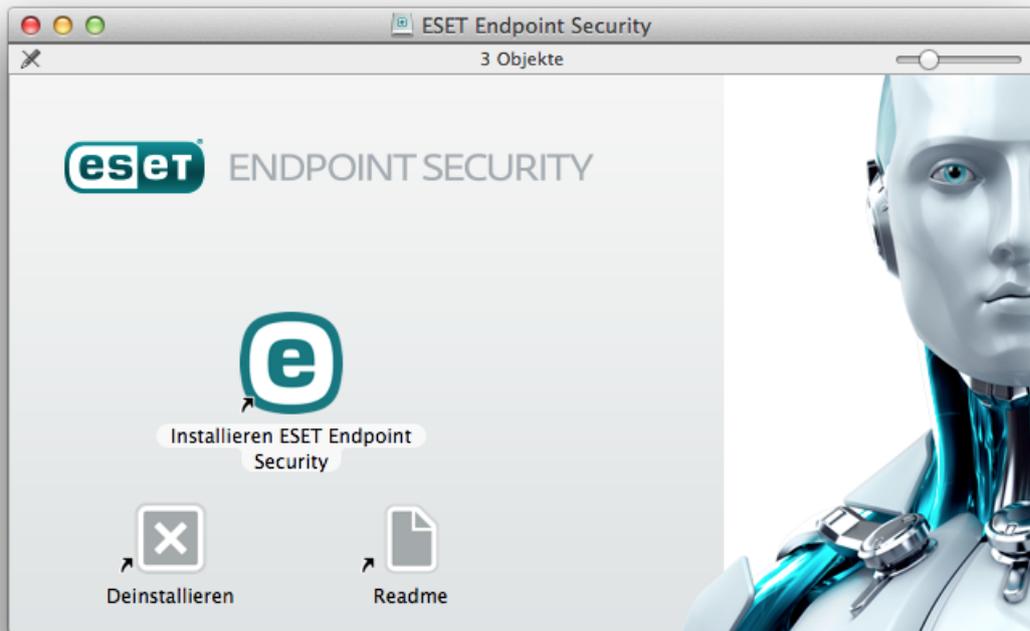
```
/tmp/esets_remote_uninstall.sh
```

Nach Abschluss der Deinstallation wird die Konsole in Apple Remote Desktop auf dem Zielcomputer angezeigt.

Installation

Der Installationsassistent führt Sie durch die grundlegende Einrichtung. Eine ausführliche Anleitung finden Sie in unserem [Knowledgebase-Artikel zur Installation](#).

1. Klicken Sie auf die heruntergeladene Datei, um das Installationsprogramm für ESET Endpoint Security for macOS zu starten.



1. Klicken Sie auf **ESET Endpoint Security for macOS installieren**, um die Installation zu starten.

Installieren mit der .pkg-Datei

! Bei der Installation und beim ersten Start Ihrer ESET-Produkte für macOS benötigt Ihr Mac Zugang zum Internet, um die Echtheit der ESET-Systemerweiterungen bei Apple zu verifizieren.

2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Zulassen**, um festzustellen, ob die Software installiert werden kann.

3. Entfernen Sie vorhandene Sicherheitsanwendungen wie Virenschutz, Anti-Spyware oder Firewall von Ihrem Computer, falls noch nicht geschehen. Klicken Sie auf **Weiter**, falls keine anderen Sicherheitsanwendungen installiert sind.

4. Überprüfen Sie die Systemanforderungen und klicken Sie auf **Weiter**.

5. Lesen Sie die ESET-Softwarelizenzvereinbarung und klicken Sie auf **Weiter** → **Zustimmen**, falls Sie zustimmen.

6. Wählen Sie den gewünschten Installationstyp aus.

- [Standardinstallation](#)
- [Benutzerdefinierte Installation](#)
- [Remoteinstallation](#)

Versions-Upgrade

i Zu Beginn der Installation prüft das Installationsprogramm automatisch online auf die neueste Produktversion. Wird eine neuere Version gefunden, erhalten Sie die Möglichkeit, vor dem Fortsetzen der Installation die neueste Version herunterzuladen.

Standardinstallation

Die Standardinstallation verwendet eine passende Konfiguration für die Anforderungen der meisten Benutzer. Diese Einstellungen bieten optimale Sicherheit und schonen gleichzeitig die Systemressourcen. Verwenden Sie daher die Standardinstallation, wenn Sie keine speziellen Anforderungen an die Konfiguration haben.

1. Wählen Sie im Fenster **ESET LiveGrid** die gewünschte Option aus und klicken Sie auf **Weiter**. Wenn Sie diese Einstellung später ändern möchten, können Sie dazu das **LiveGrid-Setup** verwenden. Weitere Informationen zu ESET Live Grid finden Sie [in unserem Glossar](#).
2. Wählen Sie im Fenster **Potenziell unerwünschte Anwendungen** die gewünschte Option aus (siehe [Was ist eine potenziell unerwünschte Anwendung?](#)) und klicken Sie auf **Weiter**. Sie können diese Einstellung später in den **erweiterten Einstellungen** ändern.
3. Klicken Sie auf **Installieren**. Falls Sie dazu aufgefordert werden, geben Sie Ihr macOS-Passwort ein und klicken Sie auf **Software installieren**.

Nach der Installation von ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. [Systemerweiterungen erlauben](#)
2. [Vollständigen Laufwerkszugriff erlauben](#).
3. Erlauben Sie ESET das Hinzufügen von Proxykonfigurationen. Sie erhalten die folgende Benachrichtigung: „ESET Endpoint Security for macOS“ **möchte Netzwerkinhalte filtern**. Wenn diese Benachrichtigung angezeigt wird, klicken Sie auf **Zulassen**. Wenn Sie auf **Nicht zulassen** klicken, können Sie den Web-Schutz nicht verwenden.



[macOS 10.15 und älter](#)

1. Auf macOS 10.13 und neueren Versionen erhalten Sie die Benachrichtigung **Systemerweiterung blockiert** von Ihrem System, und die Benachrichtigung **Ihr Computer ist nicht geschützt** von ESET Endpoint Security for macOS. Um den vollen Funktionsumfang von ESET Endpoint Security for macOS nutzen zu können, müssen Sie Kernelerweiterungen auf Ihrem Gerät erlauben. Um Kernelerweiterungen auf Ihrem Gerät zu erlauben, navigieren Sie zu **Systemeinstellungen > Sicherheit & Datenschutz** und klicken Sie auf **Zulassen**, um Systemsoftware vom Entwickler **ESET, spol. s.r.o.** zu erlauben. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).
2. Auf macOS 10.14 und höher wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Endpoint Security for macOS angezeigt. Um den vollen Funktionsumfang von ESET Endpoint Security for macOS nutzen zu können, müssen Sie ESET Endpoint Security for macOS **vollständigen Laufwerkszugriff** erlauben. Klicken Sie auf **Systemeinstellungen öffnen > Sicherheit & Datenschutz**. Öffnen Sie die Registerkarte **Datenschutz** und wählen Sie die Option **Vollständiger Laufwerkszugriff** aus. Klicken Sie auf das Schlosssymbol, um die Einstellungen bearbeiten zu können. Klicken Sie auf das Pluszeichen und wählen Sie die ESET Endpoint Security for macOS-Anwendung aus. Auf Ihrem Computer wird eine Benachrichtigung angezeigt, dass ein Neustart erforderlich ist. Klicken Sie auf **Später**. Starten Sie Ihren Computer zu diesem Zeitpunkt noch nicht neu. Klicken Sie im ESET Endpoint Security for macOS-Benachrichtigungsfenster auf **Erneut starten** oder starten Sie Ihren Computer neu. Weitere Informationen

finden Sie in unserem [Knowledgebase-Artikel](#).

Nach der Installation von ESET Endpoint Security for macOS sollten Sie Ihren Computer auf Schadcode scannen. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen** > **Smart-Scan**. Weitere Informationen zu On-Demand-Scans finden Sie im Abschnitt [On-Demand-Scan](#).

Benutzerdefinierte Installation

Die benutzerdefinierte Installation eignet sich für fortgeschrittene Benutzer, die während der Installation die erweiterten Einstellungen ändern möchten.

- **Programmkomponenten**

ESET Endpoint Security for macOS ermöglicht die Installation des Produkts ohne bestimmte Kernkomponenten (zum Beispiel ohne den Web- und E-Mail-Schutz). Deaktivieren Sie das Kontrollkästchen neben einer Produktkomponente, um sie aus der Installation zu entfernen.

- **Proxyserver**

Wenn Sie einen Proxyserver verwenden, wählen Sie **Ich nutze einen Proxyserver** aus, um die Parameter festzulegen. Geben Sie im nächsten Fenster unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Geben Sie dann im Feld **Port** den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver eine Authentifizierung erforderlich ist, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden** aus. Wenn Sie unsicher sind, ob Sie einen Proxyserver verwenden, können Sie Ihre aktuellen Systemeinstellungen verwenden, indem Sie **Systemeinstellungen verwenden (empfohlen)** auswählen.

- **Berechtigungen**

Können Sie privilegierte Benutzer oder Gruppen definieren, die berechtigt sind, die Programmeinstellungen zu ändern. Wählen Sie Benutzer in der Benutzerliste auf der linken Seite aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn Sie die Liste der privilegierten Benutzer leer lassen, gelten alle Benutzer als privilegiert.

- **ESET LiveGrid®**

Weitere Informationen zu ESET LiveGrid finden Sie [in unserem Glossar](#).

- **Evtl. unerwünschte Anwendungen**

Weitere Informationen zu potenziell unerwünschten Anwendungen finden Sie [in unserem Glossar](#).

- **Firewall-**

Wählen Sie einen Filtermodus für die Firewall aus. Weitere Informationen finden Sie unter [Filtermodi](#).

Nach der Installation von ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. [Systemerweiterungen erlauben](#)
2. [Vollständigen Laufwerkszugriff erlauben.](#)
3. Erlauben Sie ESET das Hinzufügen von Proxykonfigurationen. Sie erhalten die folgende Benachrichtigung: „ESET Endpoint Security for macOS“ **möchte Netzwerkinhalte filtern**. Wenn diese Benachrichtigung angezeigt wird, klicken Sie auf **Zulassen**. Wenn Sie auf **Nicht zulassen** klicken, können Sie den Web-Schutz nicht verwenden.



[macOS 10.15 und älter](#)

1. Auf macOS 10.13 und höher und neueren Versionen erhalten Sie die Benachrichtigung **Systemerweiterung blockiert** von Ihrem System, und die Benachrichtigung **Ihr Computer ist nicht geschützt** von ESET Endpoint Security for macOS. Um den vollen Funktionsumfang von ESET Endpoint Security for macOS nutzen zu können, müssen Sie Kernelerweiterungen auf Ihrem Gerät erlauben. Um Kernelerweiterungen auf Ihrem Gerät zu erlauben, navigieren Sie zu **Systemeinstellungen > Sicherheit & Datenschutz** und klicken Sie auf **Zulassen**, um Systemsoftware vom Entwickler **ESET, spol. s.r.o.** zu erlauben. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).
2. Auf macOS 10.14 und höher wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Endpoint Security for macOS angezeigt. Um den vollen Funktionsumfang von ESET Endpoint Security for macOS nutzen zu können, müssen Sie ESET Endpoint Security for macOS **vollständigen Laufwerkszugriff** erlauben. Klicken Sie auf **Systemeinstellungen öffnen > Sicherheit & Datenschutz**. Öffnen Sie die Registerkarte **Datenschutz** und wählen Sie die Option **Vollständiger Laufwerkszugriff** aus. Klicken Sie auf das Schlosssymbol, um die Einstellungen bearbeiten zu können. Klicken Sie auf das Pluszeichen und wählen Sie die ESET Endpoint Security for macOS-Anwendung aus. Auf Ihrem Computer wird eine Benachrichtigung angezeigt, dass ein Neustart erforderlich ist. Klicken Sie auf **Später**. Starten Sie Ihren Computer zu diesem Zeitpunkt noch nicht neu. Klicken Sie im ESET Endpoint Security for macOS-Benachrichtigungsfenster auf **Erneut starten** oder starten Sie Ihren Computer neu. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

Nach der Installation von ESET Endpoint Security for macOS sollten Sie Ihren Computer auf Schadcode scannen. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen > Smart-Scan**. Weitere Informationen zu On-Demand-Scans finden Sie im Abschnitt [On-Demand-Scan](#).

Systemerweiterungen lokal erlauben

In macOS 11 (Big Sur) wurden Kernelerweiterungen durch Systemerweiterungen ersetzt. Diese Erweiterungen müssen vom Benutzer zugelassen werden, um neue Systemerweiterungen von Drittanbietern laden zu können.

Nach der Installation von ESET Endpoint Security for macOS auf macOS Big Sur (11) und neueren Versionen erhalten Sie die Benachrichtigung „Systemerweiterung blockiert“ von Ihrem System, und die Benachrichtigung „Ihr Computer ist nicht geschützt“ von ESET Endpoint Security for macOS. Um den vollen Funktionsumfang von ESET Endpoint Security for macOS nutzen zu können, müssen Sie Systemerweiterungen auf Ihrem Gerät erlauben.

Upgrade von älteren macOS-Versionen auf Big Sur.

 Falls Sie ESET Endpoint Security for macOS bereits installiert haben und auf macOS Big Sur umsteigen möchten, müssen Sie die ESET-Kernelerweiterungen nach dem Upgrade manuell zulassen. Dazu ist physischer Zugriff auf den Clientcomputer erforderlich. Die Schaltfläche „Zulassen“ ist bei Remotezugriffen deaktiviert.

Wenn Sie das ESET-Produkt auf macOS Big Sur oder neuer installieren, müssen Sie die ESET-Systemerweiterungen manuell zulassen. Dazu ist physischer Zugriff auf den Clientcomputer erforderlich. Die Schaltfläche „Aktivieren“ ist bei Remotezugriffen deaktiviert.

Systemerweiterungen manuell zulassen

1. Klicken Sie auf **Systemeinstellungen öffnen** oder auf **Sicherheitseinstellungen öffnen** in einem der Dialogfenster.
2. Klicken Sie unten links auf das Schlosssymbol, um Änderungen im Einstellungsfenster zu erlauben.
3. Verwenden Sie Ihre Touch ID oder klicken Sie auf **Passwort verwenden** und geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie dann auf **Entsperren**.
4. Klicken Sie auf **Details**.
5. Wählen Sie alle drei ESET Endpoint Security for macOS.**app**-Optionen aus.
6. Klicken Sie auf **OK**.

Eine ausführliche Anleitung finden Sie in [unserem Knowledgebase Artikel](#) (Knowledgebase-Artikel sind nicht in allen Sprachen verfügbar).

Vollständigen Laufwerkszugriff lokal erlauben

Auf macOS 10.14 wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Endpoint Security for macOS angezeigt. Um alle Funktionen von ESET Endpoint Security for macOS nutzen zu können, müssen Sie ESET Endpoint Security for macOS **vollständigen Laufwerkszugriff erlauben**.

1. Klicken Sie im Dialogfenster mit der Warnung auf **Systemeinstellungen öffnen**.
2. Klicken Sie unten links auf das Schlosssymbol, um Änderungen im Einstellungsfenster zu erlauben.
3. Verwenden Sie Ihre Touch ID oder klicken Sie auf **Passwort verwenden** und geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie dann auf **Entsperren**.
4. Wählen Sie ESET Endpoint Security for macOS.**app** in der Liste aus.
5. Eine Benachrichtigung über den Neustart von ESET Endpoint Security for macOS wird angezeigt. Klicken Sie auf „Später“.
6. Wählen Sie den ESET **Echtzeit-Dateischutz** in der Liste aus.

ESET Echtzeit-Dateischutz nicht vorhanden

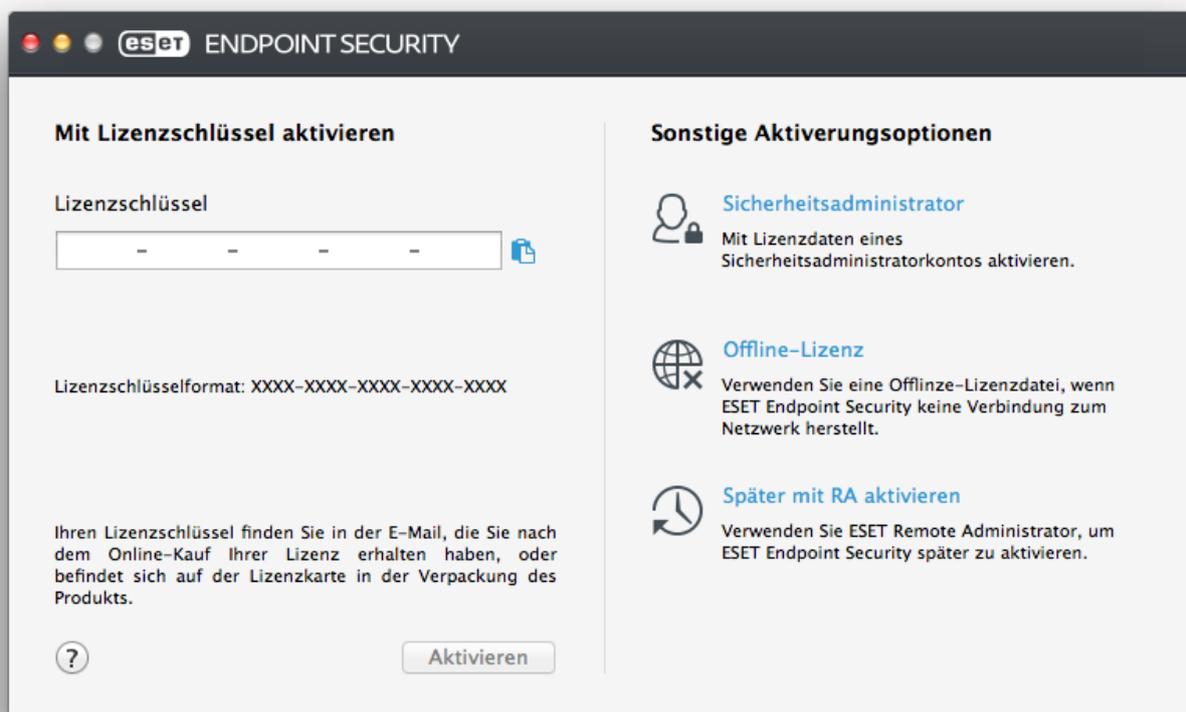
- ! Falls die Option **Echtzeit-Dateischutz** nicht in der Liste vorhanden ist, müssen Sie [Systemerweiterungen für Ihr ESET-Produkt erlauben](#).

