



**Bitdefender®**

**Endpoint Security for  
Mac**

**BENUTZERHANDBUCH**

## Endpoint Security for Mac Benutzerhandbuch

Veröffentlicht 2020.08.31

Copyright© 2020 Bitdefender

### Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuchs dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

**Warnung und Haftungsausschluss.** Dieses Produkt und die dazugehörige Dokumentation ist urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „wie besehen“ zur Verfügung gestellt und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere Webseiten, die nicht von Bitdefender erstellt wurden, und auch nicht von ihr kontrolliert werden können. Somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. Bitdefender stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass Bitdefender in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

**Warenzeichen.** Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

# Inhaltsverzeichnis

|  |     |
|--|-----|
| Zur Verwendung dieses Handbuchs .....              | v   |
| 1. Zielsetzung und Zielgruppe .....                | v   |
| 2. Über dieses Handbuch .....                      | v   |
| 3. Konventionen in diesem Handbuch .....           | vi  |
| 3.1. Typografie .....                              | vi  |
| 3.2. Symbole .....                                 | vi  |
| 4. Ihre Mithilfe .....                             | vii |
| 1. Erste Schritte .....                            | 1   |
| 1.1. Über Endpoint Security for Mac .....          | 1   |
| 1.2. Endpoint Security for Mac öffnen .....        | 1   |
| 1.3. Anwendung Hauptfenster .....                  | 2   |
| 1.4. Anwendungssymbol Dock .....                   | 4   |
| 2. Schutz vor Malware .....                        | 5   |
| 2.1. Empfohlene Vorgehensweisen .....              | 5   |
| 2.2. Ihren Mac scannen .....                       | 5   |
| 2.3. Scan-Assistent .....                          | 6   |
| 2.4. Alle beheben .....                            | 7   |
| 2.5. Quarantäne .....                              | 9   |
| 2.6. Inhalts-Steuerung .....                       | 10  |
| 2.7. Gerätesteuerung .....                         | 11  |
| 2.8. Internet-Schutz .....                         | 12  |
| 2.9. Updates .....                                 | 13  |
| 2.9.1. Benutzergesteuertes Update .....            | 14  |
| 2.9.2. Updates über einen Proxy Server .....       | 14  |
| 2.9.3. Aktualisieren auf eine neue Version .....   | 14  |
| 3. Verwenden der Verschlüsselung .....             | 16  |
| 3.1. Laufwerke verschlüsseln .....                 | 16  |
| 3.2. Laufwerke entschlüsseln .....                 | 18  |
| 3.3. Ändern des Wiederherstellungsschlüssels ..... | 19  |
| 3.4. Ändern des Verschlüsselungspassworts .....    | 20  |
| 4. Präferenzen konfigurieren .....                 | 22  |
| 4.1. Zugriff auf Präferenzen .....                 | 22  |
| 4.2. Quarantäne .....                              | 22  |
| 4.3. Verlauf .....                                 | 23  |
| 4.4. Scanner-Einstellungen .....                   | 23  |
| 5. Verwenden des Befehlszeilentools .....          | 24  |
| 5.1. Unterstützte Befehle .....                    | 24  |
| 5.2. Der authToken-Parameter .....                 | 27  |
| 5.3. Fehlercodes .....                             | 27  |
| 6. Häufig gestellte Fragen .....                   | 29  |
| 7. Hilfe erhalten .....                            | 31  |



Arten von Bösartige Software ..... 32

## Zur Verwendung dieses Handbuchs

### 1. Zielsetzung und Zielgruppe

Diese Dokumentation richtet sich an Benutzer von **Endpoint Security for Mac**, einer Security for Endpoints-Client-Software, die Computer vor Malware und anderen Internet-Bedrohungen schützt. Die bereitgestellten Informationen sollten für jeden, der im Umgang mit Macintosh-Computern erfahren ist, leicht verständlich sein.

Sie lernen, wie Sie Endpoint Security for Mac konfigurieren und einsetzen, um sich vor Viren und anderer Schad-Software zu schützen. Sie erfahren, wie Sie alles aus Bitdefender herausholen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

### 2. Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

#### [Erste Schritte \(S. 1\)](#)

Starten mit Endpoint Security for Mac und der Benutzeroberfläche.

#### [Schutz vor Malware \(S. 5\)](#)

Lernen Sie, wie Sie Endpoint Security for Mac richtig einsetzen, um sich vor gefährlicher Software zu schützen

#### [Präferenzen konfigurieren \(S. 22\)](#)

Erfahren Sie mehr über die Einstellungen von Endpoint Security for Mac.

#### [Hilfe erhalten \(S. 31\)](#)

Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

## 3. Konventionen in diesem Handbuch

### 3.1. Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der untenstehenden Tabelle entnehmen.

| Erscheinungsbild   | Beschreibung   |
|--|--|
| Syntaxbeispiele  | Syntaxbeispiele werden in einer Schriftart mit fester Laufweite angegeben.           |
| <a href="http://www.bitdefender.de">http://www.bitdefender.de</a>                | Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.            |
| <a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a> | Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.                              |
| Zur Verwendung dieses Handbuchs (S. v)   | Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.           |
| Dateiname  | Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben. |
| <b>Option</b>  | Alle Produktoptionen werden <b>fett gedruckt</b> dargestellt.                        |
| <b>Stichwort</b>   | Wichtige Stichwörter oder Begriffe werden durch <b>Fettdruck</b> hervorgehoben.      |

### 3.2. Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



#### Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

**Wichtig**

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

**Warnung**

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

## 4. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse [documentation@bitdefender.com](mailto:documentation@bitdefender.com) kontaktieren. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

## 1. ERSTE SCHRITTE

Dieses Kapitel beinhaltet die folgenden Themen:

- [Über Endpoint Security for Mac](#)
- [Endpoint Security for Mac öffnen](#)
- [Anwendung Hauptfenster](#)
- [Anwendungssymbol Dock](#)

### 1.1. Über Endpoint Security for Mac

Endpoint Security for Mac ist ein vollautomatisches Programm für die Computer-Sicherheit, das von Ihrem Netzwerkadministrator per Fernzugriff verwaltet wird. Nach der Installation schützt es Sie vor allen Arten von Malware, einschließlich Viren, Spyware, Trojaner, Keylogger, Würmer und Adware. Es kann zudem zur Durchsetzung von Unternehmensrichtlinien für die Computer- und Internet-Nutzung eingesetzt werden.

Diese App entdeckt und entfernt nicht nur Mac-Malware sondern auch Windows-Malware und verhindert so, dass Sie infizierte Dateien versehentlich an die PCs Ihrer Familie, Freunde und Kollegen weiterleiten.

### 1.2. Endpoint Security for Mac öffnen

Sie haben verschiedene Möglichkeiten, Endpoint Security for Mac zu öffnen.

- Klicken Sie im Launchpad auf das "Endpoint Security for Mac"-Symbol.
- Öffnen Sie ein Finder-Fenster, wählen Sie **Anwendungen** und doppelklicken Sie auf das **"Endpoint Security for Mac"**-Symbol.
- Sie können die Anwendung auch mit Spotlight suchen und öffnen.