7. Klicken Sie im ESET Endpoint Security for macOS-Dialogfenster auf „Neu starten“ oder starten Sie Ihren Computer neu. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren. Es stehen mehrere Aktivierungsmethoden zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmethode hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab.

Um Ihre Kopie von ESET Endpoint Security for macOS direkt in der Anwendung zu aktivieren, klicken Sie auf das ESET Endpoint Security for macOS-Symbol  in der macOS-Menüleiste (oben am Bildschirm) und dann auf **Produktaktivierung**. Sie können das Produkt auch im Hauptmenü unter **Hilfe > Lizenz verwalten** oder **Schutzstatus > Produkt aktivieren** aktivieren.



Sie können ESET Endpoint Security for macOS mit einer der folgenden Methoden aktivieren:

- **Mit Lizenzschlüssel aktivieren** – Der Lizenzschlüssel ist eine eindeutige Zeichenkette im Format XXXX-XXXX-XXXX-XXXX-XXXX und dient zur Identifizierung des Lizenzinhabers und zur Aktivierung der Lizenz. Sie finden den

Lizenzschlüssel in der E-Mail, die Sie nach dem Kauf erhalten haben, oder auf der Lizenzkarte, die in der Produktverpackung enthalten ist.

- **Security Admin** – Ein im [ESET License Administrator-Portal](#) erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.
- **Offline-Lizenz** – Eine automatisch erzeugte Datei, die zur Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Die Offline-Lizenzdatei wird im ESET License Administrator-Portal erzeugt und in Umgebungen verwendet, in denen sich die Anwendung nicht mit der Lizenzierungsstelle verbinden kann.

Sie können diesen Client auch später aktivieren, wenn Ihr Computer Mitglied eines verwalteten Netzwerks ist und Ihr Administrator die Aktivierung mit ESET Remote Administrator ausführen möchte.

Stille Aktivierung

- i** ESET Remote Administrator kann Clientcomputer mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

ESET Endpoint Security for macOS Version 6.3.85.0 (oder höher) können Sie das Produkt über die Befehlszeile aktivieren. Führen Sie dazu den folgenden Befehl aus:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Ersetzen Sie XXXX-XXXX-XXXX-XXXX-XXXX durch einen Lizenzschlüssel, der bereits für die Aktivierung von ESET Endpoint Security for macOS verwendet oder in [ESET License Administrator](#) registriert wurde. Der Befehl gibt entweder den Status „OK“ oder einen Fehler zurück, falls die Aktivierung fehlschlägt.

Deinstallation

Das Deinstallationsprogramm für ESET Endpoint Security for macOS kann auf mehrere Arten gestartet werden:

- Öffnen Sie die Installationsdatei für ESET Endpoint Security for macOS (.dmg) und doppelklicken Sie auf **Deinstallieren**.
- Öffnen Sie im **Finder** den Ordner **Programme** auf Ihrer Festplatte, halten Sie die Ctrl-Taste gedrückt, klicken Sie auf das Symbol von **ESET Endpoint Security for macOS** und wählen Sie Option **Paketinhalt zeigen**. Öffnen Sie den Ordner **Contents** > **Helpers** und doppelklicken Sie auf das Symbol **Uninstaller**.

Deinstallation

- !** Während der Deinstallation müssen Sie das Administratorpasswort mehrmals eingeben, um ESET Endpoint Security for macOS vollständig zu deinstallieren.

Übersicht

Das Hauptprogrammfenster von ESET Endpoint Security for macOS ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Das Hauptmenü bietet Zugriff auf folgende Bereiche:

- **Schutzstatus** – liefert Informationen zum Schutzstatus Ihres Computers sowie zur Firewall und zum Web- und E-Mail-Schutz.
- **Computer prüfen** – In diesem Bereich können Sie bei Bedarf eine [On-Demand-Prüfung](#) starten oder die entsprechenden Einstellungen ändern.
- **Update** – Enthält Informationen zu Modulupdates.
- **Einstellungen** – Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen.
- **Tools** – Zugriff auf [Log-Dateien](#), [Taskplaner](#), [Quarantäne](#), [Ausgeführte Prozesse](#) und andere Programmfunktionen.
- **Hilfe** – Zugriff auf die Hilfedateien, die Internet-Knowledgebase, Supportanfrageformulare und zusätzliche Informationen zum Programm.

Tastaturbefehle

Folgende Tastaturbefehle können in Verbindung mit ESET Endpoint Security for macOS verwendet werden:

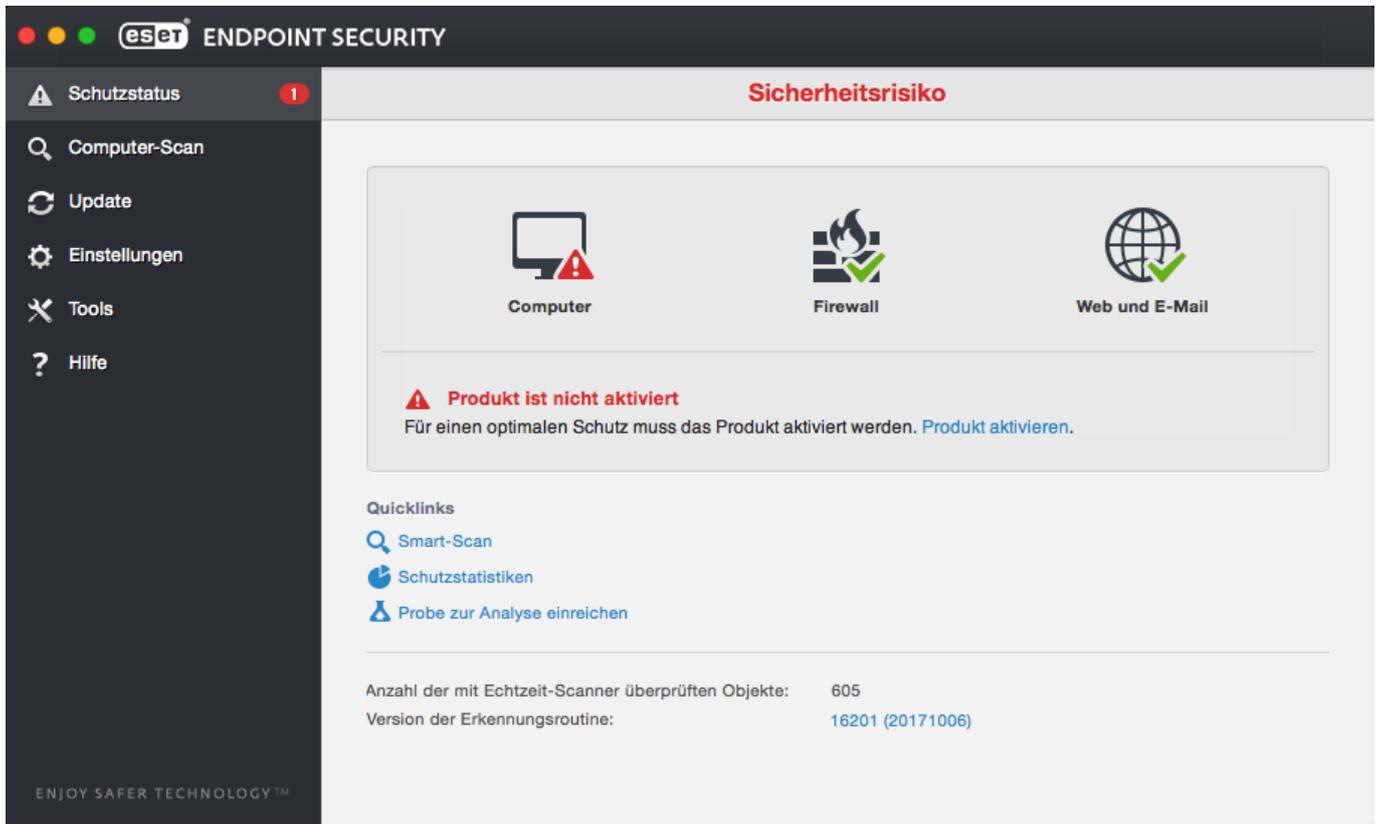
- *cmd+,* - zeigt ESET Endpoint Security for macOS-Einstellungen an,
- *cmd+O* - setzt das ESET Endpoint Security for macOS-Hauptprogrammfenster auf die Standardgröße zurück und positioniert es in der Bildschirmmitte.
- *cmd+Q* - blendet das ESET Endpoint Security for macOS-Hauptprogrammfenster aus. Um es erneut zu öffnen, klicken Sie auf das ESET Endpoint Security for macOS-Symbol  in der macOS-Menüleiste am oberen Bildschirmrand,
- *cmd+W* - schließt das ESET Endpoint Security for macOS-Hauptprogrammfenster.

Die folgenden Tastaturbefehle funktionieren nur, wenn die Option **Standardmenü verwenden** unter **Einstellungen > Erweiterte Einstellungen ... > Schnittstelle** aktiviert ist:

- *cmd+alt+L* - öffnet den Abschnitt **Log-Dateien**,
- *cmd+alt+S* - öffnet den Abschnitt **Taskplaner**,
- *cmd+alt+Q* - öffnet den Abschnitt **Quarantäne**.

Überprüfen der Funktionsfähigkeit des Systems

Um den Schutzstatus anzuzeigen, klicken Sie im Hauptmenü auf **Schutzstatus**. Im primären Fenster wird eine Darstellung des aktuellen Betriebszustands von ESET Endpoint Security for macOS angezeigt.



Vorgehensweise bei fehlerhafter Ausführung des Programms

Bei ordnungsgemäßer Funktion eines Moduls wird ein grünes Häkchen angezeigt. Wenn ein Modul nicht ordnungsgemäß funktioniert, wird ein rotes Ausrufezeichen oder ein oranges Benachrichtigungssymbol angezeigt. Zusätzlich werden in diesem Fall im Hauptprogrammfenster weitere Informationen zu dem Modul und ein Lösungsvorschlag angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf den blauen Link unter dem jeweiligen Hinweis.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, können Sie in der [ESET-Knowledgebase](#) nach einer Lösung suchen oder sich an den [ESET-Support](#) wenden. Der Support widmet sich umgehend Ihrem Anliegen, um schnell eine Lösung für Ihr Problem mit ESET Endpoint Security for macOS zu finden.

Computerschutz

Die Computerkonfiguration finden Sie unter **Einstellungen > Computer**. Sie zeigt den Status des **Echtzeit-Dateischatzes** an. Um die einzelnen Module zu deaktivieren, ändern Sie den Status des gewünschten Moduls in **DEAKTIVIERT**. Beachten Sie, dass dies die Schutzstufe des Computers herabsetzen kann. Um detaillierte Einstellungen für jedes Modul vorzunehmen, klicken Sie auf **Einstellungen**.

Viren- und Spyware-Schutz

Der Virenschutz bewahrt das System vor Attacken, indem er potenziell gefährliche Dateien verändert. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

Allgemein

Im Bereich **Allgemein (Einstellungen > Erweiterte Einstellungen... > Allgemein)** können Sie die Erkennung der folgenden Arten von Anwendungen aktivieren:

- **Eventuell unerwünschte Anwendungen** - Diese Anwendungen sind nicht unbedingt und absichtlich schädlich, können jedoch die Leistung Ihres Computers negativ beeinflussen. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Dazu zählen vor allem ungewollte Pop-up-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.
- **Potenziell unsichere Anwendungen** - In diese Kategorie fallen legitime Programme seriöser Hersteller, die jedoch von Angreifern ausgenutzt werden können, wenn sie ohne Wissen des Benutzers installiert werden. Da hierzu auch Programme für die Fernsteuerung von Computern gehören, ist diese Option standardmäßig deaktiviert.
- **Verdächtige Anwendungen** - Hierunter fallen Anwendungen, die mit sogenannten „Packer“- oder „Protector“-Programmen komprimiert wurden. Diese Art von Programmen wird oft von Malware-Autoren ausgenutzt, um einer Erkennung zu entgehen. Packer sind selbst-extrahierende Anwendungen, die zur Laufzeit mehrere Arten von Malware in ein einziges Paket verpacken. Die gängigsten Packer sind UPX, PE_Compact, PKLite und ASPack. Dieselbe Malware kann unter Umständen unterschiedlich erkannt werden, wenn für die Kompression ein anderer Packer verwendet wurde. Packer können außerdem die „Signaturen“ regelmäßig verändern, wodurch Malware schwieriger zu erkennen und zu entfernen ist.

Klicken Sie auf **Einstellungen**, um [Ausschlussfilter für Dateisystem bzw. Web- und E-Mail](#) einzurichten.

Ausschlussfilter

Im Bereich **Ausschlussfilter** können Sie festlegen, dass bestimmte Dateien/Ordner, Anwendungen oder IP/IPv6-Adressen von Scans ausgenommen werden.

Dateien und Ordner, die auf der Registerkarte **Dateisystem** aufgeführt sind, werden von allen Scans ausgeschlossen: Prüfung der Systemstartdateien, Echtzeit-Prüfung und On-Demand-Prüfung.

- **Pfad** – Pfad zu den auszuschließenden Dateien/Ordnern
- **Bedrohung** – Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Schadsoftware infiziert, erkennt der Virenschutz dies.

-  – Erstellen eines neuen Ausschlusses. Geben Sie den Pfad zum Objekt ein (Platzhalter * und ? werden unterstützt) oder wählen Sie den Ordner bzw. die Datei in der Baumstruktur aus.
-  – Entfernt ausgewählte Einträge.
- **Standard** – Setzt die Ausschlüsse auf den letzten gespeicherten Zustand zurück.

Auf der Registerkarte **Web und E-Mail** können Sie bestimmte **Anwendungen** oder **IP/IPv6-Adressen** von der Protokollprüfung ausschließen.

Systemstart-Schutz

Beim Scan der Systemstartdateien werden Dateien beim Systemstart automatisch untersucht. Diese Prüfung wird standardmäßig als geplanter Task nach der Anmeldung eines Benutzers oder nach einem erfolgreichen Update der Module ausgeführt. Klicken Sie auf **Einstellungen**, um die Einstellungen der ThreatSense-Engine für den Scan beim Systemstart zu ändern. Weitere Informationen zur Einrichtung der ThreatSense-Engine finden Sie in [diesem Abschnitt](#).

Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle Datenträger und löst beim Eintreten bestimmter Ereignisse einen Scan aus. Dank der ThreatSense-Technologie (siehe [ThreatSense-Einstellungen](#)) kann für neu erstellte Dateien ein anderer Echtzeit-Dateischutz als für bestehende Dateien eingesetzt werden. Neu erstellte Dateien können genauer kontrolliert werden.

Standardmäßig werden alle Dateien beim **Öffnen**, **Erstellen** und **Ausführen** geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit. Der Echtzeit-Dateischutz wird beim Systemstart geladen und fortlaufend ausgeführt. In besonderen Fällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Prüfprogramm) können Sie den Echtzeit-Dateischutz beenden, indem Sie auf das ESET Endpoint Security for macOS-Symbol  in der oberen Menüleiste klicken und die Option **Echtzeit-Dateischutz deaktivieren** auswählen. Der Echtzeit-Dateischutz lässt sich auch im Hauptfenster beenden. Klicken Sie dazu auf **Einstellungen > Computer** und setzen Sie die Option **Echtzeit-Dateischutz** auf **DEAKTIVIERT**.

Die folgenden Medientypen können von der Real-time-Prüfung ausgeschlossen werden:

- **Lokale Laufwerke** - Systemlaufwerke
- **Wechselmedien** - CDs/DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke

Sie sollten diese Einstellungen nur in Ausnahmefällen ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Um die erweiterten Einstellungen für den Echtzeit-Dateischutz zu ändern, wechseln Sie zu **Einstellungen > Erweiterte Einstellungen ...** (oder drücken Sie *cmd+*) > **Echtzeit-Dateischutz** und klicken Sie auf **Einstellungen...** neben **Erweiterte Optionen** (siehe Abschnitt [Erweiterte Optionen für Prüfungen](#)).

Erweiterte Einstellungen

In diesem Fenster können Sie die Objekttypen festlegen, die vom ThreatSense-Modul gescannt werden sollen. Weitere Informationen zu **selbstentpackenden Archiven**, **laufzeitkomprimierten Dateien** und **Advanced Heuristik** finden Sie unter [ThreatSense-Einstellungen](#).

Die Werte im Abschnitt **Standard-Archiveinstellungen** sollten nur geändert werden, um konkrete Probleme zu lösen, da höhere Archivverschachtelungswerte die Systemleistung beeinträchtigen können.

ThreatSense-Einstellungen für ausführbare Dateien - Standardmäßig wird bei der Dateiausführung keine **Advanced Heuristik** verwendet. Smart-Optimierung und ESET LiveGrid® sollten unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung zu minimieren.

Verbesserte Kompatibilität von Netzwerklaufwerken - Diese Option verbessert die Leistung beim Dateizugriff über das Netzwerk. Aktivieren Sie diese Option, wenn beim Zugriff auf Netzlaufwerke Geschwindigkeitsprobleme auftreten. Dieses Feature verwendet System File Coordinator unter OS X 10.10 und neueren Versionen. Achtung: Der File Coordinator wird nicht von allen Anwendungen unterstützt. Microsoft Word 2011 wird nicht unterstützt, Word 2016 dagegen schon.

Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Änderungen an den Parametern des Echtzeit-Dateischutzes sind mit Bedacht vorzunehmen. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu ändern. Dies kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder des Echtzeit-Scans eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von ESET Endpoint Security for macOS werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard** unten links im Fenster **Echtzeit-Dateischutz (Einstellungen > Erweiterte Einstellungen ... > Echtzeit-Schutz)**.

Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie die Testdatei [eicar.com](#). Diese Testdatei ist eine harmlose Datei, die von allen Virenschutzprogrammen erkannt wird. Die Datei wurde vom EICAR-Institut (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

Um den Status des Echtzeit-Dateischutzes ohne den ESET Security Management Center zu überprüfen, stellen Sie eine Remoteverbindung zum Clientcomputer über **Terminal** her und verwenden Sie den folgenden Befehl:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Der Status des Echtzeit-Scanners wird entweder als RTPStatus=Enabled oder als RTPStatus=Disabled angezeigt.

Die Ausgabe des Terminal-Bash enthält folgende Status:

- Die auf dem Clientcomputer installierte Version von ESET Endpoint Security for macOS
- Datum und Version der Erkennungsroutine
- Pfad zum Update-Server



Terminalnutzung

Die Terminal-Nutzung wird nur für fortgeschrittene Benutzer empfohlen.

Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz über das Hauptmenü zu reaktivieren, klicken Sie auf **Einstellungen > Computer** und setzen den **Echtzeit-Dateischutz** auf **AKTIVIERT**. Alternativ dazu können Sie den Echtzeit-Dateischutz im Fenster mit erweiterten Einstellungen unter **Echtzeit-Dateischutz** aktivieren. Wählen Sie dazu die Option **Echtzeit-Dateischutz aktivieren**.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

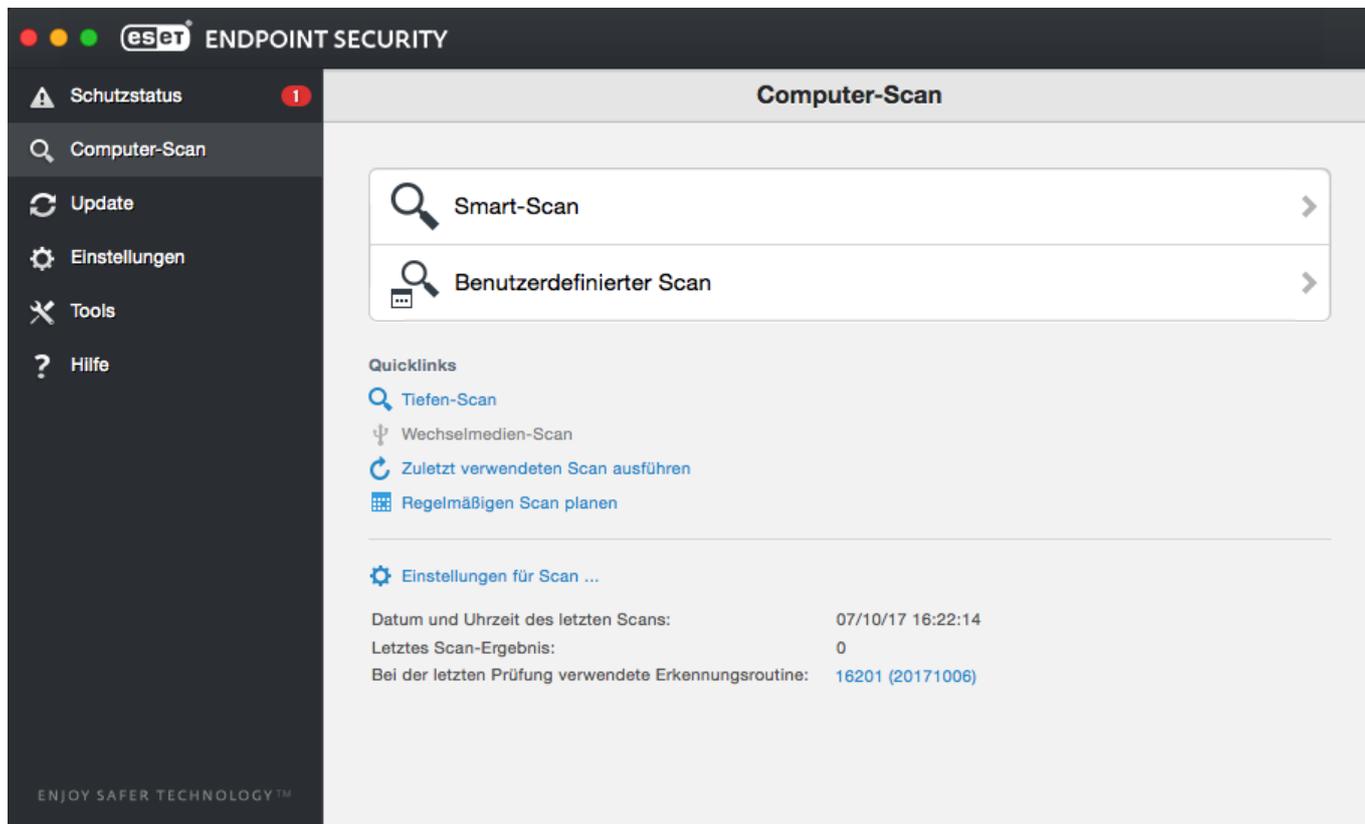
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz nicht automatisch beim Systemstart startet, können Konflikte mit anderen Programmen vorliegen. Wenden Sie sich in diesem Fall an den ESET-Support.

On-Demand-Prüfung

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), führen Sie ein **Smart-Scan** aus, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Um maximalen Schutz zu gewährleisten, sollten Sie solche Scans routinemäßig durchführen und nicht nur, wenn eine Infektion vermutet wird. Durch regelmäßige Scans kann eingedrungene Schadsoftware erkannt werden, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn die Echtzeitprüfung zum Zeitpunkt der Infektion deaktiviert war oder die Module nicht auf dem neuesten Stand sind.



Sie sollten mindestens einmal im Monat eine On-Demand-Prüfung vornehmen. Sie können die Scans als Task unter **Tools** > **Taskplaner** konfigurieren.

Sie können auch ausgewählte Dateien und Ordner von Ihrem Desktop oder aus dem **Finder**-Fenster durch Ziehen und Ablegen auf dem Hauptbildschirm, dem Dock-Symbol, dem Menüleistensymbol  (oberer Bildschirmrand) oder dem Anwendungssymbol (im Ordner */Programme*) von ESET Endpoint Security for macOS ablegen.

Prüfmethode

Es gibt zwei verschiedene Arten von On-Demand-Prüfungen. Beim **Smart-Scan** wird das System schnell gescannt, ohne dass Sie dafür weitere Scanparameter konfigurieren müssen. Bei der Methode **Benutzerdefinierter Scan** können Sie ein vordefiniertes Scanprofil und die zu scannenden Objekte auswählen.

Smart-Prüfung

Mit der Smart-Prüfung können Sie den Computer schnell überprüfen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Smart-Prüfung werden alle Dateien in allen Ordnern geprüft, und erkannte Infiltrationen werden automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter [Säubern](#).

Benutzerdefinierter Scan

Beim **Benutzerdefinierten Scan** können Sie verschiedene Scanparameter festlegen, z. B. die zu scannenden Objekte und die Scanmethoden. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können als benutzerdefinierte Scanprofile gespeichert

werden. Das ist sinnvoll, wenn Scans wiederholt mit denselben Parametern ausgeführt werden.

Zum Festlegen der zu scannenden Objekte wählen Sie **Computer scannen > Benutzerdefinierter Scan** und anschließend bestimmte **Zu scannende Objekte** aus der Baumstruktur aus. Sie können ein zu scannendes Objekt auch genauer bestimmen, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die gescannt werden sollen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion** aus. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen ... > Säubern**.

Benutzerdefinierter Scan

i Benutzerdefinierte Computerprüfungen sollten nur von fortgeschrittenen Benutzern ausgeführt werden, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

Zu prüfende Objekte

In der Baumstruktur der zu scannenden Objekte können Sie Dateien und Ordner auswählen, die auf Viren gescannt werden sollen. Je nach Profileinstellungen können Sie auch Ordner auswählen.

Sie können ein zu scannendes Objekt auch genauer definieren, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die gescannt werden sollen. Wählen Sie die zu scannenden Objekte in der Baumstruktur der verfügbaren Ordner auf dem Computer aus, indem Sie das Kontrollkästchen neben einer Datei bzw. einem Ordner aktivieren.

Prüfprofile

Ihre benutzerdefinierten Einstellungen können für zukünftige Scans gespeichert werden. Wir empfehlen Ihnen, für jeden regelmäßig durchgeführten Scan ein eigenes Profil zu erstellen (mit verschiedenen zu scannenden Objekten, Scanmethoden und anderen Parametern).

Zur Erstellung eines neuen Profils klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen...** (oder drücken *cmd+,*) > **Computer prüfen** und klicken auf **Bearbeiten...** neben der Liste der aktuell bestehenden Profile.



Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt [Einstellungen für ThreatSense](#). So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel

✓ Nehmen wir an, Sie möchten Ihr eigenes Scanprofil erstellen. Die Einstellungen des Smart-Scans eignen sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen scannen. Außerdem möchten Sie die Option „Immer versuchen, automatisch zu säubern“ anwenden. Geben Sie im Fenster **Profile für On-Demand-Prüfung** den Profilnamen ein, klicken Sie auf **Hinzufügen** und bestätigen Sie mit **OK**. Passen Sie dann die Einstellungen für **ThreatSense-Parameter** und **Zu prüfende Objekte** an Ihre Anforderungen an.

Wenn Sie das Betriebssystem nach der On-Demand-Prüfung abschalten und den Computer herunterfahren möchten, aktivieren Sie die Option **Computer nach Prüfung herunterfahren**.

Einstellungen für ThreatSense

ThreatSense ist eine proprietäre Technologie von ESET und besteht aus einer Kombination hochentwickelter Bedrohungserkennungsmethoden. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Sie verwendet eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, usw.), um die Systemsicherheit deutlich zu verbessern. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. ThreatSense -Technologie ist auch in der Lage, Rootkits zu vermeiden.

In den Einstellungen für ThreatSense können Sie verschiedene Scanparameter festlegen:

- Dateitypen und -erweiterungen, die gescannt werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Zum Öffnen der Einstellungen klicken Sie auf **Einstellungen > Erweiterte Einstellungen ...** (oder drücken Sie *cmd+*), und klicken anschließend auf die Schaltfläche **Einstellungen** für das ThreatSense-Prüfmodul im Bereich **Systemstart-Schutz**, **Echtzeit-Schutz** bzw. **Computer prüfen**, die allesamt die ThreatSense-Technologie verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Berücksichtigen Sie dies bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule:

- **Systemstart-Schutz** - Automatische Prüfung der Systemstartdateien
- **Echtzeit-Dateischutz** - Echtzeit-Dateischutz
- **Computer prüfen** - On-Demand-Prüfung
- **Web-Schutz**
- **E-Mail-Schutz**

Die ThreatSense-Einstellungen sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet. Es wird daher empfohlen, die ThreatSense-Standard-einstellungen für alle Module unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien auf Infiltrationen gescannt werden sollen.

- **Symbolische Links** - (Nur beim Computerscan) Scan von Dateien, die eine Textfolge enthalten, die vom Betriebssystem als Pfad zu einer anderen Datei oder einem anderen Verzeichnis interpretiert wird.
- **E-Mail-Dateien** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von E-Mail-Dateien.
- **Postfächer** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Benutzerpostfächern im System. Die unsachgemäße Anwendung dieser Option kann zu Konflikten mit Ihrem E-Mail-Programm führen. Für weitere Informationen über Vor- und Nachteile dieser Option lesen Sie den folgenden [Knowledgebase-Artikel](#).
- **Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung komprimierter Archivdateien (.rar, .zip, .arj, .tar usw.).
- **Selbstentpackende Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien in selbstentpackenden Archiven.
- **Laufzeitkomprimierte Dateien** - Laufzeitkomprimierte Dateien werden (anders als Standard-Archivtypen) im Arbeitsspeicher dekomprimiert. Wenn diese Option ausgewählt ist, werden statisch laufzeitkomprimierte Dateien (UPX, yoda, ASPack, FGS etc.) ebenfalls geprüft.

Optionen

Im Bereich **Optionen** können Sie die Methoden festlegen, die bei einer Prüfung des Systems auf Infiltrationen angewendet werden sollen. Folgende Optionen stehen zur Verfügung:

- **Heuristik** – Heuristische Methoden verwenden einen Algorithmus, der (böartige) Aktivitäten von Programmen analysiert. Hauptvorteil der heuristischen Erkennung ist die Fähigkeit, neue Schadsoftware erkennen zu können, die zuvor noch nicht vorhanden war.
- **Advanced Heuristik** – Als Advanced Heuristik werden besondere, von ESET entwickelte heuristische Verfahren bezeichnet, die für die Erkennung von Würmern und Trojanern optimiert sind, die in höheren Programmiersprachen geschrieben wurden. Die Erkennungsrate des Programms ist dadurch wesentlich gestiegen.

Säubern

In den Säuberungseinstellungen wird festgelegt, wie der Scanner die infizierten Dateien säubert. Es gibt 3 Arten der Schadcodeentfernung:

- **Nicht säubern** – Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und Sie werden aufgefordert, eine Aktion auszuwählen.
- **Standardmodus** – Das Programm versucht, den Schadcode aus der Datei zu entfernen oder die infizierte Datei zu löschen. Wenn es nicht möglich ist, die passende Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.
- **Automatisch säubern** – Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien (einschließlich Archive). Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, erhalten Sie eine Benachrichtigung und werden aufgefordert, die auszuführende Aktion auszuwählen.

Standardmodus – Säubern von Archiven

 Im Standardmodus „Normales Säubern“ werden ganze Archive nur gelöscht, wenn sie ausschließlich infizierte Dateien enthalten. Wenn ein Archiv saubere und infizierte Dateien enthält, wird es nicht gelöscht. Im Modus „Automatisch säubern“ wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.

Ausschlussfilter

Die Erweiterung ist der Teil eines Dateinamens nach dem Punkt. Die Erweiterung definiert Typ und Inhalt der Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die nicht geprüft werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung gescannt. Jede Erweiterung kann der Liste auszuschließender Dateien hinzugefügt werden. Über die Schaltflächen + und - können Sie festlegen, welche Erweiterungen gescannt werden sollen.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt. So empfiehlt es sich beispielsweise, Dateien vom Typ *log*, *cfg* und *tmp* auszuschließen. Das korrekte Format für die Angabe von Dateierweiterungen ist:

log

cfg

tmp

Grenzen

Im Bereich **Grenzen** können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die gescannt werden sollen:

- **Maximale Größe:** Definiert die maximale Größe der zu prüfenden Objekte. Der Virenschutz scannt dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Der Standardwert sollte nicht geändert werden; für gewöhnlich besteht dazu auch kein Grund. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte vom Scan auszuschließen.
- **Maximale Scanzeit:** Definiert die maximale Dauer, die für das Scannen eines Objekts zur Verfügung steht.

Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz das Scannen eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob der Scan abgeschlossen ist oder nicht.

- **Maximale Verschachtelungstiefe:** Legt die maximale Tiefe der Archivprüfung fest. Der Standardwert 10 sollte nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund. Wenn die Prüfung aufgrund der Anzahl verschachtelter Archive vorzeitig beendet wird, bleibt das Archiv ungeprüft.
- **Maximale Dateigröße:** Mit dieser Option können Sie die maximale Dateigröße für Dateien in Archiven (nach der Extraktion) angeben, die geprüft werden sollen. Wenn der Scan aufgrund dieses Grenzwerts vorzeitig beendet wird, bleibt das Archiv ungeprüft.

Weitere

Smart-Optimierung aktivieren

Die Smart-Optimierung passt die Einstellungen so an, dass eine wirksame Prüfung bei gleichzeitig hoher Prüfgeschwindigkeit gewährleistet ist. Die verschiedenen Schutzmodule prüfen auf intelligente Weise unter Einsatz verschiedener Prüfmethoden. Die Smart-Optimierung ist innerhalb des Produkts nicht starr definiert. Das ESET-Entwicklungsteam fügt ständig neue Ergänzungen hinzu, die dann über die regelmäßigen Updates in Ihr ESET Endpoint Security for macOS integriert werden. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern des entsprechenden Moduls für die Prüfung verwendet.