Beim Öffnen erkennt die Anwendung automatisch Ihre Systemsprache und zeigt die Benutzeroberfläche in der jeweiligen Sprache an.



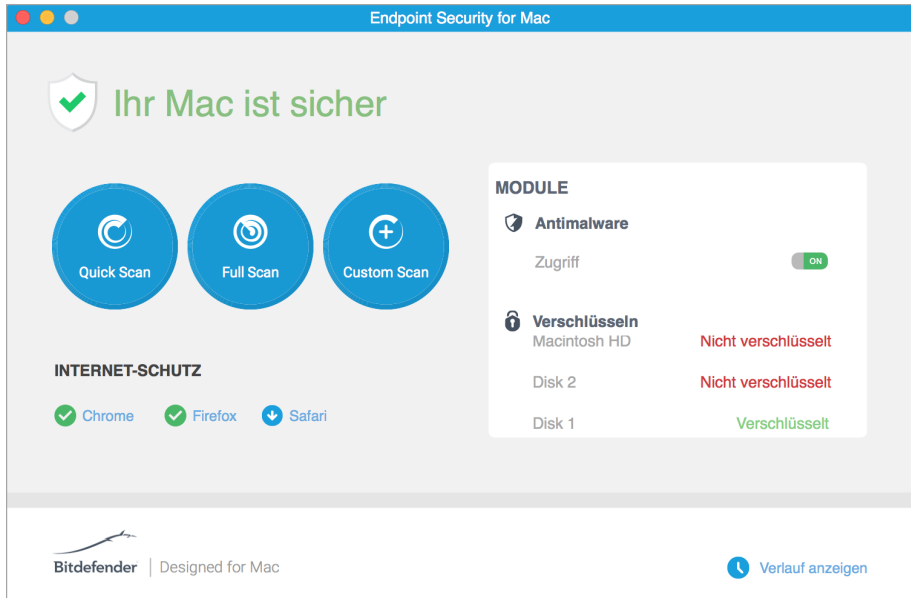
#### **Beachten Sie**

Falls Ihre Systemsprache nicht zu den in Endpoint Security for Mac unterstützten Sprachen gehört, wird standardmäßig die englische Benutzeroberfläche angezeigt.



## 1.3. Anwendung Hauptfenster

Im Hauptfenster der Anwendung können Sie wichtige Maßnahmen ergreifen, um Ihren Systemschutz zu verbessern. Hier können Sie den Sicherheitsstatus Ihres Computers einsehen und für mehr Sicherheit bei Surfen im Internet sorgen.



### Anwendung Hauptfenster

Die Statusleiste oben im Fenster informiert Sie mit eindeutigen Meldungen und Farbanzeigen über den Sicherheitsstatus des Systems.

- Grün - Keine Warnungen in Endpoint Security for Mac.
- Gelb - Es wurde ein Sicherheitsproblem gefunden.
- Rot - Die Lizenz ist abgelaufen.

Unterhalb des Statusbereiches finden Sie drei Scan-Schaltflächen, über die Sie Ihren Mac scannen können:

- **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Anwenders) auf Malware.

- **Full Scan (Vollständiger Scan)** - überprüft das gesamte System auf Malware. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.
- **Custom Scan (Benutzerdefinierter Scan)** - hilft Ihnen, bestimmte Dateien, Verzeichnisse etc. auf Malware zu überprüfen.

Weitere Informationen finden Sie unter [Ihren Mac scannen \(S. 5\)](#).

Neben den Scan-Schaltflächen finden Sie im Modulbereich die folgenden Informationen:

- **Malware-Schutz** – Informiert Sie, ob Zugriff-Scans aktiviert (An) oder deaktiviert (aus) ist.
- **Inhaltssteuerung** - hier erfahren Sie, ob die folgenden Komponenten aktiviert (An) oder deaktiviert (Aus) sind:
  - Datenverkehr-Scan
  - Anwendungs-Blacklist
  - Internet-Zugangssteuerung
  - Phishing-Schutz
- **Gerätesteuerung** - hier erfahren Sie, ob das Modul aktiviert (An) oder deaktiviert (Aus) ist.



### Beachten Sie

Die Module für die Inhaltssteuerung und die Gerätesteuerung sind ab OS X El Capitan (10.11) verfügbar. Für diese Funktionen ist eine macOS-Kernel-Erweiterung erforderlich. Die Installation von Kernel-Erweiterungen erfordert ab macOS High Sierra (10.13) Ihre Zustimmung.

- **Verschlüsselung** – hier können Sie den Verschlüsselungsstatus für jeden Datenträger (Verschlüsselt, Verschlüsselung wird durchgeführt, Entschlüsselt, Nicht verschlüsselt, Verriegelt oder Angehalten) einsehen, falls auf Ihrem Computer eine GravityZone-Verschlüsselungsrichtlinie angewendet wird.
- **EDR Sensor** - informs you if the EDR module is enabled (On) or disabled (Off).

Unter den Scan-Schaltflächen ist noch eine weitere Option verfügbar:

- **Internet-Schutz** - Filtert den Internet-Verkehr und blockiert alle schädlichen Inhalte, um Ihnen sicheres Surfen zu ermöglichen. Weitere Informationen finden Sie im Kapitel [Internet-Schutz \(S. 12\)](#).



### Beachten Sie

Der Internet-Schutz ist unter OS X Mavericks (10.9) und OS X Yosemite (10.10) verfügbar. Ab OS X El Capitan (10.11) wird diese Funktion durch die Inhaltssteuerung ersetzt.

Mit einem Klick auf **Verlauf anzeigen** unten im Fenster öffnen Sie ein ausführliches Ereignisprotokoll zu den Aktivitäten von Endpoint Security for Mac auf Ihrem Computer. Weitere Details finden Sie unter [Verlauf \(S. 23\)](#).

## 1.4. Anwendungssymbol Dock

Das "Endpoint Security for Mac"-Symbol wird sofort nach Öffnen der Anwendung im Dock angezeigt. Über das Symbol im Dock können Sie Dateien und Ordner schnell und einfach nach Malware scannen. Ziehen Sie die Datei oder den Ordner einfach per Drag und Drop auf das Symbol im Dock, um den Scan sofort zu starten.



Produktsymbol im Dock

## 2. SCHUTZ VOR MALWARE

Dieses Kapitel beinhaltet die folgenden Themen:

- [Empfohlene Vorgehensweisen](#)
- [Ihren Mac scannen](#)
- [Scan-Assistent](#)
- [Alle beheben](#)
- [Quarantäne](#)
- [Inhalts-Steuerung](#)
- [Gerätesteuerung](#)
- [Internet-Schutz](#)
- [Updates](#)

### 2.1. Empfohlene Vorgehensweisen

Um Ihr System frei von Malware zu halten und eine versehentliche Infizierung anderer Systeme zu verhindern, sollten Sie folgende Empfehlungen beachten:

- Überprüfen und beheben Sie die von Endpoint Security for Mac aufgelisteten Probleme regelmäßig. Detaillierte Informationen finden Sie unter [Alle beheben](#) (S. 7).
- Darüber hinaus sollten Sie folgende Empfehlungen berücksichtigen:
  - Sie sollten grundsätzlich alle Dateien scannen, die Sie von externen Speichern (z.B. USB-Sticks oder CDs) herunterladen, insbesondere wenn Ihnen die Quelle nicht bekannt ist.
  - Bei DMG-Dateien sollten diese zunächst gemountet und dann ihr Inhalt (die Dateien im gemounteten Volume/Image) gescannt werden.