Alternativen Datenstrom prüfen (nur On-Demand-Prüfung)

Bei den von Dateisystemen verwendeten alternativen Datenströmen (Ressourcen-/Daten-Forks) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Scantechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Infektionswege sind Webseiten, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs usw.).

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie auf **Computer prüfen**.
2. Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt [Smart-Prüfung](#)).
3. Nachdem der Scan abgeschlossen ist, überprüfen Sie im Log die Anzahl der gescannten, infizierten und gesäuberten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte scannen möchten, wählen Sie **Benutzerdefinierter Scan** und anschließend die Bereiche, die auf Viren gescannt werden sollen.

Das folgende allgemeine Beispiel zeigt, wie ESET Endpoint Security for macOS mit Schadsoftware umgeht. Angenommen, der Echtzeit-Dateischutz verwendet die Standard-Säuberungsstufe und erkennt eine

eingedrungene Schadsoftware. Der Echtzeit-Dateischutz wird versuchen, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeitschutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnfenster zur Auswahl einer Option aufgefordert. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Es wird nicht empfohlen, die Option **Keine Aktion** zu wählen, da sonst die infizierte(n) Datei(en) nicht behandelt werden. Wählen Sie diese Option nur, wenn Sie sich sicher sind, dass die Datei harmlos ist und versehentlich erkannt wurde.

Säubern und löschen

Wählen Sie „Säubern“, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Dateien in Archiven löschen

Im Standardmodus der Aktion „Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option **Immer versuchen, automatisch zu säubern** sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der übrigen Archivdateien.

Web- und E-Mail-Schutz

Klicken Sie im Hauptmenü auf **Einstellungen > Web und E-Mail**, um auf den Web- und E-Mail-Schutz zuzugreifen. Sie können von dort aus auch auf ausführliche Einstellungen für die einzelnen Module zugreifen, indem Sie auf **Einstellungen** klicken.

Scan-Ausnahmen



ESET Endpoint Security for macOS führt keine Scans der verschlüsselten Protokolle HTTPS, POP3S und IMAPS durch.

- **Web-Schutz** – Der Web-Schutz überwacht die HTTP-Kommunikation zwischen Webbrowsern und Remoteservern.
- **E-Mail-Client-Schutz** – Überwacht eingehende E-Mails, die mit dem POP3- und dem IMAP-Protokoll übertragen werden.
- **Phishing-Schutz** – Blockiert potenzielle Phishing-Angriffe von Websites oder Domänen.
- **Web-Kontrolle** - Sperrt Webseiten, die möglicherweise unerlaubte oder ungeeignete Inhalte enthalten.

Web-Schutz

Der Web-Schutz dient zur Überwachung von Verbindungen zwischen Webbrowsern und Remote-Servern auf die Einhaltung der Regeln des HTTP-Protokolls (Hypertext Transfer Protocol).

Sie können die Webfilterung aktivieren, indem Sie [Portnummern für die HTTP-Kommunikation](#) und/oder [URL-Adressen](#) definieren.

Ports

Auf der Registerkarte **Ports** können Sie die für HTTP-Verbindungen verwendeten Portnummern definieren. In der Standardeinstellung sind die Portnummern 80, 8080 und 3128 vorgegeben.

URL-Listen

Im Bereich **URL-Listen** können Sie HTTP-Adressen angeben, die gesperrt, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Auf Websites in der Liste der gesperrten Adressen kann nicht zugegriffen werden. Auf Websites in der Liste der ausgeschlossenen Adressen kann zugegriffen werden, ohne dass diese auf Schadcode gescannt werden.

Um nur den Zugriff auf die in der Liste **Zugelassene URLs** enthaltenen URLs zu erlauben, wählen Sie **URL-Zugriff einschränken** aus.

Um eine Liste zu aktivieren, wählen Sie neben dem Listennamen die Option **Aktiviert** aus. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der gegenwärtigen Liste eingeben, wählen Sie **Hinweis anzeigen** aus.

Die Sonderzeichen ***** (Sternchen) und **?** (Fragezeichen) können beim Erstellen von URL-Listen als Platzhalter verwendet werden. Das Sternchen steht für eine beliebige Zeichenfolge, das Fragezeichen für ein beliebiges Zeichen. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie außerdem darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden.

E-Mail-Schutz

Der E-Mail-Schutz überwacht eingehende E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden. Für die eingehenden Nachrichten verwendet ESET Endpoint Security for macOS alle erweiterten ThreatSense-Scanmethoden. Der POP3- und IMAP-Datenverkehr wird unabhängig vom verwendeten E-Mail-Programm gescannt.

ThreatSense-Prüfmodul: Einstellungen – In den erweiterten Prüfeinstellungen können Sie die zu prüfenden Objekte, die Erkennungsmethoden usw. konfigurieren. Klicken Sie auf **Einstellungen**, um die ausführlichen Prüfeinstellungen anzuzeigen.

Scanhinweise am Ende der E-Mail hinzufügen – An jede gescannte E-Mail wird ein Hinweis mit den Scanergebnissen angehängt. Auf diese Hinweise sollte sich der Empfänger jedoch nicht exklusiv verlassen, da sie bei problematischen HTML-Nachrichten eventuell verloren gehen oder auch von Viren gefälscht werden können. Folgende Optionen stehen zur Verfügung:

- **Nie** – Es werden keine Scanhinweise hinzugefügt.
- **Nur bei infizierten E-Mails** – Nur Nachrichten mit Schadsoftware werden als gescannt gekennzeichnet.

- **Bei allen gescannten E-Mails** – ESET Endpoint Security for macOS versieht alle gescannten E-Mails mit Scanhinweisen.

Prüfhinweis an den Betreff empfangener und gelesener infizierter E-Mails anhängen – Aktivieren Sie dieses Kontrollkästchen, um infizierte E-Mails zu kennzeichnen. Auf diese Weise können infizierte Nachrichten leicht gefiltert werden. Die Warnung erhöht außerdem die Glaubwürdigkeit beim Empfänger und bietet beim Erkennen einer Infiltration wertvolle Informationen zur Gefährdung durch eine bestimmte E-Mail oder einen Absender.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird – Hier können Sie das Betreffpräfix für infizierte E-Mails bearbeiten.

- %avstatus% – Fügt den Infektionsstatus der E-Mail hinzu („nicht infiziert“, „infiziert“ usw.)
- %virus% – Fügt den Namen der Bedrohung hinzu
- %product% – Fügt den Namen Ihres ESET-Produkts hinzu (in diesem Fall „ESET Endpoint Security for macOS“)
- %product_url% – Fügt einen Link zur ESET-Website hinzu (www.eset.com)

Im unteren Bereich dieses Fensters können Sie das Scannen von E-Mails aktivieren/deaktivieren, die über die POP3- und IMAP-Protokolle empfangen wurden. Weitere Informationen finden Sie in den folgenden Artikeln:

- [Scannen des POP3-Protokolls](#)
- [Scannen des IMAP-Protokolls](#)

Prüfen von E-Mails per POP3-Protokoll

Das POP3-Protokoll ist das am weitesten verbreitete Protokoll für den Empfang von E-Mails mit einer E-Mail-Client-Anwendung. ESET Endpoint Security for macOS bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass das Modul aktiviert ist, damit der Protokollfilter richtig funktioniert. Die Prüfung des POP3-Protokolls wird automatisch ausgeführt, ohne dass Sie den E-Mail-Client neu konfigurieren müssen. Standardmäßig wird der gesamte Datenverkehr über Port 110 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn **Prüfen von E-Mails per POP3-Protokoll aktivieren** aktiviert ist, wird der gesamte über das POP3-Protokoll empfangene Verkehr auf Schadssoftware überwacht.

Prüfen des IMAP-Protokolls

Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den Abruf von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig beim selben

Postfach anmelden und Statusinformationen zu den Nachrichten pflegen, z. B. ob die Nachricht gelesen, beantwortet oder gelöscht wurde. ESET Endpoint Security for macOS schützt dieses Protokoll unabhängig vom eingesetzten E-Mail-Programm.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass die Prüfung des IMAP-Protokolls aktiviert ist, damit das Modul richtig funktioniert. Die Prüfung des IMAP-Protokolls wird automatisch ausgeführt, ohne dass Sie den E-Mail-Client neu konfigurieren müssen. Standardmäßig wird der gesamte Datenverkehr über Port 143 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn **Prüfen von E-Mails per IMAP-Protokoll aktivieren** aktiviert ist, wird der gesamte über das IMAP-Protokoll empfangene Verkehr auf Schadsoftware überwacht.

Phishing-Schutz

Der Begriff Phishing bezeichnet eine kriminelle Vorgehensweise, die sich Social Engineering-Techniken (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Informationen wie Bankkontonummern, Kreditkartendaten, PIN-Nummer oder Benutzernamen und Passwörter zu erlangen.

Wir empfehlen, den Phishing-Schutz aktiviert zu lassen (**Einstellungen > Erweiterte Einstellungen > Phishing-Schutz**). Alle potenziellen Phishing-Angriffe von gefährlichen Webseiten oder Domänen werden blockiert, und Sie erhalten einen Warnhinweis über den Angriffsversuch.

Firewall

Die Firewall steuert den gesamten ein- und ausgehenden Netzwerkverkehr des Systems, indem sie einzelne Netzwerkverbindungen nach den festgelegten Filterregeln zulässt oder verweigert. So bietet die Firewall Schutz gegen Angriffe von Remotecomputern und ermöglicht das Blockieren bestimmter Dienste. Darüber hinaus bietet sie einen Virenschutz für die Protokolle HTTP, POP3 und IMAP.

Scan-Ausnahmen



ESET Endpoint Security for macOS führt keine Scans der verschlüsselten Protokolle HTTPS, POP3S und IMAPS durch.

Sie finden die Konfiguration für die Firewall unter **Einstellungen > Firewall**. Dort können Sie den Filtermodus auswählen, Regeln festlegen und weitere Einstellungen vornehmen. Außerdem können Sie auf genauere Einstellungen des Programms zugreifen.

Wenn Sie die Option **Alle Netzwerkverbindungen blockieren: Netzwerk trennen** aktivieren, werden alle ein- und ausgehenden Verbindungen von der Firewall blockiert. Verwenden Sie diese Option nur, wenn Sie schwerwiegende Sicherheitsrisiken befürchten, die eine Trennung der Netzwerkverbindung erfordern.

Filtermodi

Für die ESET Endpoint Security for macOS Firewall stehen drei Filtermodi zur Auswahl. Die Einstellungen für die Filtermodi finden Sie unter **Einstellungen > Erweiterte Einstellungen > Firewall**. Das Verhalten der Firewall

ändert sich je nach gewähltem Modus. Der Filtermodus bestimmt auch, wie stark der Anwender eingreifen muss.

Alle Verbindungen blockiert – Sämtliche ein- und ausgehenden Verbindungen werden blockiert.

Automatisch mit Ausnahmen – Dies ist der Standardmodus. Dieser Modus eignet sich für Anwender, die eine möglichst einfache und praktische Nutzung der Firewall wünschen, bei der keine Regeln erstellt werden müssen. Im Automatikmodus ist der ausgehende Standarddatenverkehr für das System zugelassen und nicht initiierte Verbindungen aus dem Netzwerk werden blockiert. Sie haben auch die Möglichkeit, benutzerdefinierte Regeln hinzuzufügen.

Interaktiv – Mit diesem Modus können Sie eine benutzerdefinierte Konfiguration für Ihre Firewall erstellen. Wenn eine Verbindung erkannt wird und keine Regel dafür existiert oder gilt, wird in einem Dialogfenster eine unbekannte Verbindung gemeldet. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll, und diese Auswahl kann als neue Regel für die Firewall übernommen werden. Wenn eine neue Regel erstellt wurde, werden Verbindungen dieser Art beim nächsten Verbindungsversuch entsprechend der Regel automatisch zugelassen oder blockiert.



Um genaue Informationen zu allen blockierten Verbindungen in einer Log-Datei zu speichern, aktivieren Sie die Option **Alle blockierten Verbindungen in Log aufnehmen**. Um die Log-Dateien der Firewall zu prüfen, klicken Sie im Hauptmenü auf **Tools > Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log**.

Firewall-Regeln

Regeln fassen verschiedene Bedingungen zusammen, mit denen alle Netzwerkverbindungen getestet werden, und die Aktionen, die diesen Bedingungen zugewiesen sind. Über die Regeln der Firewall können Sie festlegen, welche Aktion ausgeführt werden soll, wenn eine Verbindung aufgebaut wird, für die eine Regel existiert.

Eingehende Verbindungen stammen von Remotecomputern, die versuchen, eine Verbindung mit dem lokalen System aufzubauen. Ausgehende Verbindungen funktionieren umgekehrt – das lokale System nimmt Kontakt mit einem Remotecomputer auf.

Wenn eine neue unbekannte Verbindung erkannt wird, sollten Sie sich gut überlegen, ob Sie sie zulassen oder blockieren. Ungebetene, unsichere oder unbekannte Verbindungen stellen ein Sicherheitsrisiko für das System dar. Wenn eine solche Verbindung aufgebaut wurde, empfehlen wir Ihnen, genau auf den Remotecomputer und die Anwendung, die versucht, auf Ihren Computer zuzugreifen, zu achten. Viele Infiltrationen versuchen, an private Daten zu gelangen, solche Daten zu senden oder weitere Schadprogramme auf den Computer herunterzuladen. Mit der Firewall können Sie solche Verbindungen erkennen und beenden.

Von Apple signierte Software darf automatisch auf das Netzwerk zugreifen - Standardmäßig können die von Apple signierten Anwendungen automatisch auf das Netzwerk zugreifen. Anwendungen müssen mit einem von Apple ausgestellten Zertifikat signiert sein, um mit Apple-Diensten interagieren oder auf Geräten installiert werden zu können. Deaktivieren Sie diese Option, falls dies nicht gewünscht ist. Nicht mit einem Apple-Zertifikat signierte Anwendungen können nur mit einer Benutzeraktion oder einer Regel auf das Netzwerk zugreifen.

Wenn diese Option deaktiviert ist, muss sämtliche Netzwerkkommunikation mit von Apple signierten Diensten vom Benutzer genehmigt werden, falls keine entsprechende Firewall-Regel existiert.

Änderungen aus den Vorgängerversionen: In ESET Endpoint Security for macOS 6.8 und älteren Versionen wurde die eingehende Kommunikation an Dienste mit Apple-Zertifikat blockiert. In der aktuellen Version identifiziert ESET Endpoint Security for macOS den lokalen Empfänger der eingehenden Kommunikation, und die Kommunikation wird zugelassen, wenn diese Option aktiviert ist.

Erstellen neuer Regeln

Die Registerkarte **Regeln** enthält eine Liste aller Regeln, die auf den Datenverkehr der einzelnen Anwendungen angewendet werden. Regeln werden automatisch gemäß der Reaktion des Anwenders bei einer neuen Verbindung hinzugefügt.

1. Klicken Sie auf **Hinzufügen...**, um eine neue Regel zu erstellen. Geben Sie dann einen Namen für die Regel ein und fügen Sie das Anwendungssymbol durch Ziehen und Ablegen in das leere Feld ein oder klicken auf **Durchsuchen**, um die Anwendung im Ordner */Programme* zu suchen. Wenn Sie die Regel auf alle Anwendungen anwenden möchten, die auf Ihrem Computer installiert sind, wählen Sie **Alle Anwendungen** aus.
2. Wählen Sie im nächsten Fenster die gewünschte **Aktion** (Kommunikation zwischen ausgewählter Anwendung und Netzwerk zulassen oder blockieren) und die **Richtung** des Datenverkehrs (eingehend, ausgehend oder beides) aus. Wählen Sie **Regel in Log schreiben** aus, um die gesamte von dieser Regel betroffene Kommunikation aufzuzeichnen. Um die Firewall-Logs zu überprüfen, klicken Sie im ESET Endpoint Security for macOS-Hauptmenü auf **Tools > Logs** und wählen Sie die Option **Firewall** im Dropdownmenü **Log** aus.
3. Legen Sie im Bereich **Protokoll/Ports** das Protokoll und den Port fest, die die Anwendung für die Kommunikation verwendet (falls TCP oder UDP ausgewählt ist). Die Transportprotokoll-Ebene ermöglicht einen sicheren und effizienten Datentransfer.
4. Geben Sie zuletzt die **Zielkriterien** (IP-Adresse, Bereich, Subnetz, Ethernet oder Internet) für die Regel ein.

Firewall-Zonen

Eine Zone besteht aus einer Sammlung von Netzwerkadressen, die eine logische Gruppe ergeben. Jeder Adresse in einer Gruppe werden die gleichen Regeln zugewiesen, die zentral für die gesamte Gruppe erstellt werden.

Sie können solche Zonen erstellen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Geben Sie einen Namen im Feld **Name** und eine **Beschreibung** (optional) der Zone ein. Wählen Sie ein Profil aus, dem die Zone zugewiesen werden soll, und fügen Sie eine IPv4-/IPv6-Adresse, einen Adressbereich, ein Subnetz, ein WLAN-Netzwerk oder eine Schnittstelle hinzu.

Firewall-Profile

Unter **Profile** können Sie das Verhalten der ESET Endpoint Security for macOS-Firewall steuern. Sie können Firewall-Regeln bei der Erstellung oder Bearbeitung zu einem bestimmten Profil zuweisen. Wenn Sie ein Profil auswählen, werden nur die globalen Regeln (ohne ausgewähltes Profil) und die diesem Profil zugewiesenen Regeln angewendet. Sie können mehrere Profile mit unterschiedlichen Regeln erstellen, um das Verhalten der Firewall schnell und einfach zu ändern.

Firewall-Logs

Die ESET Endpoint Security for macOS Firewall speichert alle wichtigen Ereignisse in einer Log-Datei. Um die Log-Dateien der Firewall zu öffnen, klicken Sie im Hauptmenü auf **Tools > Logs** und wählen Sie die Option **Firewall** im Dropdown-Menü **Log** aus.

Die Log-Dateien sind ein wertvolles Instrument zum Erkennen von Fehlern und zum Aufdecken von versuchten Zugriffen auf das System. Die Log-Dateien der ESET Firewall enthalten folgende Daten:

- Datum und Uhrzeit des Ereignisses
- Name des Ereignisses
- Quelle
- Zielnetzwerkadresse
- Kommunikationsprotokoll
- Angewendete Regel
- Betroffene Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann zur Erkennung von Sicherheitsbedrohungen beitragen. Viele weitere Faktoren, die potenzielle Sicherheitsrisiken darstellen, können mit der Firewall kontrolliert werden: überdurchschnittlich häufige Verbindungen von unbekanntem Standorten, ungewöhnlich viele Verbindungsversuche, Verbindungen mit unbekanntem Anwendungen oder ungewöhnliche Portnummern.

Medienkontrolle

Mit ESET Endpoint Security for macOS können Sie Speichergeräte scannen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Speichergeräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass die Benutzer Geräte mit unerwünschten Inhalten verwenden.

Medienkontrolle auf macOS 11 und neuer

- ! Auf macOS 11 und neueren Betriebssystemen kann ESET Endpoint Security for macOS nur Speichergeräte (USB-Laufwerke, CD/DVD usw.) scannen.

Unterstützte externe Geräte auf macOS 10.15 und älteren Versionen:

- Datenträgerspeicher (Festplatten, USB-Speicher)
- CD/DVD
- USB-Drucker
- Bildverarbeitungsgerät
- Serieller Port
- Netzwerk
- Mobiles Gerät

Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Benachrichtigungsfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Im Log der Medienkontrolle werden alle Ereignisse aufgezeichnet, die die Medienkontrolle auslösen. Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Endpoint Security for macOS auf **Tools** > [Log-Dateien](#).

Regel-Editor

Die Einstellungen der Medienkontrolle können unter **Einstellungen** > **Erweiterte Einstellungen ...** > **Medienkontrolle** geändert werden.

Klicken Sie auf **Medienkontrolle aktivieren**, um die Medienkontrolle in ESET Endpoint Security for macOS zu aktivieren. Nach der Aktivierung der Medienkontrolle können Sie Regeln für die Medienkontrolle verwalten und bearbeiten. Über das Kontrollkästchen neben einem Regelnamen können Sie die entsprechende Regel aktivieren und deaktivieren.

Mit den Schaltflächen  und  können Sie Regeln hinzufügen und entfernen. Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Um die Reihenfolge zu ändern, bringen Sie die Regeln durch Ziehen und Ablegen in eine andere Position, oder klicken Sie

auf  und wählen Sie eine der Optionen aus.

ESET Endpoint Security for macOS erkennt automatisch alle aktuell eingelegten Geräte und deren Parameter (Gerätetyp, Hersteller, Modell, Seriennummer). Statt Regeln manuell zu erstellen, können Sie auch auf **Auffüllen** klicken, das Gerät auswählen und auf **Weiter** klicken, um die Regel zu erstellen.

Bestimmte Gerätetypen können je nach Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Geräteart, Logging-Schweregrad und auszuführende Aktion beim Anschließen eines Geräts an den Computer.

Name

Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über das Kontrollkästchen neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist hilfreich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Gerätetyp

Wählen Sie im Dropdown-Menü den gewünschten Typ des externen Geräts aus. Gerätetypinformationen werden über das Betriebssystem erfasst. Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer angeschlossen sind. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte stellen nur Informationen zu den eigenen Aktionen bereit, keine Benutzerinformationen. Daher können diese Geräte nur global blockiert werden.

Aktion

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

Lese-/Schreibzugriff – Der vollständige Zugriff auf das Gerät wird zugelassen.

Nur Lesezugriff – Nur Lesezugriff auf das Gerät wird zugelassen.

Sperren – Der Zugriff auf das Gerät wird gesperrt.

Kriterientyp

Wählen Sie **Gerätegruppe** oder **Gerät** aus. Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte.

Hersteller – Ermöglicht das Filtern der Liste nach Herstellername oder -ID.

Modell – Die Bezeichnung des Geräts.

Seriennummer – Externe Geräte haben meistens eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das CD/DVD-Laufwerk.

Keine Parameter definiert

i Wenn diese Parameter nicht definiert werden, ignoriert die Regel diese Felder bei der Abstimmung. Bei Filterparametern mit Textfeldern braucht die Groß-/Kleinschreibung nicht beachtet zu werden. Platzhalter (*, ?) werden nicht unterstützt.

TIPP

i Um Informationen zu einem Gerät anzuzeigen, können Sie eine Regel für die entsprechende Geräteart erstellen und das Gerät an den Computer anschließen. Nachdem das Gerät angeschlossen wurde, werden die Gerätedetails im [Medienkontroll-Log](#) angezeigt.

Logging-Schweregrad

Immer – Alle Ereignisse werden protokolliert.

Diagnose – Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.

Informationen – Zeichnet zusätzlich zu den oben genannten Einträgen informative Meldungen auf.

Warnungen – Kritische Fehler und Warnungen werden protokolliert.

Keine – Es werden keine Logs aufgezeichnet.

Benutzerliste

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur Benutzerliste hinzufügen:

Bearbeiten ... – Öffnet den **Identitäts-Editor**, in dem Sie Benutzer oder Gruppen auswählen können. Um eine Liste von Benutzern einzurichten, wählen Sie die gewünschten **Benutzer** links in der Liste Benutzer aus und klicken auf **Hinzufügen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Ausgewählte Benutzer** aus und klicken auf **Entfernen**. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn diese Liste leer ist, werden alle Benutzer zugelassen.

Einschränkungen für Benutzerregeln



Nicht alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

Web-Kontrolle

Mit der Funktion **Web-Kontrolle** können Sie Einstellungen konfigurieren, die dazu beitragen, Ihr Unternehmen vor Situationen zu schützen, für die es gesetzlich haftet. So kann mit der Web-Kontrolle beispielsweise der Zugriff auf Websites geregelt werden, die Urheberrechte verletzen. Ziel ist es, Mitarbeiter am Zugriff auf Webseiten mit ungeeigneten oder schädlichen Inhalten bzw. mit negativem Einfluss auf die Produktivität zu hindern. Arbeitgeber oder Systemadministratoren können mit dieser Funktion den Zugriff auf über 27 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Die Web-Kontrolle ist standardmäßig deaktiviert. Um sie zu aktivieren, klicken Sie auf **Einstellungen > Erweiterte Einstellungen > Web-Kontrolle** und aktivieren Sie das Kontrollkästchen neben **Web-Kontrolle aktivieren**.

Im Fenster „Regel-Editor“ werden vorhandene URL-basierte oder Kategorie-basierte Regeln angezeigt. Die Liste der Regeln enthält verschiedene Angaben zu jeder Regel, wie Regelname, Art des Sperrrens, auszuführende Aktion nach dem Zuordnen einer Regel der Web-Kontrolle und [Log](#)-Schweregrad.

Um eine neue Regel zu erstellen, klicken Sie auf die Schaltfläche . Doppelklicken Sie auf das Feld **Name** und geben Sie zur einfacheren Identifizierung eine Beschreibung der Regel ein.

Mit dem Kontrollkästchen des Felds **Aktiviert** kann die Regel aktiviert/deaktiviert werden. Dies kann hilfreich sein, wenn Sie eine Regel später verwenden und daher nicht dauerhaft löschen möchten.

Typ

URL-basierte Aktion - Zugriff auf die gegebene Website. Doppelklicken Sie auf das Feld **URL/Kategorie** und geben Sie die entsprechende URL-Adresse ein.

In der Liste der URL-Adressen können Sie die Sonderzeichen * (Sternchen) und ? (Fragezeichen) nicht verwenden. Webseitenadressen mit mehreren TLDs (Top-Level-Domains) müssen zur erstellten Gruppe eingegeben werden (*beispielseite.com, beispielseite.sk* usw.). Wenn Sie eine Domäne zur Liste hinzufügen, werden alle Inhalte der Domäne und der Unterdomänen (z. B. *unterdomäne.beispielseite.com*) je nach gewählter URL-basierter Aktion gesperrt bzw. zugelassen.

Kategorie-basierte Aktion - Doppelklicken Sie auf das Feld **URL/Kategorie** und wählen Sie die Kategorien aus.

Identität

Hier können Sie Benutzer auswählen, auf die die Regel angewendet wird.

Zugriffsrechte

Zulassen - Auf die URL-Adresse/Kategorie darf zugegriffen werden.

Sperren - Sperrt die URL-Adresse/Kategorie.

Schweregrad (für das [Filtern](#) der Log-Dateien)

Immer - Alle Ereignisse werden protokolliert.

Diagnose - Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.

Informationen - Zeichnet zusätzlich zu den oben genannten Einträgen informative Meldungen auf.

Warnungen - Kritische Fehler und Warnungen werden protokolliert.

Keine - Es werden keine Logs erstellt.

Tools

Das Menü **Tools** enthält Module zur einfacheren Verwaltung des Programms sowie zusätzliche Optionen für fortgeschrittene Benutzer.

Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Aufzeichnen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Endpoint Security for macOS heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptfenster von ESET Endpoint Security for macOS aufgerufen werden, indem Sie auf **Tools > Log-Dateien** klicken. Wählen Sie im Dropdownmenü „Log“ im oberen Bereich des Fensters das gewünschte Log aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** – Informationen zu Ereignissen in Bezug auf erkannte Bedrohungen.
2. **Ereignisse** – Alle von ESET Endpoint Security for macOS ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.
3. **Computerprüfung** – In diesem Fenster werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu einem bestimmten Computer-Scan anzeigen.
4. **Medienkontrolle** – Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.
5. **Firewall** – Das Firewall-Log zeigt alle von der Firewall entdeckten Angriffe von anderen Computern an. Firewall-Logs enthalten Informationen zu erkannten Systemangriffen. In der Spalte **Ereignis** werden die erkannten Angriffe aufgelistet. Die Spalte **Quelle** enthält weitere Informationen über den Angreifer und die Spalte **Protokoll** gibt an, welches Kommunikationsprotokoll für den Angriff verwendet wurde.
6. **Web-Kontrolle** – Zeigt gesperrte bzw. zugelassene URL-Adressen und Details zu deren Kategorien an.
7. **Gefilterte Websites** – Diese Liste ist nützlich, wenn Sie sehen möchten, welche Websites vom [Web-Schutz](#) oder der [Web-Kontrolle](#) gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL, den Status, die IP-Adresse, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.

Klicken Sie mit der rechten Maustaste auf eine beliebige Log-Datei und klicken Sie dann auf **Kopieren**, um den Inhalt dieser Log-Datei in die Zwischenablage zu kopieren.

Log-Wartung

Die Log-Konfiguration für ESET Endpoint Security for macOS können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen > Tools > Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Alte Log-Einträge automatisch löschen** – Log-Einträge, die älter als die angegebene Anzahl Tage sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren** – Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.

Alle relevanten Informationen in der grafischen Benutzeroberfläche sowie Bedrohungs- und Ereignisnachrichten können in menschenlesbarer Textform gespeichert werden, z. B. in Nur-Text- oder CSV-Dateien (durch Komma getrennte Dateien). Wenn Sie diese Dateien zur weiteren Verarbeitung in Drittanbieter-Tools verfügbar machen möchten, aktivieren Sie das Kontrollkästchen neben **Protokollierung in Textdateien aktivieren**.

Um den Zielordner für die Log-Dateien festzulegen, klicken Sie auf **Einstellungen** neben **Erweiterte Einstellungen**.

Je nach den unter **Log-Textdateien: Bearbeiten** ausgewählten Optionen können Log-Dateien mit folgenden Informationen gespeichert werden:

- Ereignisse wie *Ungültiger Benutzername/ungültiges Passwort, Module konnten nicht aktualisiert werden* usw. werden in der Datei *eventslog.txt* gespeichert.
- Durch den Systemstart-Scanner, den Echtzeit-Dateischutz oder die Computerprüfung erkannte Bedrohungen werden in der folgenden Datei gespeichert: *threatslog.txt*
- Die Ergebnisse aller durchgeführten Scans werden im Format *scanlog.NUMMER.txt* gespeichert.
- Von der Medienkontrolle blockierte Geräte werden in *devctllog.txt* aufgezeichnet.
- Alle Ereignisse in Bezug auf die Kommunikation über die Firewall werden in die Datei *firewallog.txt* geschrieben.
- Von der Web-Kontrolle blockierte Seiten werden in *webctllog.txt* aufgezeichnet.

Um die **Standardcomputer-Scanprotokolleinträge** zu konfigurieren, klicken Sie auf **Bearbeiten** und aktivieren/deaktivieren die einzelnen Log-Typen je nach Bedarf. Weitere Erläuterungen zu diesen Log-Typen finden Sie unter [Log-Filter](#).

Log-Filter

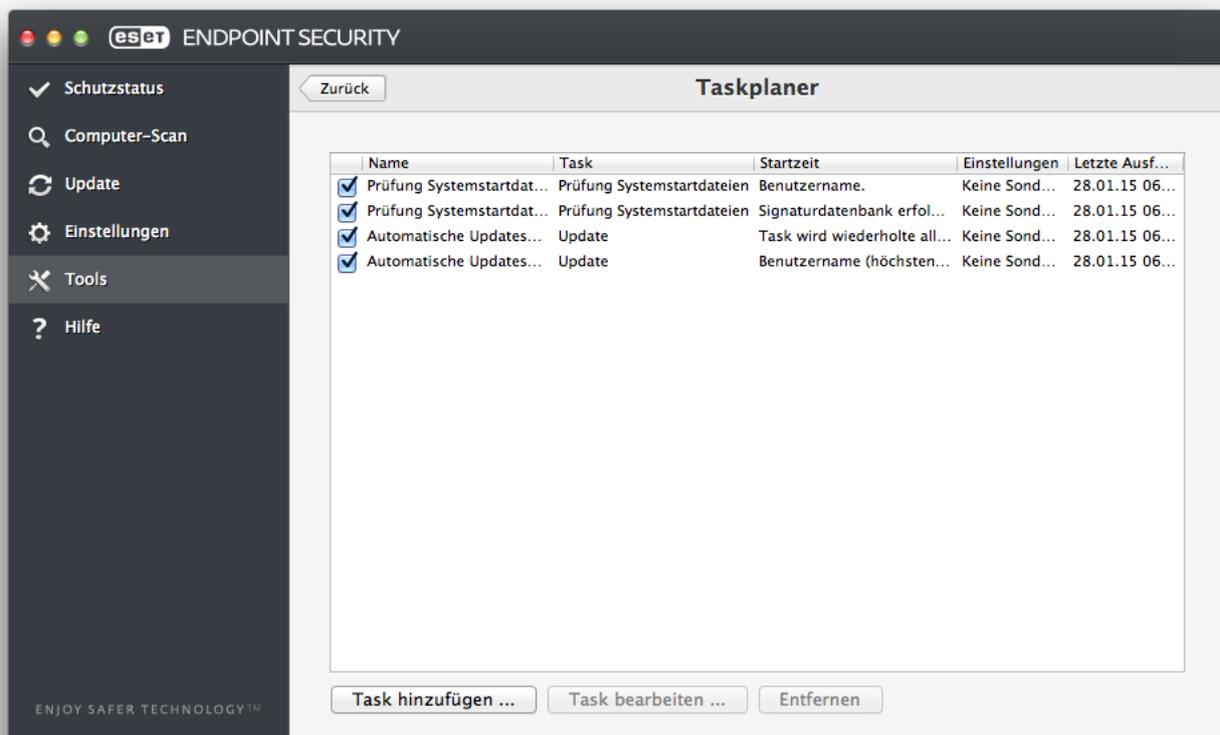
In den Logs werden Informationen über wichtige Systemereignisse gespeichert: Mit dem Log-Filter können Sie Einträge zu bestimmten Ereignissen anzeigen.

Nachfolgend sind die am häufigsten verwendeten Arten von Logs aufgelistet:

- **Kritische Warnungen** – kritische Systemfehler (z. B. „Virenschutz konnte nicht gestartet werden“)
- **Fehler** - Fehler wie z. B. „Fehler beim Herunterladen einer Datei“ und kritische Fehler
- **Warnungen** – Warnmeldungen
- **Informationen** - Meldungen wie erfolgreiche Updates, Warnungen usw.
- **Diagnosedaten** – alle bisher genannten Einträge sowie Informationen, die für die Feineinstellung des Programms erforderlich sind

Taskplaner

Um den Taskplaner zu öffnen, klicken Sie im Hauptmenü von ESET Endpoint Security for macOS unter **Tools** auf **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Scanprofils.



Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und bestimmte Profile, die bei Ausführung des Tasks verwendet werden.

Standardmäßig werden im Taskplaner die folgenden Tasks angezeigt:

- Log-Wartung (nach Aktivieren von **System-Tasks anzeigen** in den Taskplaner-Einstellungen)
- Prüfung Systemstartdateien nach Anmeldung des Benutzers
- Scannen der Systemstartdateien nach erfolgreichem Update der Erkennungsroutinen
- Automatische Updates in festen Zeitabständen
- Automatische Updates beim Anmelden des Benutzers

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, halten Sie die Ctrl-Taste gedrückt und klicken Sie auf den Task und dann auf **Bearbeiten**. Alternativ können Sie den Task, den Sie ändern möchten, auswählen und dann auf **Task bearbeiten** klicken.

Erstellen von Tasks

Zum Erstellen eines neuen Tasks im Taskplaner klicken Sie auf **Task hinzufügen** oder klicken Sie bei gedrückter Strg-Taste auf das leere Feld und wählen im Kontextmenü die Option **Hinzufügen** aus. Es gibt vier Arten von Tasks:

- Anwendung starten
- Update
- On-Demand-Scan
- Scan der Systemstartdateien

Benutzerdefinierte Tasks

i Anwendungen werden standardmäßig von einem speziellen, von ESET erstellten Benutzer mit eingeschränkten Rechten ausgeführt. Falls Sie einen anderen als den Standardbenutzer verwenden möchten, geben Sie den Benutzernamen gefolgt von einem Doppelpunkt (:) vor dem Befehl ein. Sie können auch den Benutzer **root** für diese Funktion verwenden.

Beispiel: Task als Benutzer ausführen

In diesem Beispiel starten wir die Rechner-App zu einer festgelegten Uhrzeit als Benutzer **UserOne**:

1. Wählen Sie im **Taskplaner** die Option **Task hinzufügen** aus.
2. Geben Sie einen Tasknamen ein. Wählen Sie **Anwendung ausführen** für den **geplanten Task** aus. Wählen Sie im Fenster **Task ausführen** die Option **Einmalig** aus, um den Task ein einziges Mal auszuführen. Klicken Sie auf **Weiter**.
- ✓ 3. Klicken Sie auf „Durchsuchen“, und wählen Sie die Rechner-App aus.
4. Geben Sie **UserOne:** vor dem Anwendungspfad ein (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') und klicken Sie auf **Weiter**.
5. Wählen Sie eine Uhrzeit für die Ausführung des Tasks aus und klicken Sie auf **Weiter**.
6. Wählen Sie eine alternative Option aus, falls der Task nicht ausgeführt werden kann, und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.
8. Der ESET-Taskplaner startet die Rechner-App zum ausgewählten Zeitpunkt.

Einschränkungen für Benutzernamen

- !** Vor einem Benutzernamen dürfen keine Leerzeichen stehen. Benutzernamen dürfen auch keine Leerzeichen enthalten. Verwenden Sie stattdessen ein anderes leeres Zeichen.

Scannen als Verzeichnisbesitzer

Sie können Verzeichnisse als Besitzer scannen:

i `root:for VOLUME in /Volumes/*; do sudo -u \# stat -f %u "$VOLUME" '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done`

Außerdem können Sie den Ordner „/tmp“ als aktuell angemeldeter Benutzer scannen:

`root:sudo -u \# stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp`

Beispiel: Update-Task

In diesem Beispiel erstellen wir einen Update-Task, der zu einem festgelegten Zeitpunkt ausgeführt wird.

1. Wählen Sie im Dropdownmenü **Geplanter Task** die Option **Update** aus.
2. Geben Sie im Feld **Taskname** einen Namen für den Task ein.
- ✓ 3. Wählen Sie in der Liste **Task ausführen** das gewünschte Ausführungsintervall aus. Je nach ausgewähltem Intervall werden Sie aufgefordert, verschiedene Update-Parameter festzulegen. Falls Sie **Benutzerdefiniert** auswählen, werden Sie aufgefordert, Datum und Uhrzeit im cron-Format anzugeben (nähere Informationen siehe Abschnitt [Erstellen eines benutzerdefinierten Tasks](#)).
4. Wählen Sie im nächsten Schritt eine alternative Option für den Fall aus, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann.
5. Klicken Sie auf **Fertig stellen**. Der neue geplante Task wird der Liste der aktuellen Tasks hinzugefügt.

Einige Tasks sind für die ordnungsgemäße Funktion des Systems unerlässlich und standardmäßig in ESET Endpoint Security for macOS enthalten. Diese Tasks dürfen nicht modifiziert werden und sind standardmäßig ausgeblendet. Um diese Tasks anzuzeigen, klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen** > **Taskplaner** und wählen Sie **System-Tasks anzeigen** aus.

Erstellen eines benutzerdefinierten Tasks

Wenn Sie im Dropdown-Menü „Task ausführen“ den Tasktyp „Benutzerdefiniert“ auswählen, müssen Sie einige Parameter definieren.

Datum und Uhrzeit von Tasks des Typs **Benutzerdefiniert** müssen im cron-Langformat mit Jahr angegeben werden (Zeichenfolge aus 6 Feldern, jeweils getrennt durch ein Leerzeichen):

Minute(0-59) Stunde(0-23) Tag(1-31) Monat(1-12) Jahr(1970-2099)
Wochentag(0-7) (Sonntag = 0 oder 7)

✓ **Beispiel:**
30 6 22 3 2012 4

Folgende Sonderzeichen werden in cron-Ausdrücken unterstützt:

- Sternchen (*) - Steht für alle möglichen Werte des betreffenden Felds. Beispiel: Sternchen im dritten Feld (Tag) = jeder Tag im Monat
- Bindestrich (-) - Definition von Zeiträumen, z. B. 3-9
- Komma (,) - Trennt mehrere Einträge einer Liste, z. B. 1,3,7,8
- Schrägstrich (/) -Definition von Intervallen in Zeiträumen, z. B. 3-28/5 im dritten Feld (Tag des Monats) = am 3. des Monats und anschließend alle 5 Tage.

Textbezeichnungen für Tage ((Monday-Sunday)) und Monate ((January-December)) werden nicht unterstützt.

Benutzerdefinierte Tasks
i Werden sowohl Tag als auch Wochentag angegeben, so wird der Befehl nur ausgeführt, wenn beide Bedingungen erfüllt sind.

LiveGrid®

Dank des LiveGrid®-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Infiltrationen. Das LiveGrid®-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit, neue Bedrohungen zu erkennen, sobald sie in Erscheinung treten, besteht darin, so viele unserer Kunden wie möglich einzubinden und die von ihnen erfassten Informationen zur Aktualisierung der Erkennungsmodule zu nutzen. Wählen Sie eine der beiden Optionen für LiveGrid®:

1. Sie können sich entscheiden, das LiveGrid®-Frühwarnsystem nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Endpoint Security for macOS jedoch

möglicherweise schneller auf neue Bedrohungen als die Aktualisierung der Erkennungsmodule.

2. Sie können das LiveGrid®-Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Informationen können zur detaillierten Analyse an ESET gesendet werden. Nach ihrer Untersuchung kann ESET dann die Signaturdatenbank aktualisieren und so die Erkennungsleistung des Programms verbessern.

Das LiveGrid®-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

Auch wenn es möglich ist, dass das ESET-Virenlabor auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält (zum Beispiel Benutzernamen in einem Verzeichnispfad usw.), werden diese Daten für keinen anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf neue Bedrohungen verwendet.

Zum Zugriff auf die LiveGrid®-Einrichtung klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen** > **LiveGrid®**. Wählen Sie **An ESET LiveGrid® teilnehmen (empfohlen)** aus, um LiveGrid® zu aktivieren. Klicken Sie dann neben **Erweiterte Einstellungen** auf **Einstellungen**.

Verdächtige Dateien

ESET Endpoint Security for macOS ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse an das ESET-Virenlabor eingereicht werden. Wenn Sie die Dateien nicht automatisch einreichen möchten, deaktivieren Sie die Option **Einreichen verdächtiger Dateien (Einstellungen > Erweiterte Einstellungen > LiveGrid® > Einstellungen)**.

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Klicken Sie hierzu im Hauptprogrammfenster auf **Tools** > **Datei zur Analyse einreichen**. Falls dabei schädlicher Code gefunden wird, wird dieser beim nächsten Update berücksichtigt.

Anonymisierte statistische Daten einreichen – Das ESET LiveGrid®-Frühwarnsystem erfasst anonyme Informationen zu Ihrem Computer in Bezug auf neu erkannte Bedrohungen. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer des ESET Security-Produkts sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Diese Statistikpakete werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel: Übermitteltes Statistikpaket

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
✓ # osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Ausschlussfilter – Über diese Option können Sie bestimmte Dateitypen vom Senden ausschließen. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc, .rtf usw.). Sie können der Ausschlussliste weitere Dateitypen hinzufügen.

E-Mail-Adresse für Rückfragen (optional) – Ihre E-Mail-Adresse kann dazu verwendet werden, Sie bei Rückfragen zu kontaktieren. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

Quarantäne

Hauptzweck der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Endpoint Security for macOS fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, während des Virenschutz-Scans jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an das ESET-Virenlabor eingereicht werden.

Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der erkannten Bedrohungen enthält. Der Quarantäneordner (*/Library/Application Support/Eset/esets/cache/quarantine*) bleibt auch nach der Deinstallation von ESET Endpoint Security for macOS im System bestehen. Die Quarantäne-dateien werden sicher verschlüsselt gespeichert und können nach der Reinstallation von ESET Endpoint Security for macOS wiederhergestellt werden.

Quarantäne für Dateien

ESET Endpoint Security for macOS kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Im Fenster „Quarantäne“ können Sie auf „Quarantäne“ klicken, um eine Datei manuell zur Quarantäne hinzuzufügen. Sie können auch jederzeit bei gedrückter Strg-Taste auf eine Datei klicken und im Kontextmenü „Dienste“ > „ESET Endpoint Security for macOS - Dateien zur Quarantäne hinzufügen“ auswählen, um eine Datei in die Quarantäne zu verschieben.

Wiederherstellen aus der Quarantäne

Dateien können aus der Quarantäne an ihrem ursprünglichen Speicherort wiederhergestellt werden. Wählen Sie hierzu eine Datei aus und klicken Sie auf **Wiederherstellen**. Die Wiederherstellungsfunktion ist auch über das Kontextmenü verfügbar. Halten Sie die Strg-Taste gedrückt, klicken Sie auf die gewünschte Datei im Quarantäfenster und klicken Sie anschließend auf **Wiederherstellen**. Über die Funktion **Wiederherstellen nach** können Sie eine Datei an einem anderen als dem ursprünglichen Speicherort wiederherstellen.

Einreichen von Dateien aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an das ESET-Virenlabor. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, drücken Sie die Strg-Taste und klicken Sie auf die Datei. Wählen Sie dann im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen** aus.

Berechtigungen

Die Einstellungen von ESET Endpoint Security for macOS können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Deshalb können Sie auswählen, welche Benutzer die Programmkonfiguration bearbeiten dürfen.

Sie können privilegierte Benutzer unter **Einstellungen > Erweiterte Einstellungen > Benutzer > Rechte** konfigurieren.

Maßgeblich für einen wirksamen Schutz Ihres Systems ist die richtige Konfiguration des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um die Liste der privilegierten Benutzer einzurichten, wählen Sie die gewünschten Benutzer links in der Liste **Benutzer** aus und klicken auf **Hinzufügen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Privilegierte Benutzer** rechts aus und klicken auf **Entfernen**. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus.

Leere privilegierte Benutzerliste

i Wenn die Liste der privilegierten Benutzer leer ist, können alle Systembenutzer die Programmeinstellungen bearbeiten.

Präsentationsmodus

Der **Präsentationsmodus** ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Präsentationsmodus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Popup-Fenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Um den Präsentationsmodus manuell zu aktivieren, klicken Sie auf **Einstellungen > Erweiterte Einstellungen ... > Präsentationsmodus > Präsentationsmodus aktivieren**.

Aktivieren Sie das Kontrollkästchen neben **Präsentationsmodus im Vollbildmodus automatisch aktivieren**, wenn der Präsentationsmodus beim Ausführen von Anwendungen im Vollbildmodus automatisch ausgelöst werden soll. Wenn diese Funktion aktiviert ist, wird der Präsentationsmodus gestartet, sobald Sie eine Vollbildanwendung initiieren, und automatisch beendet, wenn Sie diese Vollbildanwendung beenden. Dies ist besonders zum Beginnen einer Präsentation hilfreich.

Mit der Option **Präsentationsmodus automatisch deaktivieren nach** können Sie außerdem die Zeit in Minuten festlegen, nach der der Präsentationsmodus automatisch deaktiviert wird.

Im Präsentationsmodus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol von ESET Endpoint Security for macOS orange und mit einer Warnung angezeigt.

Interaktiver und Präsentationsmodus in der Firewall

Wenn sich die Firewall im interaktiven Filtermodus befindet und der Präsentationsmodus aktiviert wird, kann es zu Problemen beim Aufbau einer Internetverbindung kommen. Dies kann beim Ausführen einer Anwendung, die eine Internetverbindung verwendet, zu Problemen führen. Üblicherweise müssen Sie eine solche Aktion bestätigen (sofern keine Verbindungsregeln oder -ausnahmen festgelegt wurden), doch im Präsentationsmodus kann der Benutzer keine derartigen Eingaben machen. Um dies zu umgehen, muss entweder eine Verbindungsregel für jede Anwendung festgelegt werden, mit der es im Präsentationsmodus zu Konflikten kommen kann, oder es muss eine andere Filtermethode für die Firewall gewählt werden. Bedenken Sie, dass Sie im Präsentationsmodus bei dem Versuch, eine Website zu besuchen oder eine Anwendung auszuführen, die möglicherweise Sicherheitsrisiken darstellen, nicht benachrichtigt bzw. gewarnt werden, dass diese blockiert sind. Grund dafür ist die deaktivierte Benutzerinteraktion.

Ausgeführte Prozesse

Die Liste **Ausgeführte Prozesse** zeigt die auf Ihrem Computer ausgeführten Prozesse an. ESET Endpoint Security for macOS liefert detaillierte Informationen zu den ausgeführten Prozessen, um Benutzern den Schutz der ESET LiveGrid®-Technologie zu bieten.

- **Prozess** - Name des aktuell auf Ihrem Computer ausgeführten Prozesses. Sie können die auf dem Computer ausgeführten Prozesse auch mit der Aktivitätsanzeige (*/Applications/Utilities*) anzeigen.
- **Risikostufe** - In den meisten Fällen weisen ESET Endpoint Security for macOS und die ESET LiveGrid®-Technologie den Objekten (Dateien, Prozesse usw.) eine Risikostufe zu. Dies erfolgt unter Einsatz einer Reihe heuristischer Regeln, die die Eigenschaften des Objekts untersuchen und auf dieser Grundlage den Verdacht auf Schadcode abwägen. Den Objekten wird auf Grundlage dieser heuristischen Regeln eine Risikostufe zugewiesen. Bekannte Anwendungen, die grün markiert und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen. Dies sorgt für schnellere On-Demand- und Echtzeit-Scans. Eine als unbekannt eingestufte Anwendung (gelb) enthält nicht unbedingt Schadcode. Meist handelt es sich einfach um eine neuere Anwendung. Wenn Sie sich bei einer Datei nicht sicher sind, können Sie sie zur Analyse an das ESET-Virenlabor einreichen. Wenn sich herausstellt, dass die Datei Schadcode enthält, wird die entsprechende Signatur zu einem zukünftigen Update hinzugefügt.
- **Anzahl Benutzer** - gibt die Anzahl der Benutzer an, die eine bestimmte Anwendung verwenden. Diese Information wird durch die ESET LiveGrid®-Technologie erfasst.
- **Erkennungszeit** - gibt an, wann die Anwendung von der ESET LiveGrid®-Technologie erkannt wurde.
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.

Wenn Sie auf einen Prozess klicken, werden am unteren Bildschirmrand folgende Informationen angezeigt:

- **Datei** - Speicherort der Anwendung auf Ihrem Computer
- **Dateigröße** - physikalische Größe der Datei auf dem Datenträger
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung vom Betriebssystem

- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.
- **Dateiversion** - Informationen vom Herausgeber der Anwendung
- **Produktname** - Anwendungs- und/oder Firmenname

Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Sie finden diese Optionen unter **Einstellungen > Erweiterte Einstellungen > Benutzeroberfläche**.