### 2.2. Ihren Mac scannen

Das Modul für die Zugriff-Scans überwacht Ihren Computer kontinuierlich, um Malware-ähnliches Verhalten frühzeitig zu erkennen und zu verhindern, dass Malware auf Ihr System gelangt. Die Zugriff-Scans werden von Ihrem Netzwerkadministrator mithilfe von Sicherheitsrichtlinien gesteuert.

Sie können Ihren Mac und einzelne Dateien aber auch jederzeit selbst scannen. Dateien, Ordner und Volumes lassen sich bequem scannen, indem Sie sie per Drag & Drop auf das Dock-Symbol ziehen. Der Scan-Assistent wird angezeigt und leitet Sie durch den Scan-Vorgang.

So starten Sie einen Scan:

1. Öffnen Sie Endpoint Security for Mac.
2. Klicken Sie auf einen der drei Scan-Schaltflächen, um den gewünschten Scan zu starten.
  - **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Anwenders) auf Malware.
  - **Full Scan (Vollständiger Scan)** - überprüft das gesamte System auf Malware. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.

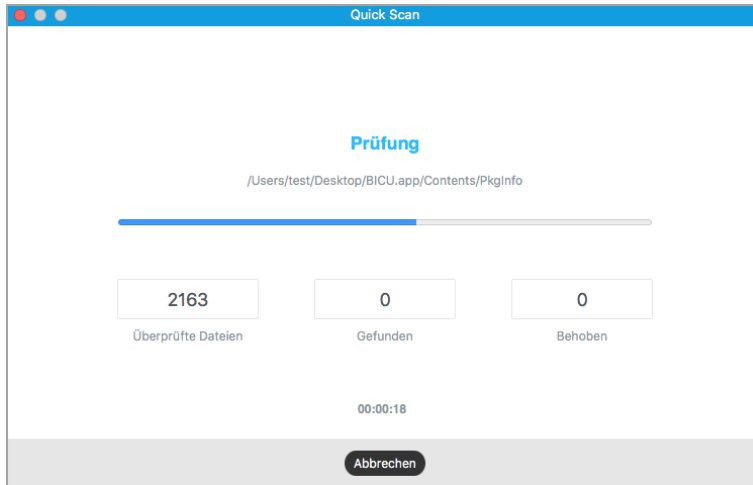


### Beachten Sie

- Je nach Größe Ihrer Festplatte kann ein vollständiger System-Scan einige Zeit in Anspruch nehmen (bis zu einer Stunde und mehr). Um die Systemleistung nicht zu beeinträchtigen, sollte diese Aufgabe nicht zeitgleich mit anderen ressourcenintensiven (z.B. Videobearbeitung) Aufgaben ausgeführt werden.
  - You can also run a quick scan or a full scan by using the **productConfigurationTool** [Verwenden des Befehlszeilentools \(S. 24\)](#).
- **Custom Scan (Benutzerdefinierter Scan)** - hilft Ihnen, bestimmte Dateien, Verzeichnisse etc. auf Malware zu überprüfen.

## 2.3. Scan-Assistent

Sobald Sie einen Scan starten, öffnet sich der Endpoint Security for Mac-Scan-Assistent.



Scan läuft...

Sie erhalten Echtzeitinformationen über den Scan, so zum Beispiel die Anzahl der erkannten Bedrohungen und die Anzahl der gelösten Probleme.

Warten Sie, bis Endpoint Security for Mac den Scan abgeschlossen hat.



### Beachten Sie

Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

## 2.4. Alle beheben

Endpoint Security for Mac spürt automatisch mögliche Probleme, die die Sicherheit Ihres Systems beeinflussen können, auf und informiert Sie.

Die erkannten Probleme könnten folgende Ursachen haben:

- Es wurden keine neuen Malware-Signaturen und Produkt-Updates von den Bitdefender-Servern heruntergeladen.
- Auf Ihrem System wurden Sicherheitsbedrohungen gefunden.
- Das Modul für die Zugriff-Scans wurde deaktiviert.
- Die Lizenz ist abgelaufen.

Die Probleme, die von Endpoint Security for Mac angezeigt werden, lassen sich schnell und bequem beheben. So können Sie alle Sicherheitsrisiken zügig neutralisieren.

Um erkannte Probleme zu überprüfen und zu beheben:

1. Öffnen Sie Endpoint Security for Mac.
2. Überprüfen Sie die Farbe des Statusbereichs:
  - Grün - Ihr Mac ist sicher.
  - Gelb oder rot - Auf Ihrem Mac sind Probleme aufgetreten. Die nächsten Schritte erläutern die weitere Vorgehensweise.
3. Überprüfen Sie die Beschreibung für weitere Informationen.
4. Je nach Anzahl und Schwere der gefundenen Probleme wird unter Umständen eine Schaltfläche im Statusbereich angezeigt:
  - **Problem beheben**, falls nur ein Problem gefunden wurde. Klicken Sie auf die Schaltfläche, um das Sicherheitsrisiko schnell zu neutralisieren.
  - **Probleme anzeigen**, falls mehrere Probleme gefunden wurden. Klicken Sie auf die Schaltfläche, um die Probleme anzuzeigen. Zur Problembehebung wird ein neues Fenster angezeigt.

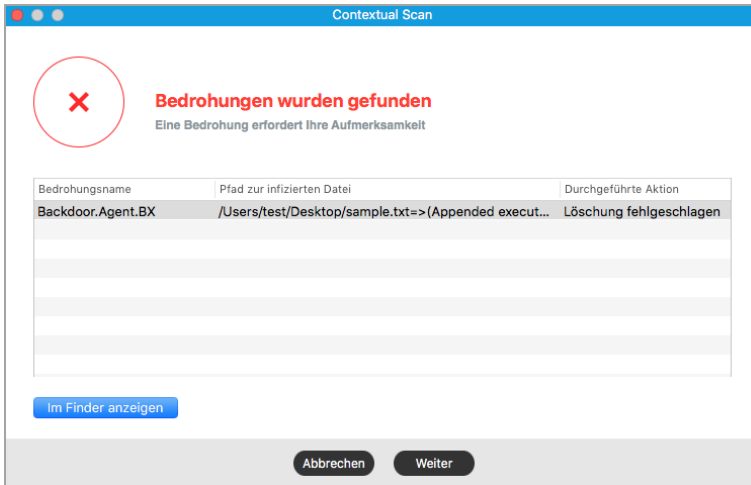
Falls Malware gefunden wurde, versucht die Anwendung automatisch, diese zu entfernen und die ursprüngliche Datei zu rekonstruieren. Dieser Vorgang wird als Desinfektion bezeichnet. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um die Infektion einzudämmen.

Falls die Datei weder desinfiziert noch in die Quarantäne verschoben werden kann, informiert Sie Endpoint Security for Mac über das Problem, damit Sie die Datei manuell löschen können.

So können Sie Infektionen manuell entfernen:

- Klicken Sie auf die Schaltfläche **Im Finder anzeigen**.
- Wählen Sie Datei aus und löschen Sie sie von Ihrem System.

Falls die Datei zu einer installierten Anwendung gehört, sollten Sie die Installation reparieren, damit das Programm wieder ordnungsgemäß funktioniert.



Fenster mit nicht beseitigten Bedrohungen

Einige Probleme müssen unter Umständen von Ihrem Netzwerkadministrator über die Management-Konsole behoben werden, so zum Beispiel:

- Aktivierung des Moduls für Zugriff-Scans über Sicherheitsrichtlinien.
- Verlängerung einer abgelaufenen Lizenz.

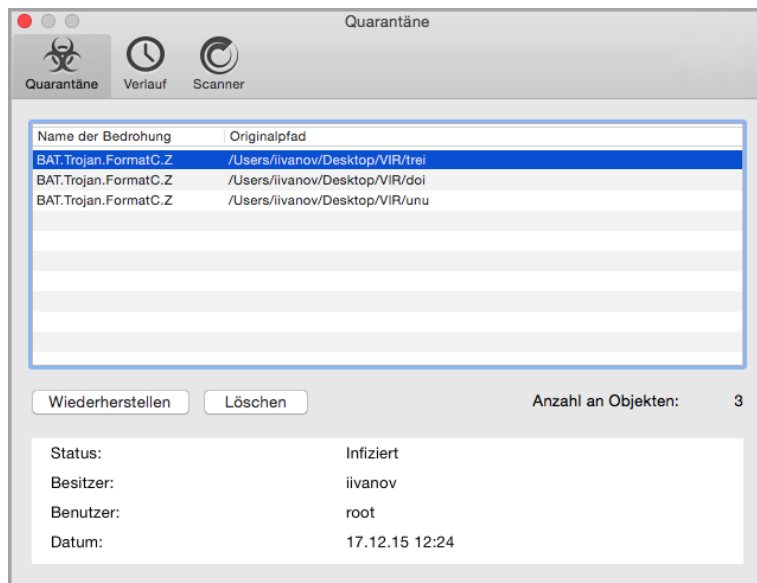
## 2.5. Quarantäne

Endpoint Security for Mac können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Schädliche Anwendungen, die in die Quarantäne verschoben wurden, können weder ausgeführt oder gelesen werden.

Öffnen Sie das **Quarantäne**-Fenster, um die Dateien in Quarantäne anzuzeigen und zu verwalten:

1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Menüleiste.
2. Klicken Sie in der Optionsliste auf **Einstellungen**. Ein neues Fenster öffnet sich.
3. Klicken Sie auf den Reiter **Quarantäne anzeigen**.





### Dateien in Quarantäne

Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden.

Um eine Datei aus der Quarantäne zu löschen, wählen Sie sie und klicken Sie auf **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

## 2.6. Inhalts-Steuerung

Beim Surfen im Netz schützt Sie die Inhaltssteuerung vor Phishing-Angriffen, Betrugsversuchen und unangemessenen Inhalten. Es umfasst zudem umfangreiche Optionen für die Benutzersteuerung, mit denen der Netzwerkadministrator Nutzungsrichtlinien für Computer und Internet durchsetzen kann. Dieses Modul ist verfügbar für Chrome, Firefox und Safari.

- **Datenverkehr-Scan.** Diese Komponente verhindert, dass Malware auf den Endpunkt heruntergeladen wird, indem der Internet-Datenverkehr in Echtzeit gescannt wird.

- **Anwendungs-Blacklist.** Diese Komponente verhindert, dass Mitarbeiter in Ihrem Unternehmen auf nicht autorisierte Anwendungen zugreifen können. Es steht in der Verantwortung des Administrators, Regeln für die im Unternehmen zugelassenen Anwendungen aufzustellen.
- **Internet-Zugangssteuerung.** Diese Komponente nutzt vom Administrator festgelegte Regeln, um zu verhindern, dass gefährliche Websites aufgerufen werden.
- **Phishing-Schutz.** Diese Komponente blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unwissentlich private oder vertrauliche Informationen an Online-Betrüger weitergeben.



### Beachten Sie

Die Inhaltssteuerung ist ab OS X El Capitan (10.11) verfügbar. Für diese Funktion ist eine macOS-Kernel-Erweiterung erforderlich. Die Installation von Kernel-Erweiterungen erfordert ab macOS High Sierra (10.13) Ihre Zustimmung. Sie erhalten eine Benachrichtigung, dass eine Systemerweiterung von Bitdefender blockiert wurde, und Sie werden aufgefordert, diese in den Einstellungen unter **Sicherheit & Datenschutz** zuzulassen. Solange Sie Ihre Zustimmung für die Bitdefender-Systemerweiterung nicht erteilt haben, funktioniert dieses Modul nicht und die Benutzeroberfläche von Endpoint Security for Mac zeigt ein kritisches Problem an, das Sie zur Zustimmung auffordert.

## 2.7. Gerätesteuerung

Das Modul **Gerätesteuerung** verhindert die unbeabsichtigte Weitergabe von sensiblen Daten sowie Malware-Infektionen über externe Geräte, die an den Endpunkt angeschlossen werden. Hierzu werden per Richtlinie Blockierungsregeln auf einer Vielzahl von Gerätetypen angewendet. Der Administrator ist für die Verwaltung der Berechtigungen für die folgenden Gerätetypen verantwortlich:

- Bluetooth-Geräte
- CD-ROM-Geräte
- Bildgebende Geräte
- Modems
- Windows Mobile
- Drucker
- Netzwerkadapter
- Drahtlosnetzwerkadapter
- Externe Speichermedien

### **i** Beachten Sie

Die Inhaltssteuerung ist ab OS X El Capitan (10.11) verfügbar. Für diese Funktion ist eine macOS-Kernel-Erweiterung erforderlich. Die Installation von Kernel-Erweiterungen erfordert ab macOS High Sierra (10.13) Ihre Zustimmung. Sie erhalten eine Benachrichtigung, dass eine Systemerweiterung von Bitdefender blockiert wurde, und Sie werden aufgefordert, diese in den Einstellungen unter **Sicherheit & Datenschutz** zuzulassen. Solange Sie Ihre Zustimmung für die Bitdefender-Systemerweiterung nicht erteilt haben, funktioniert dieses Modul nicht und die Benutzeroberfläche von Endpoint Security for Mac zeigt ein kritisches Problem an, das Sie zur Zustimmung auffordert.

## 2.8. Internet-Schutz

Endpoint Security for Mac nutzt die TrafficLight-Erweiterungen, um Ihnen sicheres Surfen im Internet zu ermöglichen. Die TrafficLight-Erweiterungen lesen, verarbeiten und filtern den gesamten Datenverkehr und blockieren dabei alle schädlichen Inhalte.

Die Erweiterungen lassen sich in die folgenden Browser integrieren: Mozilla Firefox, Google Chrome and Safari.

### **i** Beachten Sie

Diese Funktion ist unter OS X Mavericks (10.9) und OS X Yosemite (10.10) verfügbar. Ab OS X El Capitan (10.11) wird der Internet-Schutz durch die Inhaltssteuerung ersetzt.

Ihnen steht eine Reihe an Funktionen zur Verfügung, die Sie vor allen möglichen Bedrohungen im Internet schützen:

- Hochentwickelter Phishing-Filter - Verhindert, dass Sie Websites aufrufen, die für Phishing-Angriffe eingesetzt werden.
- Malware-Filter - Blockiert jede Art von Malware, mit der Sie im Internet in Kontakt kommen.
- Suchergebnisanalyse - Warnt Sie schon in Ihren Suchergebnissen vor gefährlichen Websites.
- Betrugsfilter - Schützt Sie im Internet vor betrügerischen Websites.
- Tracker-Warnung - Erkennt Tracker auf den Webseiten, die Sie besuchen, und schützt so Ihre Privatsphäre im Internet.




## Aktivierung von Linkchecker-Erweiterungen

Um die TrafficLight-Erweiterungen zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie Endpoint Security for Mac.
2. Klicken Sie auf **Jetzt lösen**, um das Fenster für den Internet-Schutz zu öffnen.
3. Endpoint Security for Mac erkennt automatisch, welche Web-Browser Sie auf Ihrem System installiert haben. Zur Installation der TrafficLight-Erweiterungen für den gewünschten Browser, klicken Sie im entsprechenden Bereich auf **Erweiterungen herunterladen**.
4. Sie werden an folgende Internet-Adresse weitergeleitet:  
<http://www.bitdefender.com/solutions/trafficlight.html>
5. Wählen Sie hier **Kostenloser Download**.
6. Folgen Sie den Anweisungen, um die TrafficLight-Erweiterung im ausgewählten Browser zu installieren.

## Seitenbewertung und Warnungen

Abhängig von der Linkchecker-Einstufung für die Webseite, die sie gerade besuchen, wird eines der folgenden Symbole in diesem Bereich eingeblendet:

-  Diese Seite ist sicher. Sie können Ihre Arbeit bedenkenlos fortsetzen.
-  Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen wollen.
-  Sie sollten diese Website umgehend verlassen. Alternativ können Sie sich für eine der verfügbaren Optionen entscheiden:
  - Die Website über einen Klick auf **Ich gehe lieber auf Nummer sicher** verlassen.
  - Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.

## 2.9. Updates

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Endpoint Security for Mac stets mit den neuesten Virensignaturen betreiben.

Solange die **Zugriff-Scans** aktiviert sind, werden Malware-Signaturen und Produkt-Updates automatisch auf Ihren Computer heruntergeladen. Falls Ihr Netzwerkadministrator die Zugriff-Scans über die Sicherheitsrichtlinien deaktivieren sollte, müssen Sie die Updates für Ihre Endpoint-Security-for-Mac-Installation manuell anfordern.

Die Aktualisierung der Malware-Signaturen wird "on the fly" durchgeführt. Das bedeutet, dass die entsprechenden Dateien stufenweise ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System zu keiner Zeit gefährdet.

### 2.9.1. Benutzergesteuertes Update

Ein manuelles Update können Sie jederzeit durchführen. Bevor Sie einen umfassenden Scan starten, empfehlen wir ein manuelles Update (Update by user request).

Für regelmäßige Updates und Downloads ist eine aktive Internetverbindung nötig.

Für ein manuelles Update:

1. Öffnen Sie Endpoint Security for Mac.
2. Klicken Sie auf **Aktionen** in der Menüleiste.
3. Klicken Sie auf **Virendatenbank aktualisieren**.

Der Update-Fortschritt und die downgeloadeten Dateien werden eingeblendet.

### 2.9.2. Updates über einen Proxy Server

Endpoint Security for Mac kann Updates über einen Proxy Server nur dann durchführen, wenn dafür keine Autorisierung notwendig ist. Sie müssen keine Programmeinstellungen konfigurieren.

Erfolgt Ihre Internetverbindung über einen Proxy Server, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um Updates zur Malware-Signaturen downloaden zu können.

### 2.9.3. Aktualisieren auf eine neue Version

Gelegentlich wird es Produktaktualisierungen geben, um die Produktfunktionen zu verbessern. Bei diesen Updates kann es notwendig werden, das System neu zu starten, um die Installation neuer Dateien zu ermöglichen. Falls ein Update einen Neustart erforderlich macht, wird Endpoint Security for Mac standardmäßig bis

zum Neustart des Systems die bereits vorhandenen Dateien nutzen. So beeinträchtigt der Aktualisierungsprozess Sie nicht in Ihrer Arbeit.

Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Fall Sie diese Benachrichtigung verpassen, können Sie das System manuell neu starten oder in der Menüleiste auf **Für das Upgrade neu starten** klicken.

## 3. VERWENDEN DER VERSCHLÜSSELUNG

Das Verschlüsselungsmodul ermöglicht eine vollständige Festplattenverschlüsselung auf Ihrem Mac durch Richtlinien, die von Ihrem Sicherheitsadministrator angewendet werden. Der Sicherheitsagent nutzt FileVault, um das Boot-Laufwerk des Mac zu verschlüsseln, und das Befehlszeilenprogramm diskutil, um alle Nicht-Boot-Laufwerke zu verschlüsseln. Wechseldatenträger werden nicht verschlüsselt.

Dieses Kapitel beinhaltet die folgenden Themen:

- [Laufwerke verschlüsseln](#)
- [Laufwerke entschlüsseln](#)
- [Ändern des Wiederherstellungsschlüssels](#)
- [Ändern des Verschlüsselungspassworts](#)

### 3.1. Laufwerke verschlüsseln

Gehen Sie wie folgt vor, wenn auf Ihrem Mac eine Verschlüsselungsrichtlinie zur Anwendung kommt:

- Boot-Laufwerke:
  1. Sie werden in einem neuen Fenster zur Eingabe des Systembenutzernamens und des Passworts aufgefordert.



Endpoint Security for Mac

### Mit FileVault verschlüsseln

Geben Sie Ihre Systemanmeldeinformationen ein, um das folgende Laufwerk zu verschlüsseln: Macintosh HD

User:

Password:

Jetzt nicht

2. Klicken Sie auf die Schaltfläche **OK**, um den Verschlüsselungsvorgang zu starten.

Wenn Sie die Option **Jetzt nicht** anklicken, wird der Verschlüsselungsprozess verschoben, aber das Fenster wird nach einiger Zeit erneut eingeblendet. Solange die Verschlüsselungsrichtlinie auf dem Mac aktiv ist, wird das Fenster immer wieder eingeblendet.

3. Folgendes passiert, nachdem das **Mit FileVault verschlüsseln**-Fenster geschlossen wird:
  - Auf Betriebssystemversion, die älter als macOS Catalina (10.15) sind, startet der Verschlüsselungsvorgang sofort.
  - Wenn Sie einen Mac mit macOS Catalina (10.15) verwenden, werden Sie von Endpoint Security for Mac ("fdesetup") in einem neuen Fenster aufgefordert, Ihre Zustimmung zur Aktivierung von FileVault zu geben. Klicken Sie auf die Schaltfläche **OK**, um den Verschlüsselungsvorgang zu starten. Wenn Sie auf **Nicht zulassen** klicken, startet Endpoint Security for Mac den Verschlüsselungsvorgang nicht und fordert Sie alle paar Minuten erneut auf, Ihre Zustimmung zu geben.



### Beachten Sie

Bei einem Dual-Boot-System wird das andere Boot-Laufwerk nicht verschlüsselt.

- Nicht-Boot-Laufwerke:
  1. Sie werden in einem neuen Fenster aufgefordert, ein eigenes Passwort für die Verschlüsselung jedes Laufwerks zu festzulegen. Dieses Passwort wird nur benötigt, um ein bestimmtes Nicht-Boot-Laufwerk zu entsperren.
  2. Klicken Sie auf den **Speichern**. Der Verschlüsselungsvorgang wird sofort gestartet.

Wenn Sie die Option **Verwerfen** anklicken, wird der Verschlüsselungsprozess verschoben. Das Dialogfenster wird nach einiger Zeit aber dennoch eingeblendet und wird immer wieder eingeblendet, solange die Verschlüsselungsrichtlinie auf dem Mac aktiv ist.



Endpoint Security for Mac

## Verschlüsselungspasswort festlegen

NonBoot

Passwort auswählen

Passwort wiederholen

Passwortanforderungen:

- ✘ Mindestens 8 und höchstens 30 Zeichen
- ✘ Sollte Groß- und Kleinbuchstaben enthalten
- ✘ Sollte eine Zahl enthalten

Dismiss **Speichern**

Wenn der Mac mehr als ein Laufwerk hat, erscheinen die Dialogfenster zur Verschlüsselung für alle Laufwerke gleichzeitig.

## 3.2. Laufwerke entschlüsseln

Gehen Sie wie folgt vor, wenn auf Ihrem Mac eine Entschlüsselungsrichtlinie zur Anwendung kommt:

- Boot-Laufwerke:
  1. Sie werden in einem Dialogfenster zur Eingabe des Systembenutzernamens und des Passworts aufgefordert.
  2. Klicken Sie auf **OK**. Der Entschlüsselungsvorgang wird sofort gestartet.
- Nicht-Boot-Laufwerke:
  1. Sie werden in einem Dialogfenster zur Eingabe des Verschlüsselungspassworts aufgefordert.
  2. Klicken Sie auf **Speichern**. Der Entschlüsselungsvorgang wird sofort gestartet.

Wenn Sie die Option **Verwerfen** anklicken, wird der Entschlüsselungsprozess verschoben. Das Dialogfenster wird nach einiger Zeit aber dennoch eingeblendet und wird immer wieder eingeblendet, solange die Verschlüsselungsrichtlinie auf dem Mac aktiv ist.

Wenn der Mac mehr als ein Laufwerk hat, erscheinen die Dialogfenster zur Entschlüsselung für alle Laufwerke gleichzeitig.

### 3.3. Ändern des Wiederherstellungsschlüssels

Nach dem Start des Verschlüsselungsvorgangs sendet Endpoint Security for Mac einen Wiederherstellungsschlüssel an die Verwaltungskonsole des Sicherheitsadministrators. Der Wiederherstellungsschlüssel ist für Ihren Sicherheitsadministrator nützlich, falls Sie Ihre Anmeldeinformationen oder die Verschlüsselungspasswörter vergessen und Sie die Laufwerke nicht mehr entsperren können, oder wenn der Mac von einem anderen Benutzer verwendet wird, der nicht auf eines der Laufwerke zugreifen kann.

Sie können den Wiederherstellungsschlüssel für das Boot-Laufwerk ändern, ohne dafür Ihre Anmeldedaten ändern zu müssen.

Gehen Sie folgendermaßen vor, um den Wiederherstellungsschlüssel für das Boot-Laufwerk zu ändern:

1. Klicken Sie im Hauptfenster von Endpoint Security for Mac auf den Namen des verschlüsselten Boot-Laufwerks.
2. Klicken Sie auf die Option **Wiederherstellungsschlüssel ändern**.
3. Geben Sie Ihren Systembenutzernamen und Ihr Passwort ein.
4. Klicken Sie auf den Button **Speichern**.

Endpoint Security for Mac

## Wiederherstellungsschlüssel ändern

Geben Sie Ihre Systemanmeldeinformationen an, um den Wiederherstellungsschlüssel für das folgende verschlüsselte Laufwerk zu ändern: Macintosh HD

User:

Password:

Abbrechen

Die Option zum Ändern des Wiederherstellungsschlüssels ist nur verfügbar, wenn eine Verschlüsselungsrichtlinie auf Ihrem Mac angewendet wird.

Wenn Sie das Systempasswort ändern, bleibt das verschlüsselte Boot-Laufwerk unverändert, ohne dass ein Eingreifen Ihrerseits erforderlich ist.

### 3.4. Ändern des Verschlüsselungspassworts

Sie können das Verschlüsselungspasswort für Nicht-Boot-Laufwerke über die Benutzeroberfläche von Endpoint Security for Mac ändern. Nach der Änderung des Passworts sendet Endpoint Security for Mac einen neuen Wiederherstellungsschlüssel an die Verwaltungskonsole des Sicherheitsadministrators.

Gehen Sie folgendermaßen vor, um das Verschlüsselungspasswort für Nicht-Boot-Laufwerke zu ändern:

1. Klicken Sie im Hauptfenster von Endpoint Security for Mac auf den Namen des verschlüsselten Datenträgers.
2. Klicken Sie auf **Passwort ändern**.
3. Legen Sie im Fenster **Verschlüsselungspasswort ändern** das neue Passwort fest.
4. Klicken Sie auf **Speichern**.

Endpoint Security for Mac

## Verschlüsselungspasswort ändern

NonBoot

Altes Passwort

Passwort auswählen

Passwort wiederholen

---

Passwortanforderungen:

- ✘ Mindestens 8 und höchstens 30 Zeichen
- ✘ Sollte Groß- und Kleinbuchstaben enthalten
- ✘ Sollte eine Zahl enthalten

Dismiss

Die Option zum Ändern des Verschlüsselungspasswort ist nur verfügbar, wenn eine Verschlüsselungsrichtlinie auf Ihrem Mac angewendet wird.

## 4. PRÄFERENZEN KONFIGURIEREN

Mit Endpoint Security for Mac können Endbenutzer nur einige wenige Optionen konfigurieren, da die Lösung vom Netzwerkadministrator über die zugewiesene Richtlinie verwaltet wird.

Dieses Kapitel beinhaltet die folgenden Themen:

- [Zugriff auf Präferenzen](#)
- [Quarantäne](#)
- [Verlauf](#)
- [Scanner-Einstellungen](#)

### 4.1. Zugriff auf Präferenzen

So öffnen Sie das Fenster für die **Einstellungen**:

1. Öffnen Sie Endpoint Security for Mac.
2. Wählen Sie eine der folgenden Methoden:
  - Klicken Sie im Anwendungsmenü auf Endpoint Security for Mac und wählen Sie danach **Einstellungen** aus.
  - Klicken Sie mit rechts auf das Bitdefender-Symbol im Statusmenü und wählen Sie **Einstellungen** aus.
  - Drücken Sie Befehl-Komma (,).
3. Klicken Sie auf den Reiter für die Funktion, die Sie konfigurieren möchten. Nähere Informationen dazu finden Sie in dieser Dokumentation.

### 4.2. Quarantäne

Der Quarantänebereich zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner auf Ihrem lokalen Computer befinden.

Um eine Datei in Quarantäne zu löschen, wählen Sie sie aus und klicken Sie auf **Löschen**. Wenn Sie eine Datei in Quarantäne wieder an Ihrem ursprünglichen Speicherort wiederherstellen möchten, wählen Sie sie aus und klicken Sie auf **Wiederherstellen**.

## 4.3. Verlauf

Im detaillierten Ereignisprotokoll finden Sie alle Aktionen, die Endpoint Security for Mac auf Ihrem Computer durchgeführt hat. Alle Ereignisse, die sich auf die Sicherheit Ihres Systems oder Ihre Daten auswirken, werden als neue Nachricht in den Verlauf von Endpoint Security for Mac aufgenommen. Ereignisse haben einen hohen Stellenwert für die Überwachung und Verwaltung Ihrer Computersicherheit. So können Sie zum Beispiel bequem überprüfen, ob ein Update erfolgreich abgeschlossen wurden, ob Malware auf Ihrem Computer gefunden wurde usw.

Wenn Sie den Verlauf löschen möchten, klicken Sie auf **Verlauf löschen**. Über die **Kopieren**-Schaltfläche können Sie die entsprechenden Informationen in der Zwischenablage speichern.

## 4.4. Scanner-Einstellungen

Über dieses Fenster können Sie festlegen, ob Endpoint Security for Mac auch die Backup-Dateien scannen soll. Die Anwendung kann Sie nur über eine bestehende Bedrohung informieren, da OS X Ihr Time-Machine-Laufwerk schützt und verhindert, dass Endpoint Security for Mac Dateien entfernt. Sollten dadurch infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt werden, wird Endpoint Security for Mac diese automatisch erkennen und entsprechend aktiv werden.

Die Backup-Dateien werden standardmäßig vom Scan ausgenommen. Deaktivieren Sie die Option **Time-Machine-Laufwerk nicht scannen**, um auch diesen Bereich zu scannen.

## 5. VERWENDEN DES BEFEHLSZEILENTOOLS

Mit Endpoint Security for Mac können Sie gewisse Aufgaben unter Verwendung des Befehlszeilentools **productConfigurationTool** ausführen. So können Sie zum Beispiel Informationen zum Produktstatus abrufen und schnelle oder vollständige Scans des Systems durchführen.

Gehen Sie zur Verwendung von **productConfigurationTool** folgendermaßen vor:

1. Öffnen Sie auf Ihrem Computer das **Terminal**.
2. Wechseln Sie das Arbeitsverzeichnis mit dem folgenden Befehl:

```
cd /Library/Bitdefender/AVP/enterprise.bundle/
```

3. Führen Sie unterstützte Befehle mit Administratorrechten aus (**sudo**-Befehl).

```
enterprise.bundle — -bash — 80x24
Last login: Fri Nov  3 15:58:02 on ttys000
MacBooks-pro:~ ██████$ cd /Library/Bitdefender/AVP/enterprise.bundle/
MacBooks-pro:enterprise.bundle ██████$ sudo ./productConfigurationTool -authToken ██████ -asksForStatus
Password:
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69754",
    "productVersion" : "4.0.0.176693",
    "lastUpdateTime" : 1509967463
  }
}
```

Verwenden von **productConfigurationTool** im Terminal

In diesem Kapitel finden Sie die folgenden Themen im Zusammenhang mit dem **productConfigurationTool**:

- [Unterstützte Befehle](#)
- [Der authToken-Parameter](#)
- [Fehlercodes](#)

### 5.1. Unterstützte Befehle

Die **productConfigurationTool**-Benutzeroberfläche unterstützt die folgenden Befehle:

### asksForStatus

Ruft die folgenden Informationen ab:

- Status des Malware-Schutz-Moduls (aktiviert oder deaktiviert).
- Version der Malware-Schutz-Signaturen.
- Produktversion.
- Zeitpunkt des letzten Updates.

Verwendungshinweise:

```
sudo ./productConfigurationTool -authToken [password]
-asksForStatus
```

Beispiel für die Ausgabe falls erfolgreich:

```
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69440",
    "productVersion" : "4.0.0.175873",
    "lastUpdateTime" : 1507185205
  }
}
```

Beispiel für die Ausgabe falls nicht erfolgreich:

```
"error" : 100
```

### asksForAScanToRun

Startet eine Scan-Aufgabe und liefert nach Abschluss Einzelheiten zum Prozess: Gesamtzahl der gescannten Objekte, Scan-Dauer, Protokollpfad und Angaben zu gefundenen Infektionen.

Auf diesen Befehl folgt ein für jeden Scan-Aufgabentyp vordefinierter Bezeichner:

- **Quick Scan** (ID: da29f7c8-23b1-4974-8d11-209959ac694b) – Diese Aufgabe ist für grundlegende Sicherheit und geringen Ressourcenverbrauch konfiguriert. Die Hauptziele des Scans sind laufende Prozesse und eine



Reihe anfälliger Speicherorte. Es kann jeweils nur eine Instanz dieser Aufgabe ausgeführt werden.

Gehen Sie folgendermaßen vor, um einen Quick Scan durchzuführen:

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
da29f7c8-23b1-4974-8d11-209959ac694b
```

- **Full Scan** (ID: dcf483c4-26d0-4e6f-ba28-6a53a00adae1) – Diese Aufgabe ist für maximalen Schutz vor jedem Malware-Typ konfiguriert. Es kann jeweils nur eine Instanz dieser Aufgabe ausgeführt werden.

Gehen Sie folgendermaßen vor, um einen vollständigen Scan durchzuführen:

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
dcf483c4-26d0-4e6f-ba28-6a53a00adae1
```

Beispiel für die Ausgabe falls der Befehl `asksForAScanToRun` erfolgreich ausgeführt wurde:

```
{  
  "error" : 0,  
  "stdout" : {  
    "scanDuration" : 13,  
    "logfilepath" : "\\Library\\Application Support\\  
      /Antivirus for Mac\\Logs\\  
      /da29f7c8-23b1-4974-8d11-209959ac694b.xml",  
    "totalScanned" : 6158,  
    "infection" : "NO"  
  }  
}
```

Beispiel für die Ausgabe falls nicht erfolgreich:

```
"error" : 95
```



### Beachten Sie

- Sie können mit **productConfigurationTool** keinen benutzerdefinierten Scan durchführen.
- Manche Scan-Aufgaben können einige Zeit in Anspruch nehmen. So kann ein vollständiger Scan zum Beispiel über 20 Minuten andauern.

## 5.2. Der authToken-Parameter

Dieser Parameter verhindert die nicht autorisierte Nutzung von **productConfigurationTool**. Er muss bei jeder Befehlsausführung verwendet werden.



### Beachten Sie

Als vorübergehende Maßnahme erfordert der Parameter `authToken` ein Passwort. Dieses erhalten Sie vom Bitdefender Business Support.

## 5.3. Fehlercodes

Die Benutzeroberfläche von **productConfigurationTool** gibt unter Umständen die folgenden Fehlercodes zurück:

| Fehler | Beschreibung   |
|--------|--|
| 100    | Die <b>productConfigurationTool</b> -Parameter sind <b>nicht korrekt</b> .   |
| 99     | Das Tool wird nicht mit Administratorrechten ausgeführt.   |
| 98     | <code>"/Library/Bitdefender/AVP/enterprise.bundle/epsdk.dylib"</code> nicht gefunden. Aktualisieren Sie das Produkt.   |
| 97     | Die Funktionstypen <code>f_EPSDK_GetInstance</code> und <code>f_EPSDK_ReleaseInstance</code> konnten nicht aus der Bibliothek geladen werden. Aktualisieren Sie das Produkt.   |
| 96     | Bei der <code>.json</code> -Antwort fehlen einige erwartete Felder oder sie hat ein nicht erwartetes Format. Aktualisieren Sie das Produkt.  |
| 95     | Eine bestimmte Abfrage benötigt Ereignisse, um alle relevanten Daten abzurufen, es wurden aber nicht alle Ereignisse gefunden. Aktualisieren Sie das Produkt. Sollte der Fehler weiterhin bestehen, wenden Sie sich an den Bitdefender Business Support. |



| Fehler | Beschreibung   |
|--------|--|
| 94     | <code>"/Library/Bitdefender/AVP/EndpointSecurityforMac.app/Contents/Info.plist"</code> wurde nicht gefunden oder <code>"CFBundleVersion"</code> wurde in der <code>.plist</code> -Datei nicht gefunden. Aktualisieren Sie das Produkt. |
| 93     | <b>productConfigurationTool</b> wird in dieser Version von Endpoint Security for Mac nicht unterstützt. Aktualisieren Sie das Produkt.   |
| 92     | Das angegebene <code>authToken</code> -Passwort stimmt nicht mit dem erwarteten Wert überein.  |
| 0      | Der Befehl wurde erfolgreich ausgeführt.   |

## 6. HÄUFIG GESTELLTE FRAGEN

**Das Scan-Protokoll zeigt noch nicht gelöste Probleme an. Wie kann ich diese beheben?**

Mögliche noch nicht gelöste Probleme im Scan-Protokoll sind zum Beispiel:

- Archive mit eingeschränktem Zugriff (rar, rar usw.)

**Lösung:** Lokalisieren Sie die Datei über die Option **Im Finder anzeigen** und löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.

- Postfächer mit eingeschränktem Zugriff (Thunderbird usw.)

**Lösung:** Entfernen Sie den Eintrag mit der infizierten Datei mithilfe der Anwendung.

- Dateien, die einem anderen Benutzer gehören

**Lösung:** Lokalisieren Sie die Datei über die Option **Im Finder anzeigen** und fragen Sie den Besitzer, ob diese Datei gefahrlos entfernt werden kann. Ist dies gefahrlos möglich, löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.



### **Beachten Sie**

Dateien mit beschränktem Zugriff sind Dateien, die Endpoint Security for Mac zwar öffnen, aber nicht bearbeiten kann.



**Kann ich Endpoint Security for Mac über einen Proxy-Server aktualisieren?**

Endpoint Security for Mac kann nur über Proxy-Server aktualisiert werden, bei denen keine Authentifizierung erforderlich ist. Sie müssen dafür keine Programmeinstellungen konfigurieren.

Erfolgt Ihre Internetverbindung über einen Proxy Server, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um Updates zur Malware-Signaturen downloaden zu können.

**Wie entferne ich die TrafficLight-Erweiterungen aus meinem Browser?**

- Um die TrafficLight-Erweiterungen aus Mozilla Firefox zu entfernen, gehen Sie folgendermaßen vor:
  1. Öffnen Sie den Firefox-Browser.
  2. Klicken Sie auf **Tools** und danach auf **Add-ons**.

3. Klicken Sie in der Spalte links auf **Erweiterungen**.
  4. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
  5. Starten Sie den Browser neu, um den Entfernungsvorgang abzuschließen.
- Um die TrafficLight-Erweiterungen aus Google Chrome zu entfernen, gehen Sie folgendermaßen vor:
    1. Öffnen Sie Ihren Chrome-Browser.
    2. Klicken Sie in der Browser-Symboleiste auf .
    3. Klicken Sie auf **Tools** und danach auf **Erweiterungen**.
    4. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
    5. Klicken Sie auf **Deinstallieren**, um den Entfernungsvorgang zu bestätigen.
  - Um Bitdefender TrafficLight aus Safari zu entfernen, gehen Sie folgendermaßen vor:
    1. Öffnen Sie Ihren Safari-Browser.
    2. Klicken Sie in der Browser-Symboleiste auf  und danach auf **Einstellungen**.
    3. Wählen Sie den Reiter **Erweiterungen** aus und suchen Sie in der Liste die Erweiterung **Bitdefender TrafficLight auf Safari**.
    4. Wählen Sie die Erweiterung aus und klicken Sie auf **Deinstallieren**.
    5. Klicken Sie auf **Deinstallieren**, um den Entfernungsvorgang zu bestätigen.

## 7. HILFE ERHALTEN

Bei Problemen und Fragen zu Endpoint Security for Mac wenden Sie sich bitte an Ihren Netzwerkadministrator.

Für Produkt- und Kontaktdaten öffnen Sie das Fenster **Über Endpoint Security for Mac**.

1. Öffnen Sie Endpoint Security for Mac.
2. Klicken Sie in der Menüleiste auf **Endpoint Security for Mac**.
3. Wählen Sie **Über Endpoint Security for Mac** .

## Arten von Bösertige Software

### Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

### Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind nicht grundsätzlich als schädlich anzusehen. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen vorsätzlich als kriminelles Mittel eingesetzt (um beispielsweise private Daten wie Anmeldedaten oder Kreditkartendaten zu sammeln).

### Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

### Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Software-Tools die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem

zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

## Spyware

Software, die unentdeckt vom Nutzer Anwenderdaten über seine Internetverbindung sammelt und abrufen. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes besteht Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

## Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert. Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten



Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

### **Virus**

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt. Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein. Die meisten Viren können sich selber vervielfältigen. Alle Computerviren sind von Menschenhand geschrieben. Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben. Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

### **Wurm**

Ein Programm, das sich über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.