- Um das ESET Endpoint Security for macOS-Startbild beim Programmstart zu aktivieren, aktivieren Sie die Option **Startbild anzeigen**.
- Mit der Option **Anwendung in Dock anzeigen** wird das ESET Endpoint Security for macOS-Symbol  im macOS-Dock angezeigt, und Sie können mit der Tastenkombination `cmd+tab` zwischen ESET Endpoint Security for macOS und anderen geöffneten Anwendungen wechseln. Die Änderungen werden beim nächsten Start von ESET Endpoint Security for macOS (in der Regel nach einem Neustart des Computers) wirksam.
- Mit der Option **Standardmenü verwenden** können Sie bestimmte Tastaturbefehle verwenden (siehe [Tastenkombinationen](#)) und Standardmenüeinträge (Benutzeroberfläche, Einstellungen und Tools) in der OS X-Menüleiste am oberen Bildschirmrand anzeigen.
- Aktivieren Sie **QuickInfo anzeigen**, damit QuickInfos angezeigt werden, wenn der Cursor über bestimmte Optionen von ESET Endpoint Security for macOS bewegt wird.
- Wenn **Versteckte Dateien anzeigen** aktiviert ist, können Sie im Einstellungsbereich **Zu scannende Objekte** der Funktion **Computer scannen** auch versteckte Dateien sehen und diese auswählen.
- Standardmäßig wird das ESET Endpoint Security for macOS-Symbol  in den Menüleisten-Extras auf der rechten Seite der macOS-Menüleiste am oberen Bildschirmrand angezeigt. Sie können diese Funktion über die Option **Symbol in Menüleisten-Extras anzeigen** deaktivieren. Die Änderungen werden beim nächsten Start von ESET Endpoint Security for macOS (in der Regel nach einem Neustart des Computers) wirksam.

Warnungen und Benachrichtigungen

Im Bereich **Warnungen und Benachrichtigungen** können Sie konfigurieren, wie Warnungen, Schutzstatus- und Systembenachrichtigungen in ESET Endpoint Security for macOS behandelt werden.

Wenn Sie die Option **Warnungen anzeigen** deaktivieren, werden keinerlei Warnfenster angezeigt. Dies wird nur für bestimmte Situationen empfohlen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten. Die verfügbaren Optionen werden [in diesem Kapitel](#) beschrieben.

Wenn Sie die Option **Hinweise auf dem Desktop anzeigen** aktivieren, werden Warnfenster, die keinen Benutzereingriff erfordern, auf dem Desktop angezeigt (standardmäßig oben rechts auf dem Bildschirm). Wie lang

solche Hinweise erscheinen, können Sie über den Wert **Hinweise automatisch schließen nach X Sekunden** festlegen (der Standardwert beträgt 5 Sekunden).

Seit ESET Endpoint Security for macOS Version 6.2 können Sie außerdem bestimmte **Schutzstatusanzeigen** im Hauptbildschirm des Programms (Fenster **Schutzstatus**) deaktivieren. Weitere Informationen hierzu finden Sie unter [Schutzstatus](#).

Warnungen anzeigen

Bei neuen Programmversionen und Betriebssystem-Updates, beim Deaktivieren bestimmter Programmkomponenten, beim Löschen von Logs usw. werden in ESET Endpoint Security for macOS Warn- und Hinweisfenster angezeigt. Diese können Sie mit Wirkung für die Zukunft unterdrücken, indem Sie im jeweiligen Dialogfenster die Option **Dialogfenster nicht mehr anzeigen** aktivieren.

Liste der Dialogfenster (Einstellungen > Erweiterte Einstellungen >> Warnungen und Benachrichtigungen > Warnungen anzeigen: Einstellungen) enthält Sie eine Liste aller Warnungsdialoge in ESET Endpoint Security for macOS. Über das Kontrollkästchen neben **Dialogname** können Sie die Anzeige der einzelnen Benachrichtigungsarten aktivieren oder unterdrücken. Wenn Sie das Kontrollkästchen aktivieren, wird die Benachrichtigung immer angezeigt, und die **Anzeigebedingungen** gelten nicht. Wenn Sie keine Benachrichtigung für ein bestimmtes Ereignis erhalten möchten, deaktivieren Sie diese Option oder legen Sie **Anzeigebedingungen** fest, unter denen eine bestimmte Aktion ausgeführt wird.

Schutzstatus

Der aktuelle Schutzstatus von ESET Endpoint Security for macOS kann durch Aktivieren oder Deaktivieren von Statusmeldungen in **Einstellungen > Erweiterte Einstellungen... > Warnungen und Benachrichtigungen > Im Bildschirm Schutzstatus anzeigen: Einstellungen** geändert werden. Der Status verschiedener Programmfunktionen wird im ESET Endpoint Security for macOS-Hauptbildschirm (Fenster **Schutzstatus**) ein- oder ausgeblendet.

Sie können den Schutzstatus der folgenden Programmfeatures ausblenden:

- Firewall
- Phishing-Schutz
- Web-Schutz
- E-Mail-Schutz
- Präsentationsmodus
- Betriebssystem-Update
- Lizenzablauf
- Computerneustart erforderlich

Kontextmenü

Um Funktionen von ESET Endpoint Security for macOS im Kontextmenü verfügbar zu machen, klicken Sie auf **Einstellungen > Erweiterte Einstellungen > Kontextmenü** und aktivieren Sie das Kontrollkästchen neben **In Kontextmenü integrieren**. Die Änderungen werden nach dem Abmelden und einem Neustart des Computers übernommen. Die Optionen des Kontextmenüs werden auf dem Desktop im **Finder**-Fenster angezeigt, wenn Sie bei gedrückter STRG-Taste auf eine beliebige Datei klicken.

Update

Für optimalen Schutz muss ESET Endpoint Security for macOS regelmäßig aktualisiert werden. Das Updatemodul lädt die neuesten Erkennungsroutinen herunter und sorgt dafür, dass die Anwendung immer auf dem neuesten Stand ist.

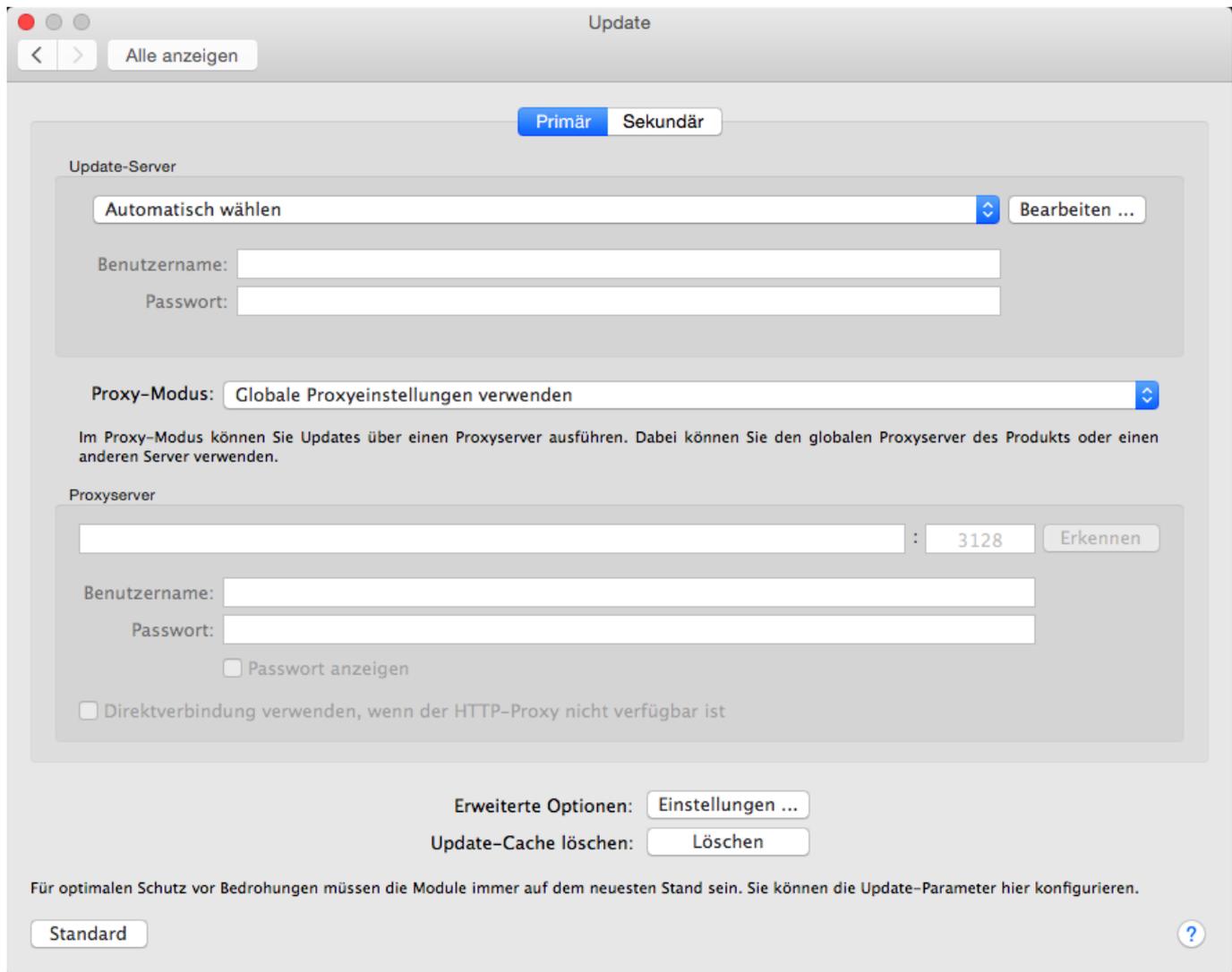
Über **Update** im Hauptmenü können Sie sich den aktuellen Update-Status anzeigen lassen. Hier sehen Sie Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Klicken Sie auf **Jetzt aktualisieren**, um den Updatevorgang manuell zu starten.

Wenn beim Update-Download keinerlei Zwischenfälle auftreten und Sie über die neuesten Module verfügen, wird im Update-Fenster der Hinweis *Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand* angezeigt. Wenn die Module nicht aktualisiert werden können, sollten Sie die [Update-Einstellungen](#) überprüfen. Die häufigste Fehlerursache sind falsch eingegebene [Lizenzdaten](#) oder fehlerhaft konfigurierte [Verbindungseinstellungen](#).

Im Fenster **Update** wird auch die Versionsnummer der Erkennungsroutine angezeigt. Diese Nummer ist ein Link zur ESET-Website, auf der weitere Updateinformationen für die Erkennungsroutine angezeigt werden.

Einstellungen für Updates

In den Einstellungen für Updates finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Lizenzdaten für diese Server. Standardmäßig ist die Option **Update-Server** auf **Automatisch wählen** eingestellt. So werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist.



Das Dropdownmenü **Update-Server** enthält eine Liste der aktuellen Update-Server. Um einen neuen Update-Server hinzuzufügen, klicken Sie auf **Bearbeiten**, geben Sie die Adresse des neuen Servers in das Eingabefeld **Update-Server** ein und klicken Sie auf **Hinzufügen**.

In ESET Endpoint Security for macOS können Sie einen alternativen Update-Server oder Failover-Update-Server festlegen. Beispielsweise könnten Sie unter **Primärer Server** Ihren Mirror-Server und unter **Sekundär Server** den normalen ESET-Update-Server festlegen. Der sekundäre Server wird nur verwendet, wenn sich diese beiden Angaben unterscheiden. Wenn Sie die Angaben für den sekundären Server (Update-Server, Benutzername, Passwort) leer lassen, kann natürlich auch kein Update über einen sekundären Server durchgeführt werden. Wenn Sie „Automatisch auswählen“ aktivieren und Ihren Benutzernamen und das Passwort in die entsprechenden Felder eingeben, wählt ESET Endpoint Security for macOS automatisch den am besten geeigneten Update-Server aus.

Im **Proxy-Modus** können Sie die Erkennungsmodule über einen Proxyserver aktualisieren (z. B. einen lokalen HTTP-Proxy). Sie können entweder den globalen Proxyserver angeben, der für alle Programmfeatures verwendet wird, die eine Verbindung benötigen, oder einen anderen Server. Die globalen Proxyservereinstellungen wurden entweder während der Installation definiert oder können in den [Proxyserver-Einstellungen](#) konfiguriert werden.

Um einen Client so zu konfigurieren, dass Updates nur über einen Proxyserver heruntergeladen werden:

1. Wählen Sie **Verbindung über Proxyserver** im Dropdown-Menü aus.
2. Wenn Sie auf **Erkennen** klicken, füllt ESET Endpoint Security for macOS die IP-Adresse und die Portnummer aus (standardmäßig **3128**).
3. Geben Sie die entsprechenden Informationen in die Felder **Benutzername** und **Passwort** ein, falls für den Proxyserver eine Authentifizierung erforderlich ist.

ESET Endpoint Security for macOS erkennt die Proxy-Einstellungen aus den macOS-Systemeinstellungen. Sie finden diese Einstellungen in macOS unter  > **Systemeinstellungen** > **Netzwerk** > **Erweitert** > **Proxies**.

Wenn Sie die Option **Direktverbindung verwenden, wenn Proxy nicht verfügbar ist** aktivieren, versucht ESET Endpoint Security for macOS automatisch, sich ohne Proxy mit den Updateservern zu verbinden. Diese Option wird für mobile Benutzer mit MacBooks empfohlen.

Wenn beim Herunterladen der Updates für die Erkennungsmodule Fehler auftreten, klicken Sie auf **Update-Cache löschen, um temporäre Update-Dateien zu löschen**.

Erweiterte Einstellungen

Um die Benachrichtigungen zu erfolgreichen Updates zu deaktivieren, wählen Sie **Keine Benachrichtigung über erfolgreiche Updates anzeigen** aus.

Aktivieren Sie den Testmodus, um Entwicklungsmodule herunterzuladen, die sich in der abschließenden Testphase befinden. Die Updates des Testmodus enthalten oft Korrekturen für Produktprobleme. Mit dem verzögerten Update werden die Updates einige Stunden nach ihrer Veröffentlichung heruntergeladen, um sicherzustellen, dass die Clients die Updates erst erhalten, wenn bestätigt ist, dass keine Probleme mit den Updates auftreten.

ESET Endpoint Security for macOS zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der Funktion **Update-Rollback** auf. Lassen Sie die Option **Snapshots der Update-Dateien erstellen** aktiviert, damit ESET Endpoint Security for macOS diese Snapshots automatisch aufzeichnet. Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder eines Programmmoduls beschädigt oder nicht stabil ist, können Sie ein Update-Rollback ausführen, um eine vorherige Version wiederherzustellen, und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren. Wenn Sie die Funktion „Update-Rollback“ verwenden, um eine frühere Version wiederherzustellen, legen Sie im Dropdown-Menü „Dauer für Aussetzen festlegen auf“ den Zeitraum fest, für den die Updates ausgesetzt werden sollen. Wenn Sie „Bis zur Aufhebung“ auswählen, werden die normalen Updates erst fortgesetzt, wenn Sie dies manuell wiederherstellen. Legen Sie den Zeitraum zum Aussetzen der Updates mit Bedacht fest.

Maximales Alter der Erkennungsroutine automatisch festlegen – Hier können Sie eine Zeitdauer (in Tagen) festlegen, nach der die Erkennungsmodule spätestens als veraltet gemeldet werden. Der Standardwert ist 7 Tage.

So erstellen Sie Update-Tasks

Klicken Sie auf Update > **Modul-Update**, um eine Aktualisierung der Module manuell zu starten.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Endpoint Security for macOS folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie unter [Taskplaner](#).

System-Updates

Die Systemupdatefunktion für macOS ist eine wichtige Komponente zum Schutz des Benutzers vor Schadcode. Zur Gewährleistung des bestmöglichen Schutzes empfohlen wird, die Updates möglichst umgehend zu installieren, sobald sie verfügbar sind. ESET Endpoint Security for macOS zeigt je nach Wichtigkeit der Updates Benachrichtigungen zu fehlenden Updates an. Sie können festlegen, ab welcher Wichtigkeit Update-Benachrichtigungen angezeigt werden. Navigieren Sie hierzu zu **Einstellungen > Erweiterte Einstellungen > Warnungen und Benachrichtigungen > Einstellungen** und verwenden Sie das Dropdown-Menü **Anzeigebedingungen** neben **Betriebssystem-Updates**.

- **Alle Updates anzeigen** - Benachrichtigungen werden für alle fehlenden Updates angezeigt
- **Nur empfohlene Updates anzeigen** - Benachrichtigungen werden nur für empfohlene Updates angezeigt

Wenn Sie keine Benachrichtigungen zu fehlenden Updates erhalten möchten, deaktivieren Sie das Kontrollkästchen neben **Betriebssystem-Updates**.

Das Benachrichtigungsfenster enthält eine Übersicht der verfügbaren Updates für das macOS-Betriebssystem und für die Anwendungen, die über das native MacOS-Tool für Software-Updates aktualisiert werden. Sie können das Update direkt über das Benachrichtigungsfenster ausführen oder über die **Startseite** von ESET Endpoint Security for macOS, indem Sie hier auf **Fehlendes Update installieren** klicken.

Das Benachrichtigungsfenster enthält den Anwendungsnamen, die Version, die Größe, Eigenschaften (Flags) und zusätzliche Informationen zu den verfügbaren Updates. Die **Flags**-Spalte enthält folgende Informationen:

- **[empfohlen]** - Der Hersteller des Betriebssystem empfiehlt die Installation dieses Updates, um die Sicherheit und Stabilität des Systems zu verbessern.
- **[Neustart]** - Nach der Installation ist ein Neustart des Computers erforderlich
- **[Herunterfahren]** - Der Computer muss heruntergefahren und nach der Installation wieder eingeschaltet werden

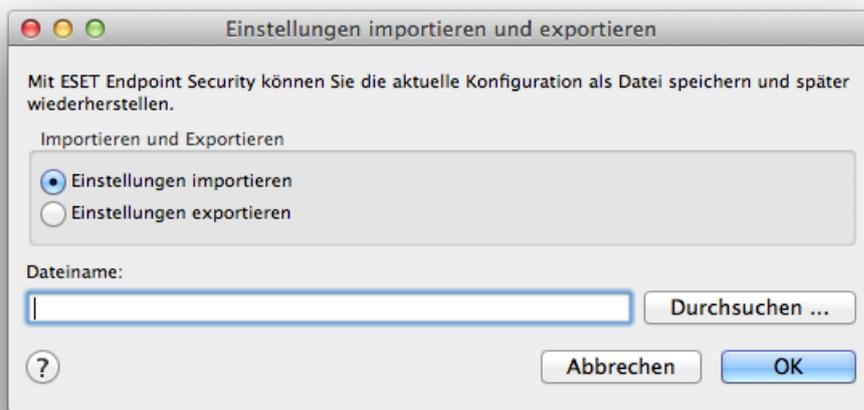
Das Benachrichtigungsfenster zeigt die vom Befehlszeilenwerkzeug 'softwareupdate' abgerufenen Updates an. Die von diesem Werkzeug abgerufenen Updates können sich von den in der Anwendung 'Software Updates' angezeigten Updates unterscheiden. Wenn Sie alle im Fenster 'Fehlende Systemupdates' angezeigten,

verfügbaren Updates installieren möchten, einschließlich der nicht in der Anwendung 'Software Updates' angezeigten Updates, verwenden Sie das Befehlszeilenwerkzeug 'softwareupdate'. Weitere Informationen zu diesem Werkzeug finden Sie im Handbuch zu 'softwareupdate', auf das Sie durch Eingabe des Befehls `man softwareupdate` in einem **Terminal**fenster zugreifen können. Wir empfehlen die Nutzung des Werkzeugs nur für fortgeschrittene Benutzer.

Einstellungen importieren/exportieren

Um eine vorhandene Konfiguration zu importieren oder die aktuelle Konfiguration von ESET Endpoint Security for macOS zu exportieren, klicken Sie auf **Einstellungen > Einstellungen importieren und exportieren**.

Diese Funktionen sind nützlich, wenn Sie die aktuelle Konfiguration von ESET Endpoint Security for macOS für eine spätere Verwendung sichern möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration von ESET Endpoint Security for macOS auf mehreren Systemen verwenden möchten. Sie können die Konfigurationsdatei einfach importieren, um ihre gewünschten Einstellungen zu übertragen.



Um eine Konfiguration zu importieren, wählen Sie **Einstellungen importieren** aus und klicken Sie auf **Durchsuchen**, um nach der zu importierenden Konfigurationsdatei zu suchen. Um eine Konfiguration zu exportieren, wählen Sie **Einstellungen exportieren** aus und navigieren Sie mit Ihrem Browser zu einem Speicherort auf Ihrem Computer, an dem die Konfigurationsdatei gespeichert werden soll.

Einstellungen für den Proxyserver

Sie können die Einstellungen für den Proxyserver unter **Einstellungen > Erweiterte Einstellungen > Proxyserver** konfigurieren. Durch Angabe eines Proxyserver auf dieser Ebene legen Sie globale Proxyserver-Einstellungen für alle Funktionen von ESET Endpoint Security for macOS fest. Die hier festgelegten Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen. ESET Endpoint Security for macOS unterstützt Basic Access- und NTLM (NT LAN Manager)-Authentifizierung.

Um die Proxy-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende IP-Adresse bzw. URL ein. Geben Sie dann im Feld „Port“ den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig (3128)). Wenn Sie auf **Erkennen** klicken, füllt das Programm beide Felder für Sie aus.

Wenn für die Kommunikation mit dem Proxyserver eine Authentifizierung erforderlich ist, geben Sie in den Feldern **Benutzername** und **Passwort** die entsprechenden Informationen ein.

Freigegebener lokaler Cache

Um die Verwendung des freigegebenen lokalen Cache zu aktivieren, klicken Sie auf „Einstellungen“ > „Erweiterte Einstellungen“ > „Freigegebener lokaler Cache“ und aktivieren Sie das Kontrollkästchen neben „Cache mit freigegebenem lokalen ESET-Cache aktivieren“. Diese Funktion steigert die Leistung in virtualisierten Umgebungen, indem doppelte Scans im Netzwerk vermieden werden. Somit wird jede Datei nur einmal gescannt und im gemeinsamen Cache gespeichert. Wenn die Funktion aktiviert ist, werden Informationen zu den gescannten Dateien und Ordnern im Netzwerk in einem lokalen Cache gespeichert. Bei der Durchführung eines neuen Scans sucht ESET Endpoint Security for macOS im Cache nach gescannten Dateien. Wenn übereinstimmende Dateien gefunden werden, werden diese vom Scannen ausgeschlossen.

Die Einstellungen für den freigegebenen lokalen Cache umfassen Folgendes:

- **Serveradresse** – Name oder IP-Adresse des Computers, auf dem sich der Cache befindet.
- **Port** – Portnummer für die Kommunikation (Standardwert: (3537)
- **Passwort** – Passwort für den freigegebenen lokalen Cache (optional)

Ausführliche Anweisungen

i Ausführliche Anweisungen zur Installation und Konfiguration des freigegebenen lokalen ESET-Cache finden Sie im [Benutzerhandbuch für den freigegebenen lokalen ESET-Cache](#). (Dieses Handbuch ist nur auf Englisch verfügbar.)

Endbenutzer-Lizenzvereinbarung

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND AKZEPTIEREN DIE [DATENSCHUTZERKLÄRUNG](#).**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, (im Folgenden "ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche "Ich stimme zu" oder "Ich stimme zu..." beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung nicht einverstanden sind, klicken Sie auf die Schaltfläche "Ablehnen" oder "Ich stimme nicht zu". Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. Software. Mit "Software" wird in dieser Vereinbarung bezeichnet: (i) das mit dieser Vereinbarung ausgelieferte Computerprogramm und all dessen Komponenten; (ii) alle Inhalte der Disks, CD-ROMs, DVDs, E-Mails und Anlagen oder sonstiger Medien, denen diese Vereinbarung beigelegt ist, einschließlich der Objektcodeform der Software, die auf einem Datenträger, in einer E-Mail oder durch Herunterladen im Internet bereitgestellt wurde; (iii) alle verwandten erklärenden Schriftdokumente und andere Dokumentationen in Bezug auf die Software, insbesondere Beschreibungen der Software und ihrer Spezifikationen, jede Beschreibung der Softwareeigenschaften oder -funktionen, Beschreibungen der Betriebsumgebung, in der die Software verwendet wird, Anweisungen zu Installation und zum Einsatz der Software ("Dokumentation"); (iv) Kopien der Software, Patches für mögliche Softwarefehler, Hinzufügungen zur Software, Erweiterungen der Software, geänderte Versionen und Aktualisierungen der Softwarebestandteile, sofern zutreffend, deren Nutzung der Anbieter gemäß Artikel 3 dieser Vereinbarung gewährt. Die Software wird ausschließlich in Form von ausführbarem Objektcode ausgeliefert.

2. Installation, Computer und ein Lizenzschlüssel. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. Lizenz. Unter der Voraussetzung, dass Sie dieser Vereinbarung zugestimmt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) Installation und Nutzung. Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) Anzahl der Lizenzen. Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem "Endbenutzer" ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; wenn der Umfang einer Lizenz sich nach der Anzahl von Postfächern richtet, ist ein Endbenutzer (ii) ein Computerbenutzer, der E-Mail über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer

der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Business Edition.** Für die Verwendung der Software auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** OEM-Software darf ausschließlich auf dem Computer genutzt werden, mit dem Sie sie erhalten haben. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz.** Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. **Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung.** Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Die Verbindung mit dem Internet und den entsprechenden Datenerfassungen ist für die folgenden Funktionen der Software erforderlich:

a) **Software-Updates.** Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) bereitzustellen, ist hierzu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzrichtlinie.

b) **Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter.** Die Software enthält Funktionen zur Erfassung neuer Computerviren und anderer schädlicher Computerprogramme sowie von verdächtigen, problematischen, potenziell unsicheren Objekten wie Dateien, URLs, IP-Pakete und Ethernet-Rahmen (im Folgenden "Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess und die Plattform, auf der die Software installiert ist, oder anderen Informationen über Betrieb und Funktionsweise der Software (im Folgenden "Informationen") an den Anbieter übertragen. Die Informationen und die Infiltrationen können Daten über den Endbenutzer oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist (inklusive zufällig oder unbeabsichtigt erfasste personenbezogene

Daten), sowie von eingedrungener Schadsoftware betroffene Dateien mit den entsprechenden Metadaten.

Die folgenden Funktionen der Software können Informationen und Infiltrationen sammeln:

- i. Das LiveGrid Reputationssystem sammelt und sendet Einweg-Hashes im Zusammenhang mit eingedrungener Schadsoftware an den Anbieter. Diese Funktion ist in den Standardeinstellungen der Software aktiviert.
- ii. Das LiveGrid-Reputationssystem erfasst Infiltrationen und überträgt diese zusammen mit den entsprechenden Metadaten und anderen Informationen an den Anbieter. Diese Funktion kann vom Endbenutzer bei der Installation der Software aktiviert werden.

Der Anbieter verwendet die erhaltenen Informationen und Infiltrationen ausschließlich zur Analyse und Erforschung der Infiltrationen, zur Verbesserung der Software und zur Überprüfung der Echtheit von Lizenzen und unternimmt angemessene Anstrengungen, um die erhaltenen Infiltrationen und Informationen zu schützen. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzrichtlinie und gemäß geltender Gesetze Infiltrationen und Informationen erfassen und verarbeiten. Sie können diese Funktionen jederzeit deaktivieren.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbieters übertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist. Sie stimmen dem Empfang von Benachrichtigungen und Nachrichten zu, inklusive, jedoch nicht ausschließlich, Marketinginformationen.

Details zur Privatsphäre, zum Schutz persönlicher Daten und zu Ihren Rechten als betroffene Person finden Sie in der Datenschutzrichtlinie auf der Webseite des Anbieters oder direkt beim Installationsprozess. Sie finden diese Informationen außerdem im Hilfebereich der Software.

5. Ausübung der Rechte des Endbenutzers. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Sie dürfen die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz der Computer verwenden, für die Sie eine Lizenz erworben haben.

6. Beschränkungen der Rechte. Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.

g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. Urheberrecht. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompiieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. Rechtevorbehalt. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. Beginn und Gültigkeitsdauer der Vereinbarung. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten

zurückgeben. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEDWEGE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. Keine weiteren Verpflichtungen. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. HAFTUNGSAUSSCHLUSS. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEDWEGE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. Technischer Support. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. Übertragung der Lizenz. Die Software darf von einem Computersystem auf ein anderes übertragen werden, sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software

zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. Gültigkeitsnachweis für die Softwarelizenz. Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. Lizenzvergabe an Behörden und die US-Regierung. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. Einhaltung von Handelskontrollen.

a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen (im Folgenden „angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Exportkontrollgesetze“)

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Sanktionsgesetze“).

b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19.a dieser Vereinbarung verletzt hat oder vermutlich verletzen wird; oder

ii. ein Endbenutzer und/oder die Software fällt unter die Handelskontrollgesetze, und ESET ist nach eigenem Ermessen der Ansicht, dass die weitere Erfüllung der Verpflichtungen aus der Vereinbarung dazu führen könnte, dass ESET oder ein angeschlossenes Unternehmen die Handelskontrollgesetze verletzt oder dass sonstige negative Folgen zu erwarten sind.

c) Die Vereinbarung ist nicht darauf ausgelegt und darf nicht so interpretiert oder ausgelegt werden, dass eine der Parteien dazu aufgefordert oder verpflichtet wird, auf irgendeine Weise zu handeln oder Handlungen zu

unterlassen (oder Handlungen bzw. deren Unterlassung zuzustimmen), die geltende Handelskontrollgesetze verletzt oder gemäß dieser Gesetze unter Strafe steht oder verboten ist.

20. Kündigungen. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. Geltendes Recht, Gerichtsstand. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. Allgemeine Bestimmungen. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Bei Widersprüchen zwischen übersetzten Versionen dieser Vereinbarung hat die englische Version Vorrang. Änderungen an dieser Vereinbarung bedürfen der Schriftform und müssen von einem bevollmächtigten Vertreter des Anbieters unterzeichnet werden.

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

ESET, spol. s r. o., mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slowakei, eingetragen im Handelsregister Bratislava I, Abschnitt Sro, Eintragsnummer 3586/B, Firmenregisternummer 31333532 als Datenverarbeiter („ESET“ oder „Wir“) hat das Ziel, die persönlichen Daten und die Privatsphäre seiner Kunden transparent zu behandeln. Daher veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endkunde“ oder „Sie“) über die folgenden Themen zu informieren:

- Verarbeitung persönlicher Daten,
- Vertraulichkeit der Daten,
- Rechte betroffener Personen.

Verarbeitung persönlicher Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden unter den Bestimmungen der Endbenutzer-Lizenzvereinbarung („EULA“) bereitgestellt. Einige dieser Dienste erfordern jedoch möglicherweise zusätzliche Aufmerksamkeit. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Produktdokumentation beschriebene Dienste an, darunter die Upgrade- und Updatedienste, ESET LiveGrid®, den Schutz vor dem Missbrauch von Daten, Support usw. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

- Update- und sonstige Statistiken und Informationen zum Installationsprozess und Ihrem Computer, z. B. die Plattform, auf der unser Produkt installiert wird, oder Informationen zum Betrieb und Funktionsumfang unserer Produkte wie Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse

und Konfigurationseinstellungen des Produkts.

- Einweg-Hashes für Schadsoftware als Teil unseres LiveGrid®-Reputationssystems, das die Wirksamkeit der Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.
- Verdächtige Samples und Metadaten „aus freier Wildbahn“ als Teil unseres ESET LiveGrid®-Reputationssystems, mit denen ESET unmittelbar auf die Anforderungen unserer Kunden reagieren und sie vor den neuesten Bedrohungen schützen kann. Wir benötigen die folgenden Daten von Ihnen:

O Eingedrungene Schadsoftware, z. B. potenzielle Sample von Viren und anderen Schadprogrammen, sowie verdächtige, problematische, potenziell unerwünschte oder potenziell unsichere Objekte wie ausführbare Dateien oder E-Mail-Nachrichten, die von Ihnen als Spam markiert oder von unserem Produkt markiert wurden;

O Informationen zu Geräten im lokalen Netzwerk wie Art, Hersteller, Modell und/oder Name des Geräts;

O Informationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;

O Absturzabbilder und darin enthaltenen Informationen.

Wir haben kein Interesse daran, Daten außerhalb des genannten Umfangs zu erfassen, allerdings lässt sich dies manchmal nicht vermeiden. Versehentlich erfasste Daten können in der Schadsoftware (ohne Ihr Wissen oder Ihre Zustimmung erfasst) oder als Teil von Dateinamen oder URLs enthalten sein. Es ist nicht unsere Absicht, diese Daten in unseren Systemen oder für die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

- Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.
- Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.

Vertraulichkeit der Daten

ESET ist ein weltweit operierendes Unternehmen über angeschlossene Unternehmen oder Partner im Rahmen unseres Distributions-, Dienst- und Supportnetzwerks. Die von ESET verarbeiteten Informationen können zur Erbringung der EULA von und zu angeschlossenen Unternehmen übertragen werden, beispielsweise für die Bereitstellung von Diensten, Supportleistungen oder Abrechnungen. Je nach Ihrem Standort und den von Ihnen ausgewählten Diensten müssen wir Ihre Daten unter Umständen in Länder ohne Gleichstellungsbeschluss der Europäischen Kommission übertragen. Selbst in diesem Fall unterliegen alle Datenübertragungen den Datenschutzbestimmungen und finden nur bei Bedarf statt. Übliche Vertragsklauseln, bindende Unternehmensregeln oder andere geeignete Mechanismen müssen ausnahmslos umgesetzt werden.

Wir unternehmen größte Anstrengungen, um zu verhindern, dass Ihre Daten bei der Bereitstellung von Diensten im Rahmen der EULA länger als notwendig gespeichert werden. Unser Aufbewahrungszeitraum ist unter Umständen länger als die Gültigkeitsdauer Ihrer Lizenz, um Ihnen eine problemlose und komfortable Erneuerung zu ermöglichen. Minimierte und pseudonymisierte Statistiken und sonstige Daten aus ESET LiveGrid® können zu statistischen Zwecken weiterverarbeitet werden.

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Falls jedoch Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sind, müssen wir die Aufsichtsbehörden sowie die betroffenen Personen informieren. Betroffene Personen haben das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

Rechte betroffener Personen

ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Im Rahmen der geltenden Datenschutzgesetze haben Sie als betroffene Person die folgenden Rechte:

- das Recht, Ihre persönlichen Daten von ESET anzufordern,
- das Recht, Ihre persönlichen Daten bei Bedarf zu berichtigen (Sie haben auch das Recht, unvollständige persönliche Daten zu vervollständigen),
- das Recht, die Löschung Ihrer persönlichen Daten anzufordern,
- das Recht, eine Einschränkung der Verarbeitung Ihrer persönlichen Daten anzufordern,
- Einlegen von Einspruch gegen die Verarbeitung
- Einlegen von Beschwerden sowie
- das Recht auf Übertragbarkeit der Daten.

Falls Sie Ihre Rechte als betroffene Person in Anspruch nehmen möchten oder Fragen oder Bedenken haben, schicken Sie uns eine Nachricht an:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk