Handbuch für Symantec™ Endpoint Protection 14.3 RU1 für Mac-Client

November 2020

Wie Symantec Endpoint Protection den Mac schützt

Symantec Endpoint Protection schützt mit einer Kombination verschiedener Schutzschichten vor Viren und Spyware sowie vor Angriffsversuchen.

Schutztypen beschreibt jede Schutzschicht.

Table 1: Schutztypen

Schutz	Beschreibung
Viren- und Spyware-Schutz	Symantec Endpoint Protection enthält geplante Virenscans, vom Administrator angeforderte Scans sowie Auto-Protect, eine Funktion die den Computer im Hintergrund auf Viren überwacht. Wird ein Virus erkannt, wird dieser von Symantec Endpoint Protection beseitigt. Funktionsweise des Viren- und Spyware-Schutzes
Netzwerkbedrohungsschutz	Symantec Endpoint Protection fängt die Daten in der Netzwerkschicht ab. Signaturen werden zum Scannen von Paketen bzw. Paketströmen verwendet. Jedes Paket wird einzeln gescannt, indem nach Mustern gesucht wird, die Netzwerk- oder Browser-Angriffen entsprechen. Der Netzwerkbedrohungsschutz enthält Folgendes: • Angriffsschutz erkennt Angriffe auf Betriebssystemkomponenten und der Anwendungsschicht. Symantec Endpoint Protection blockiert erkannte Netzwerkbedrohungen. • Firewall, die Netzwerkverkehr anhand von Firewall-Richtlinien und -Regeln zulässt oder blockiert. (Ab Version 14.2.) Funktionsweise des Netzwerkbedrohungsschutzes für Mac
Gerätesteuerung	Symantec Endpoint Protection Manager-Administratoren konfigurieren eine Gerätesteuerungsrichtlinie. Geräte können mit dieser Richtlinie durch Gerätenamen, Geräthändler, Gerätemodell oder Seriennummer blockiert werden oder die Blockierung kann aufgehoben werden. Auf einem verwalteten Client können Sie die Einstellungen für Gerätesteuerung auf der Registerkarte **Erweitert** anzeigen. Die Gerätesteuerung ist nicht für nicht verwaltete Clients verfügbar. Info zur Gerätesteuerung des Symantec Endpoint Protection-Clients für Mac
Endpoint Detection and Response	Symantec Endpoint Protection Manager-Administratoren konfigurieren eine Activity Recorder-Richtlinie, die es ermöglicht, verdächtige Netzwerkaktivitäten zu erkennen und aufzudecken.

Der Client lädt die Virendefinitionen, IPS-Definitionen und Produkt-Updates automatisch auf den Computer herunter.

Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware

Funktionsweise des Viren- und Spyware-Schutzes

Symantec Endpoint Protection verwendet Virendefinitionen, um bekannte Viren während geplanter Scans und manueller Scans zu erkennen. Auto-Protect verwendet Virendefinitionen, um Ihre Computeraktivität ständig zu scannen.

Symantec Endpoint Protection benachrichtigt Sie bei Erkennen eines Virus oder anderer Sicherheitsrisiken. Ein Virus oder ein anderes Sicherheitsrisiko wird in folgenden Fällen erkannt:

- Auto-Protect sucht während der Überwachung des Computers Viren.
- Auto-Protect sucht Viren in Scans, die von Ihnen geplant oder manuell gestartet wurden.

Anhand der Standardeinstellungen versucht Symantec Endpoint Protection automatisch, gefundene Viren zu beseitigen. Kann eine infizierte Datei nicht repariert werden, isoliert der Client die Datei, damit Sie den Computer nicht beschädigen

kann. Der Client führt diese Reparaturen i. d. R. ohne Eingreifen Ihrerseits aus. Wird ein Virus auf dem Computer gefunden, können Sie Informationen dazu an Symantec melden.

In bestimmten Fällen werden Sie gefragt, ob eine erkannte infizierte Datei repariert, gelöscht oder wiederhergestellt werden soll. Ihre Antwort bestimmt, welchen Vorgang der Client ausführt.

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Aktivieren bzw. Deaktivieren des Sendens von Sicherheitsinformationen an Symantec

Funktionsweise des Netzwerkbedrohungsschutzes für Mac

Der Netzwerkbedrohungsschutz enthält Folgendes:

- Angriffsschutz
- Firewall

Angriffsschutz

Angriffsschutz erkennt automatisch Netzwerkangriffe und blockiert diese. Der Angriffsschutz ist eine innere Verteidigungsschicht zum Schutz von Clientcomputern. Intrusion Prevention wird manchmal IPS (Intrusion Prevention-System) genannt.

Der Angriffsschutz fängt Daten in der Netzwerkschicht ab. Signaturen werden zum Scannen von Paketen bzw. Paketströmen verwendet. Jedes Paket wird einzeln gescannt, indem nach Mustern gesucht wird, die Netzwerk- oder Browser-Angriffen entsprechen. Angriffsschutz erkennt Angriffe auf Betriebssystemkomponenten und der Anwendungsschicht.

Der Angriffsschutz erkennt Angriffe auf Clientcomputern anhand von Signaturen. Bei bekannten Angriffe verwirft Intrusion Prevention automatisch die Pakete, die den Signaturen entsprechen.

Firewall

Die Firewall überwacht den Netzwerkverkehr und blockiert potenziell schädlichen Datenverkehr, um den Mac zu schützen. Für nicht verwaltete Clients ist die Symantec Endpoint Protection-Firewall nicht verfügbar.

Die Symantec Endpoint Protection-Firewall überwacht den Datenverkehr auf der Transport- und Internetschicht. Die integrierte macOS-Firewall überwacht den Datenverkehr in der höheren Anwendungsschicht, nachdem er von der Symantec Endpoint Protection-Firewall überwacht wurde. Daher können Sie beide Firewalls parallel ausführen.

Die Firewall verwendet folgende Arten von Regeln, um Netzwerkverkehr zuzulassen oder zu blockieren:

- Standardregeln
- Benutzerdefinierte Regeln
- Integrierte Regeln
- Schutzregeln

Zu diesen Regeln gehören Port-Scan-Erkennung, Denial-of-Service-Erkennung, Anti-MAC-Spoofing, Smart DHCP und Smart DNS. Die Firewall-Einstellungen werden vollständig vom Symantec Endpoint Protection Manager-Administrator gesteuert. Sie können die Firewall nur aktivieren oder deaktivieren, wenn der Administrator die Clientsteuerung durch Benutzer über den Mac zulässt.

Firewall-Schutz wurde in Version 14.2 hinzugefügt.

Verwalten von Intrusion Prevention

Verwalten des Firewall-Schutzes für den macOS-Client

Kompatibilität des Betriebssystems mit Symantec Endpoint Protection für Mac

Symantec Endpoint Protection für Mac unterstützt die folgenden Betriebssystemversionen:

- macOS 10.15 bis 10.15.5
- macOS 10.14
- macOS 10.13

Weitere Informationen zur Unterstützung älterer Mac-Betriebssystemversionen finden Sie unter Mac-Kompatibilität mit dem Endpoint Protection-Client.

Info zum Autorisieren von Kernel-Erweiterungen für Symantec Endpoint Protection für macOS 10.13 und höher

Versionshinweise, neue Fehlerbehebungen und Systemanforderungen für alle Versionen von Endpoint Protection

So installieren Sie den Symantec Endpoint Protection-Client für Mac

Sie können einen Symantec Endpoint Protection-Client direkt auf einem Mac installieren, wenn Sie Remote-Push nicht verwenden können oder möchten. Die Schritte sind bei verwalteten und nicht verwalteten Clients ähnlich.

Die einzige Möglichkeit zum Installieren eines verwalteten Client ist der Einsatz eines von Symantec Endpoint Protection Manager erstellten Pakets. Sie können einen nicht verwalteten Client jederzeit in einen verwalteten Client konvertieren, indem Sie die Clientserver-Kommunikationseinstellungen in den Mac-Client importieren.

> **NOTE**
> Um den Symantec Endpoint Protection-Client für Mac zur Verwendung mit Software zur Remote-Bereitstellung von anderen Herstellern zu konfigurieren, lesen Sie Exportieren und Bereitstellen eines Symantec Endpoint Protection-Clients über Apple Remote Desktop oder Casper.

Table 2: Methoden zur Installation des Mac-Clients

Wenn Sie die Installationsdatei heruntergeladen haben.	1. Extrahieren Sie den Inhalt in einen Ordner auf einem Mac-Computer, und öffnen Sie den Ordner. 2. Öffnen Sie `SEP_MAC`. 3. Kopieren Sie `Symantec Endpoint Protection.dmg` auf den Desktop des Mac-Computers. 4. Doppelklicken Sie auf `Symantec Endpoint Protection.dmg`, um die Datei als virtuellen Datenträger zu installieren. Dann installieren Sie den Symantec Endpoint Protection-Client für Mac.
Wenn Sie über ein Client-Installationspaket im Format .zip vom Broadcom Support Portalverfügen.	1. Kopieren Sie die Datei auf den Desktop des Mac-Computers. Die Datei wird `Symantec Endpoint Protection.zip` oder `Symantec_Endpoint_Protection_version_Mac_Client.zip` genannt, wobeiversiondie Produktversion ist. 2. Klicken Sie mit der rechten Maustaste auf "**Öffnen mit > Archivierungs-Dienstprogramm**", um den Inhalt der Datei zu extrahieren. 3. Öffnen Sie den resultierenden Ordner. Dann installieren Sie den Symantec Endpoint Protection-Client für Mac.

Das resultierende Image der virtuellen Festplatte bzw. der Ordner enthält das Installationsprogramm und den Ordner "Additional Resources". Beide Elemente müssen im selben Speicherort vorhanden sein. Wenn Sie das Installationsprogramm in einen anderen Speicherort kopieren, müssen Sie auch den Ordner "Additional Resources" kopieren.

So installieren Sie den Symantec Endpoint Protection-Client für Mac:

1. Doppelklicken Sie auf `Install Symantec Endpoint Protection`.
2. Um die Installation zu starten, klicken Sie auf **Install**.
3. Zum Installieren eines Hilfsprogramms, das für die Installation des Symantec Endpoint Protection-Clients erforderlich ist, geben Sie den Administrator-Benutzernamen und das Kennwort für den Mac-Computer ein, und klicken Sie dann auf **Install Helper**.
4. Klicken Sie nach der Installation auf **Continue**, um die Einrichtung Ihres Symantec Endpoint Protection-Clients abzuschließen.
5. Gehen Sie folgendermaßen vor, um Ihren Symantec Endpoint Protection-Client einzurichten:

Symantec Endpoint Protection-Systemerweiterung autorisieren	Klicken Sie im Dialogfeld **Security & Privacy** auf der Registerkarte **General** unter **System software from application "Symantec Endpoint Protection" was blocked from loading** auf **Allow**. Klicken Sie ggf. auf das Schlosssymbol, um die Änderungen vorzunehmen. Sie müssen die Systemerweiterung für Symantec Endpoint Protection autorisieren, damit sie ordnungsgemäß funktioniert. Info zum Autorisieren der Systemerweiterungen für Symantec Endpoint Protection für macOS 10.15 und höher
Vollständigen Datenträgerzugriff zulassen	Stellen Sie im Dialogfeld **Security & Privacy** auf der Registerkarte **Privacy** sicher, dass **Symantec System Extension** Zugriff auf Daten und Verwaltungseinstellungen für alle Benutzer auf Ihrem Mac-Gerät hat. Klicken Sie ggf. auf das Schlosssymbol, um die Änderungen vorzunehmen.
Änderungen am Netzwerkprofil zulassen	Wenn **Symantec Endpoint Protection would like to filter network content** in einem Dialogfeld angezeigt wird, klicken Sie auf **Allow**.

6. Klicken Sie auf **Complete**.

Info zum Autorisieren der Systemerweiterungen für Symantec Endpoint Protection für macOS 10.15 und höher

Die erforderliche Autorisierung von Systemerweiterungen ist eine neue Sicherheitsfunktion ab macOS 10.15.Sie müssen die Systemerweiterung für Symantec Endpoint Protection autorisieren, damit sie ordnungsgemäß funktioniert.

Um die Systemerweiterung für Symantec Endpoint Protection beim Einrichten des Symantec Endpoint Protection-Clients zu autorisieren, klicken Sie im Dialogfeld **Security & Privacy** auf der Registerkarte **General** unter **System software from application "Symantec Endpoint Protection"** auf **Allow**.

Installieren des Symantec Endpoint Protection-Clients für Mac

Upgradeaufforderung für den Symantec Endpoint Protection-Client für Mac

Symantec Endpoint Protection Manager-Administratoren können einem Clientinstallationspaket das automatische Upgrade der verwalteten Clientcomputer zuweisen, mit Einstellungen für die Clientinstallation.

Wenn Sie beim Mac eingeloggt sind, wird möglicherweise eine Aufforderung zum Neustart angezeigt, um die Installation abzuschließen. Je nach Clientinstallationseinstellung sind Sie möglicherweise in der Lage, den Neustart zu verschieben.

Wenn Sie nicht beim Mac eingeloggt sind, startet die Installation den Mac automatisch neu.

Erste Schritte mit dem Symantec Endpoint Protection-Client

Wenn Sie den Symantec Endpoint Protection-Client öffnen, wird oben die Meldung **You are Protected** angezeigt, es sei denn, es liegt ein Problem vor, das behoben werden muss. Klicken Sie auf **Beheben**, um etwaige Probleme zu beheben.

Der Symantec Endpoint Protection-Client zeigt die wichtigsten Aufgaben an, die Sie ausführen können.

Table 3: Seiten des Symantec Endpoint Protection-Clients

Option	Beschreibung
Sicherheit	Zeigt den Schutzstatus Ihres Computers an.
Scans	Ermöglicht es Ihnen, Ihren Computer zu scannen. Sie können einen schnellen oder vollständigen Scan ausführen. Sie können auch eine Datei oder einen Ordner angeben, die bzw. der gescannt werden soll. Ausführen eines manuellen Scans
LiveUpdate	Führt LiveUpdate aus, um die Definitionen und Produktdateien für Symantec Endpoint Protection zu aktualisieren. Sofortiges Aktualisieren des Content in Symantec Endpoint Protection
Erweitert	Enthält ausführlichere Optionen für Viren- und Spyware-Schutz, Netzwerkbedrohungsschutz und LiveUpdate.

Verwalten des Schutzes auf dem Mac mit Symantec Endpoint Protection

Die Standardeinstellungen in Symantec Endpoint Protection schützen den Mac vor verschiedener Malware. Entweder verarbeitet der Client die Malware automatisch, oder fordert Sie auf, die Vorgehensweise zu wählen.

Abhängig von den vom Administrator eingestellten Einstellungen , sollten Sie zum Aufrechterhalten des Schutzes folgende Aufgaben ausführen.

> **NOTE**
> Ihr Administrator hat Ihnen eventuell die entsprechenden Rechte nicht erteilt.

Table 4: Schützen des Computers

Schritte	Beschreibung
Schritt 1: Prüfen Sie, ob Viren- und Spyware-Schutz sowie Netzwerkbedrohungsschutz aktiviert sind.	Auf der Seite **Sicherheit** wird ein grünes Häkchen und die Meldung **You are Protected** angezeigt, wenn der Schutz aktiviert ist. Aktivieren und Deaktivieren des Viren- und Spyware-Schutzes Aktivieren bzw. Deaktivieren des Netzwerkbedrohungsschutzes
Schritt 2: Sorgen Sie dafür, dass Software und Definitionen auf dem neuesten Stand sind.	Auf der Seite **Sicherheit** wird angezeigt, wann die Definitionen für den Viren- und Spyware-Schutz sowie Netzwerkbedrohungsschutz zuletzt aktualisiert wurden. Unter **LiveUpdate** wird das Datum des letzten Produkt-Updates angezeigt. Um die Versionsnummer der Software anzuzeigen, klicken Sie auf **Hilfe > Info**.
Schritt 3: Aktualisieren Sie die Software bzw. Definitionen bei Bedarf.	Klicken Sie im Symantec Endpoint Protection-Client auf **LiveUpdate**, um Software und Definitionen sofort zu aktualisieren. Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware
Schritt 4: Führen Sie einen Scan aus.	Sie können Scan so planen, dass Sie in regelmäßigen Abständen oder sofort ausgeführt werden. Einrichten geplanter Scans Ausführen eines manuellen Scans

Verwalten der Einstellungen für den Viren- und Spyware-Schutz

Erneuern Ihrer Produktlizenz

Möglicherweise wird die Meldung unter dem Symantec Endpoint Protection-Clientsymbol auf der Menüleiste angezeigt, dass die Lizenz für Symantec Endpoint Protection abgelaufen ist. Der Symantec Endpoint Protection-Client verwendet eine Lizenz, um Folgendes zu aktualisieren:

- Die neue Clientsoftware
- Die Dateien der Schutzdefinitionen für Viren und Spyware-Scans sowie den Angriffsschutz

Der Client kann eine Testlizenz oder eine Volllizenz verwenden. Sind diese Lizenzen abgelaufen, aktualisiert der Client die Definitionen bzw. die Software nicht.

Unabhängig vom Lizenztyp müssen Sie sich an Ihren Administrator wenden, um die Lizenz zu aktualisieren bzw. zu verlängern.

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Aktivieren oder Deaktivieren der Gerätesteuerung des Symantec Endpoint Protection-Clients für Mac

Symantec Endpoint Protection Manager-Administratoren können verwaltete Clients mit einer Gerätesteuerungsrichtlinie konfigurieren. Geräte können mit dieser Richtlinie durch Gerätenamen, Geräthändler, Gerätemodell oder Seriennummer blockiert werden oder die Blockierung kann aufgehoben werden.

Sie können die Gerätesteuerungsaktivität auf der Seite **Erweitert** anzeigen, indem Sie auf **Aktivität > Security History** klicken.

Mit den Einstellungen im Symantec Endpoint Protection-Client für **Device Control** können Sie die Gerätesteuerung aktivieren oder deaktivieren. Wenn die Gerätesteuerung aktiviert ist, können Sie Benachrichtigungen beliebig aktivieren oder deaktivieren, wenn die Geräte blockiert sind oder nicht blockiert sind.

Um die Einstellungen zu ändern, müssen Sie sich mit Mac-Administrator-Zugangsdaten authentifizieren. Wenn diese Einstellungen ausgegraut sind, dann hat der Administrator sie gesperrt, um Sie am Aktivieren oder am Deaktivieren dieser Funktion zu hindern.

Sie können keine Geräte, die durch die Symantec Endpoint Protection-Clientschnittstelle blockiert werden oder deren Blockierung aufgehoben werden soll, hinzufügen oder bearbeiten.

> **NOTE**
> Die Gerätesteuerungsrichtlinie aus Symantec Endpoint Protection Manager steuert die Gerätesteuerungseinstellungen. Beim folgenden Heartbeat werden alle Änderungen, die Sie für diese Einstellungen vornehmen, zurückgesetzt auf das, was die Richtlinie vorschreibt.

Die Gerätesteuerung ist nicht für nicht verwaltete Clients verfügbar.

Info zur WSS-Datenverkehrsumleitung für den macOS-Client

Die Web Security Service (WSS)-Datenverkehrsumleitung (WDU) automatisiert die Umleitung des Datenverkehrs an Symantec Web Security Service und schützt den Webdatenverkehr auf allen Computern, die Symantec Endpoint Protection nutzen.

Der Administrator steuert die Einstellungen der WSS-Datenverkehrsumleitung, zu denen die URL der Proxy-Konfiguration und das optionale Stammzertifikat für Symantec Web Security Service gehören. Nur der Symantec Endpoint Protection Manager-Administrator kann diese Einstellungen konfigurieren, da sie nicht in der Benutzeroberfläche des Symantec Endpoint Protection-Client verfügbar sind. Sie können die URL der Proxy-Konfigurationsdatei unter **Systemeinstellungen > Netzwerk** im Abschnitt **Proxies** anzeigen. Das Cloud-Services-Zertifikat wird unter **Schlüsselbund** angezeigt.

Die WSS-Datenverkehrsumleitung wird nur von den Webbrowsern Safari, Chrome und Firefox (Version 65) unterstützt. In Symantec Endpoint Protection-Versionen vor 14.2 RU1 werden nur Safari und Chrome unterstützt.

Deinstallieren des Symantec Endpoint Protection-Clients für Mac

Sie deinstallieren den Symantec Endpoint Protection-Client für Mac über das Clientsymbol auf der Menüleiste. Die Deinstallation des Symantec Endpoint Protection-Client für Mac erfordert administrative Login-Informationen.

> **NOTE**
> Nachdem Sie den Symantec Endpoint Protection-Client deinstalliert haben, werden Sie aufgefordert, den Clientcomputer neu zu starten, um die Deinstallation abzuschließen. Stellen Sie sicher, dass Sie unfertige Arbeit speichern oder alle geöffneten Anwendungen schließen, bevor Sie anfangen.

So deinstallieren Sie den Symantec Endpoint Protection-Client für Mac

1. Öffnen Sie auf dem macOS-Computer den Symantec Endpoint Protection-Client und wählen Sie "**Symantec Endpoint Protection > Symantec Endpoint Protection deinstallieren**".
2. Klicken Sie erneut auf **Deinstallation**, um die Deinstallation zu starten.
3. Zum Installieren eines Hilfsprogramms, das für die Deinstallation des Symantec Endpoint Protection-Clients erforderlich ist, geben Sie den Administrator-Benutzernamen und das Kennwort für den Mac-Computer ein, und klicken Sie dann auf **Install Helper**.
4. Geben Sie im Dialogfeld **Symantec Endpoint Protection is trying to modify a System Extension** den Administrator-Benutzernamen und das Kennwort für den Mac-Computer ein, und klicken Sie auf **OK**.

   Beim Deinstallieren des Client werden Sie eventuell zum Eingeben eines Kennworts aufgefordert. Dieses Kennwort kann sich vom macOS-Administratorkennwort unterscheiden.
5. Sobald die Deinstallation abgeschlossen ist, klicken Sie auf **Jetzt neu starten**.

Wenn Symantec Uninstaller einen Fehler ausgibt, müssen Sie möglicherweise ein anderes Deinstallierungsverfahren verwenden. Weitere Informationen finden Sie unter:

Deinstallieren von Symantec Endpoint Protection

Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware

Symantec-Produkte benötigen stets aktuelle Informationen, damit der Computer vor neu auftretenden Bedrohungen geschützt werden kann. Symantec stellt Symantec Endpoint Protection diese Informationen über LiveUpdate zur Verfügung. LiveUpdate ruft Produkt- und Definitions-Updates über die Internetverbindung ab.

Definitions-Updates sorgen mit den neuesten Bedrohungsschutzfunktionen dafür, dass Symantec-Produkte immer auf dem neuesten Stand sind. LiveUpdate lädt die neuen Angriffsschutzsignaturen bzw. Virendefinitionen von einer Symantec-Website herunter und ersetzt die alten Dateien.

Programm-Updates dienen zur Verbesserung des installierten Clients. Produkt-Updates dienen im Allgemeinen dazu, die Betriebssystem- oder Hardwarekompatibilität zu erweitern, Leistungsprobleme anzupassen oder Produktfehler zu beheben. Produkt-Updates werden nach Bedarf herausgegeben. Der Client erhält Produkt-Updates direkt von einem LiveUpdate-Server. Die Kombination aus Produkt- und Definitions-Updates wird "Content-Update" genannt.

Table 5: Methoden zur Aktualisierung von Inhalt auf Ihrem Computer

Aufgabe	Beschreibung
Sofortiges Aktualisieren des Inhalts	Sie können LiveUpdate sofort ausführen. Sofortiges Aktualisieren des Content in Symantec Endpoint Protection

Verwalten des Schutzes auf dem Mac mit Symantec Endpoint Protection

Sofortiges Aktualisieren des Content in Symantec Endpoint Protection

Sie können Definitionen und Produktdateien sofort mit LiveUpdate aktualisieren. Sie sollten LiveUpdate aus folgenden Gründen manuell ausführen:

- Die Clientsoftware wurde vor Kurzem installiert.
- Der letzte Scan liegt länger zurück.
- Sie vermuten, dass Sie einen Virus oder andere Malware haben.

So aktualisieren Sie Content in Symantec Endpoint Protection

Sie haben folgende Möglichkeiten, um LiveUpdate zu starten:

- Klicken Sie mit der rechten Maustaste auf das Symbol Symantec Endpoint Protection in der Menüleiste, und klicken Sie dann auf **LiveUpdate**.
- Öffnen Sie den Symantec Endpoint Protection-Client, und klicken Sie dann auf **LiveUpdate**.

LiveUpdate stellt eine Verbindung zum konfigurierten LiveUpdate-Server her, sucht nach verfügbaren Updates, führt den Download aus und installiert sie automatisch. Eine Statusleiste zeigt den Fortschritt des Downloads an.

Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware

Geplantes Aktualisieren des Content in Symantec Endpoint Protection

Zeitpläne auf verwalteten Mac OS-Clients

Standardmäßig erhalten verwaltete Mac OS-Clients einen Zeitplan von Symantec Endpoint Protection Manager, der LiveUpdate alle vier Stunden ausführt. Der Symantec Endpoint Protection Manager-Administrator steuert den Zeitplan.

Verwaltete Clients können den vom Administrator erstellten Zeitplan nicht entfernen, ändern oder anzeigen und keinen neuen erstellen.

Zeitpläne auf nicht verwalteten Mac OS-Clients

Sie können einen Zeitplan erstellen, damit LiveUpdate automatisch in geplanten Abständen ausgeführt wird. Es empfiehlt sich, die Ausführung von LiveUpdate während eines Zeitraums zu planen, in dem Sie Ihren Computer nicht verwenden.

So erstellen Sie einen Zeitplan zum Aktualisieren des Content in Symantec Endpoint Protection:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Product Settings** (Produkteinstellungen), und klicken Sie anschließend auf das Einstellungssymbol für **Scheduled LiveUpdate** (Geplantes LiveUpdate).

   Der aktuelle Zeitplan wird angezeigt.

2. Wählen Sie in der Dropdown-Liste "LiveUpdate-Zeitplan:" ein Intervall aus.

   Die Standardeinstellung ist alle **4** Stunden. Sie können eine Uhrzeit bzw. ein Datum und eine Uhrzeit auswählen, um den Vorgang **Täglich** bzw. **Wöchentlich** auszuführen.

3. Klicken Sie auf **Änderungen übernehmen**.

Sofortiges Aktualisieren des Content in Symantec Endpoint Protection

Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware

Infos zum Verbinden des Management-Server über einen Proxy-Server

Sie werden eventuell gebeten zuzulassen, dass Symantec Endpoint Protection Ihre Zugangsdaten zum Herstellen einer Verbindung zum Management-Server über einen Proxy verwendet. Sie erhalten eine Meldung und werden gefragt, ob Sie dem `symdaemon`-Prozess Zugriff auf Ihre Zugangsdaten gewähren möchten.

Sie müssen in der Meldung auf **Immer zulassen** klicken. Andernfalls wird diese Meldung jedesmal angezeigt, wenn der Client eine Verbindung zum LiveUpdate-Server herstellt. Wenn Sie auf **Verweigern** klicken, kann der Client keine Updates für Software oder Definitionen abrufen.

Aktualisieren von Viren- und Angriffsschutzdefinitionen sowie der Clientsoftware

Verwalten der Einstellungen für den Viren- und Spyware-Schutz

Standardmäßig schützt Symantec Endpoint Protection vor Viren und Sicherheitsrisiken, auch Netzwerkbedrohungen, sobald der Computer hochgefahren wird. Der Viren- und Spyware-Schutz enthält die Funktion "Auto-Protect", die laufende Programme auf Viren scannt. Es überwacht Ihren Computer auch auf Aktivitäten, die auf das Vorhandensein eines Virus oder Sicherheitsrisikos hinweisen könnten. Die aktivierte Auto-Protect-Funktion verhindert, dass Viren Ihren Computer infizieren. Sie sollten Auto-Protect aktiviert lassen.

Bei verwalteten Clients hängt die Kontrolle, die Sie über diese Einstellungen haben, davon ab, wie der Administrator den Client konfigurierte. Zusätzlich werden alle Änderungen, die Sie an diesen Einstellungen vornehmen, möglicherweise beim folgenden Heartbeat zurückgesetzt auf das, was die Richtlinie vorschreibt.

Verwalten von Viren- und Spyware-Schutz beschreibt die Aufgaben zum Verwalten des Viren- und Spyware-Schutzes auf Ihrem Mac.

Table 6: Verwalten von Viren- und Spyware-Schutz

Schritte	Beschreibung
Schritt 1: Aktivieren oder Deaktivieren des Viren- und Spyware-Schutzes	Sie können den Viren- und Spyware-Schutz einfach aktivieren und deaktivieren. Symantec empfiehlt, dass Sie diese Option aktiviert lassen. Aktivieren und Deaktivieren des Viren- und Spyware-Schutzes
Schritt 2: Anpassen der Auto-Protect-Einstellungen	Auto-Protect ist ein wichtiger Teil des Viren- und Spyware-Schutzes. Sie können diese Optionen auf der Seite **Erweitert** konfigurieren. Konfigurieren der Auto-Protect- und Scan-Zonen-Einstellungen
Schritt 3: Scannen des Computers auf Viren	Sie können Virenscans so einrichten, dass Sie im Rahmen eines Zeitplans oder sofort ausgeführt werden. Einrichten geplanter Scans Anhalten, Verschieben und Beenden von Scans Ausführen eines manuellen Scans
Schritt 4: Reagieren auf von Symantec Endpoint Protection erkannte Viren	Wenn Symantec Endpoint Protection Ihren Computer scannt, kann Folgendes passieren: • Sie werden über Aktionen informiert, die Sie ausführen können. • Sie werden über Schutzmaßnahmen informiert, die für Sie durchgeführt wurden. Reagieren auf Meldungen über erkannte Infektionen und Risiken

Aktivieren und Deaktivieren des Viren- und Spyware-Schutzes

Der Viren- und Spyware-Schutz und Auto-Protect sind standardmäßig aktiviert.

Sie können Auto-Protect präziser steuern, indem Sie bestimmte Optionen festlegen.

Ist der Viren- und Spyware-Schutz deaktiviert, werden auf der Seite **Status** ein rotes "x" sowie die Meldung **Viren- und Spyware-Schutz ist deaktiviert** angezeigt. Ist der Schutz deaktiviert, sollten Sie ihn so bald wie möglich aktivieren.

NOTE
Geplante Scans werden fortgesetzt, unabhängig davon, ob der Viren- und Spyware-Schutz aktiviert oder deaktiviert ist. Ihr Administrator kann den Zugriff auf bestimmte Symantec Endpoint Protection-Einstellungen einschränken. Sie können diese Einstellungen eventuell nicht deaktivieren, keine Scans planen oder die Schutzoptionen nicht anpassen.Sie müssen eventuell Ihr Mac-Administratorkennwort angeben, damit Sie diese Einstellungen ändern können.

So aktivieren bzw. deaktivieren Sie den Viren- und Spyware-Schutz:

1. Um den Viren- und Spyware-Schutz zu aktivieren, klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Protect My Mac**, und aktivieren Sie dann **Automatic Scans**.
2. Um den Viren- und Spyware-Schutz zu deaktivieren, klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Protect My Mac**, und deaktivieren Sie dann **Automatic Scans**.

Konfigurieren der Auto-Protect- und Scan-Zonen-Einstellungen

Verwalten der Einstellungen für den Viren- und Spyware-Schutz

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Konfigurieren der Auto-Protect- und Scan-Zonen-Einstellungen

Auf verwalteten Clients können Sie anpassen, wie Auto-Protect Viren überwacht und infizierte Dateien repariert, wenn Ihr Administrator dies zulässt.

Die Auto-Protect-Einstellungen werden als Optionen unter **Protect My Mac** angezeigt. Sie müssen **Automatic Scans** aktivieren, um Auto-Protect zu aktivieren.

In den **Scan-Zonen-Einstellungen** können Sie angeben, welche Dateien gescannt bzw. nicht gescannt werden sollen.

So konfigurieren Sie die Auto-Protect-Einstellungen:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Protect My Mac**, und klicken Sie anschließend auf das Einstellungssymbol für **Automatic Scans**.
2. Sie können folgende Optionen anpassen:

Automatisch isolieren	Sie können wählen, ob Sie Dateien, die nicht bereinigt werden können, in die Quarantäne verschieben möchten.
Automatisch reparieren	Sie können wählen, von Auto-Protect automatisch alle infizierten Dateien, die gefunden werden, bereinigen zu lassen.
Scan	Sie können **Data Disks** und **All other disks** auswählen.
Komprimierte Dateien scannen	Sie können wählen, ob komprimierte Dateien bei einem Auto-Protect-Scan eingeschlossen werden sollen. Der Scan umfasst die komprimierte Datei und die Dateien innerhalb der komprimierten Datei.

WARNING
Wenn Sie die Funktion **Automatisch reparieren** nicht aktivieren, werden infizierte Dateien nicht isoliert, auch wenn Sie die Option **Automatisch isolieren** aktivieren.Die Software fragt, ob Sie eine infizierte Datei reparieren möchten. Wenn Sie die Datei nicht reparieren, bleibt sie auf dem Computer. Wenn Sie die Funktion **Automatisch reparieren** aktivieren, und die Option **Automatisch isolieren** nicht aktivieren, werden die infizierten Dateien gelöscht.

3. Klicken Sie auf **Fertig**.

So konfigurieren Sie die Scan-Zonen-Einstellungen:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Protect My Mac**, und klicken Sie anschließend auf das Einstellungssymbol für **Scan Zone Settings**.
2. Sie können folgende Optionen anpassen:

Alle scannen	Alle Dateien und Prozesse auf dem Computer werden gescannt, wenn Sie darauf zugreifen.
Nur Scannen	Nut die von Ihnen angegebenen Dateien oder Ordner werden gescannt.
Nicht scannen	Alle Dateien bzw. Ordner, außer den von Ihnen angegebenen, werden gescannt.

Standardeinstellungen	Ist diese Option aktiviert, wird alles gescannt.

3. Klicken Sie auf **OK**.

Funktionsweise des Viren- und Spyware-Schutzes

Aktivieren und Deaktivieren des Viren- und Spyware-Schutzes

Verwalten isolierter Dateien

Einrichten geplanter Scans

Symantec Endpoint Protection führt automatisch einen Standardscan aus, wenn Sie einen verwalteten Client nutzen. Wenn Ihr Administrator dies zulässt, können Sie weitere Scans planen.

> **NOTE**
> Auf einem nicht verwalteten Client müssen Sie Ihre eigenen Scans ausführen.Symantec empfiehlt, so bald wie möglich einen vollständigen manuellen Scan auszuführen und dann einen regelmäßigen geplanten Scan einzurichten. Sie können einen beliebigen (geplant oder manuell) Scan anhalten oder verzögern.

Auf einem verwalteten Client wird der Standardscan täglich um 20:00 Uhr ausgeführt. Die Option "Automatisch reparieren" ist aktiviert.

Ausführen eines manuellen Scans

So richten Sie geplante Scans ein:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Protect My Mac** (Meinen Mac schützen), und klicken Sie anschließend auf das Einstellungssymbol für **Scheduled Scans** (Geplante Scans).
2. Klicken Sie im Dialogfeld auf **Geplante Scans hinzufügen** bzw. auf den aktuellen geplanten Scan und anschließend auf **Bearbeiten**, um die Einstellungen dafür anzupassen.
3. Auf der Registerkarte **Elemente scannen** können Sie folgende Optionen einstellen:

Laufwerke	Hier können Sie festlegen, ob **Festplatten** und **Wechseldatenträger** gescannt werden sollen.
Ordner	Hier können Sie festlegen, dass **Benutzerordner (aktiver Benutzer)**, **Anwendungen** und **Bibliothek** gescannt werden sollen. Wenn zum Zeitpunkt des geplanten Scans eines Benutzerordners kein Benutzer eingeloggt ist, wird der Scan nicht ausgeführt.
Scanoptionen	Sie können aus folgenden Optionen wählen: • **Komprimierte (Dateien) scannen** • **Automatisch reparieren** • **Automatisch isolieren** • **Leerlaufzeitscan aktivieren**

4. Auf der Registerkarte **Scanzeitplan** können Sie folgende Optionen einstellen:

Scanzeitplan	Sie können einen Scan so einrichten, dass er in einem bestimmten Intervall stündlich, täglich, wöchentlich oder monatlich ausgeführt wird. **In bestimmtem Intervall ausführen** ist beim Planen neuer Scans standardmäßig aktiviert.
Ausführung alle	Verfügbar, wenn **In bestimmtem Intervall ausführen** unter **Scanzeitplan** ausgewählt ist.
Startzeit	Verfügbar, wenn **Täglich**, **Wöchentlich** oder **Monatlich** für den Scanzeitplan ausgewählt ist. Sie können die Uhrzeit auswählen, zu der der Scan ausgeführt werden soll. Sie sollten einen Zeitpunkt wählen, zu dem der Computer normalerweise nicht genutzt wird, da Scans die Leistung des Computers beeinträchtigen können.

Ein	Verfügbar, wenn **Wöchentlich** oder **Monatlich** für den Scanzeitplan ausgewählt ist. Sie können den Wochentag auswählen, an dem der Scan ausgeführt werden soll. Sie sollten einen Zeitpunkt wählen, zu dem der Computer normalerweise nicht genutzt wird, da Scans die Leistung des Computers beeinträchtigen können.

5. Auf der Registerkarte **Tuning** können Sie einstellen, wie die Leistung des Scans optimiert wird.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Fertig**.

Anhalten, Verschieben und Beenden von Scans

Verwalten des Schutzes auf dem Mac mit Symantec Endpoint Protection

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Aktivieren bzw. Deaktivieren des Sendens von Sicherheitsinformationen an Symantec

Ausführen eines manuellen Scans

Sie müssen möglicherweise einige Dateien manuell scannen. Beispiel: Sie müssen möglicherweise die Dateien scannen, die vor der Installation von Symantec Endpoint Protection auf dem Computer gespeichert wurden. Oder Sie können sich evtl. dafür entscheiden, dass einige Dateien gescannt werden müssen, die von einem geplanten Scan ausgeschlossen wurden.

> **NOTE**
> Sie können einen beliebigen (geplant oder manuell) Scan anhalten oder verzögern.

So führen Sie einen manuellen Scan aus:

Führen Sie auf dem Symantec Endpoint Protection-Client auf der Seite **Scans** einen der folgenden Schritte aus:

- Um einen Schnellscan zu starten, klicken Sie auf **Quick Scan**, und klicken Sie anschließend auf **Start a Quick Scan**.
- Um einen vollständigen Scan zu starten, klicken Sie auf **Full Scan**, und klicken Sie anschließend auf **Start a Full Scan**.
- Um eine Datei oder einen Ordner zu scannen, klicken Sie auf **File Scan**, und klicken Sie anschließend auf **Select a file**.Der Finder wird geöffnet, und Sie können zwischen **Show Hidden Files** und **Scan Compressed Files** auswählen. Außerdem können Sie die Optionen **Auto Repair** und **Auto Quarantine** aktivieren.

Anhalten, Verschieben und Beenden von Scans

Einrichten geplanter Scans

Aktivieren bzw. Deaktivieren des Sendens von Sicherheitsinformationen an Symantec

Anhalten, Verschieben und Beenden von Scans

Mit der Funktion "Unterbrechen" können Sie einen Scan anhalten und später wieder fortsetzen. Sie können einen beliebigen Scan auch anhalten und abbrechen. Für den Einsatz dieser Funktionen brauchen Sie keine Administratorrechte.

Wenn ein Scan fortgesetzt wird, startet der Scan dort, wo er angehalten wurde.

> **NOTE**
> Wenn Sie einen Scan unterbrechen, während der Client eine komprimierte Datei scannt, kann es einige Minuten dauern, bis der Client auf die Unterbrechungsanfrage reagiert.

Wenn das Verschieben aktiviert ist, können Sie auch einen Scan verschieben, aber nur, bevor der Scan anfängt. Sie können keinen laufenden Scan verschieben.

So unterbrechen Sie einen laufenden geplanten Scan bzw. halten ihn an:

1. Klicken Sie im Dialogfeld "Scanstatus" auf **Unterbrechen**.
2. Klicken Sie im Dialogfeld "Scanstatus" auf **Fortsetzen** bzw. auf **Stopp**. Sie können auch auf **Fertig** klicken, um das Dialogfeld zu schließen.

So unterbrechen Sie einen laufenden manuellen Scan bzw. halten ihn an:

1. Klicken Sie im Dialogfeld "Scanstatus" auf **Unterbrechen**, um den Scan zu unterbrechen.
2. Klicken Sie auf **Abbrechen**, um einen manuellen Scan anzuhalten bzw. auf **Fortsetzen**, um ihn fortzusetzen.

So verschieben Sie einen Scan kurz dem Start:

1. Im Fenster, das angezeigt wird, klicken Sie auf das Dropdown-Menü, um einen Wert auszuwählen, der verschoben werden soll. Sie können ihn für nur 15 Minuten verschieben oder für einen Tag.
2. Klicken Sie auf **OK**, um den Scan zu verschieben.

   Sie brauchen nichts zu tun, wenn Sie möchten, dass der Scan wie geplant ausgeführt wird.

Einrichten geplanter Scans

Ausführen eines manuellen Scans

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Sie können prüfen, ob Ihr Computer infiziert ist und einige zusätzliche Aufgaben ausführen, wenn Ihnen die Sicherheit oder Leistung nicht ausreicht.

Ihr Administrator kann Ihren Client verwalten, oder Sie können einen nicht verwalteten Client ausführen. Die Schutzaufgaben, die Sie durchführen können, sind davon abhängig, wie viel Kontrolle Ihr Administrator über den Client behalten möchten.

Erkennt Symantec Endpoint Protection einen Virus oder ein Sicherheitsrisiko, werden Sie eventuell gebeten eine Aktion auszuwählen. Abhängig von den vom Administrator definierten Einstellungnen werden Sie eventuell über die automatisch von Client ausgeführten Aktionen.

Table 7: Reagieren auf Meldungen über erkannte Infektionen

Inhalt der Meldung	Aktion erforderlich
Bereinigte die infizierte Datei	Keine
Holt Ihre Zustimmung zum Bereinigen der infizierten Datei ein	Stimmen Sie der Bereinigung zu. Diese Option ist von Ihren Auto-Protect-Einstellungen abhängig. Verwalten der Einstellungen für den Viren- und Spyware-Schutz Wenn die Option zur automatischen Bereinigung infizierter Dateien deaktiviert ist, müssen Sie die Datei manuell reparieren. Reparieren infizierter Dateien
Infizierte Datei konnte nicht bereinigt werden	Verwalten Sie die Infektion in der Quarantäne. Verwalten isolierter Dateien

Funktionsweise des Viren- und Spyware-Schutzes

Reparieren infizierter Dateien

Wird eine infizierte Datei nicht automatisch repariert oder isoliert, können Sie sie aus den Scanergebnissen reparieren. Sie können Dateien auf der Festplatte des Computers oder auf Wechselmedien manuell bereinigen.

So bereinigen Sie infizierte Dateien:

1. Wählen Sie in der Liste mit den Scanergebnissen die zu bereinigende Datei aus und klicken Sie anschließend auf **Reparieren**.

   Sie können auch im **Finder** oder Menü **Suchen** mit der rechten Maustaste auf eine Datei klicken.
2. Wiederholen Sie dies bei Bedarf.
3. Führen Sie einen weiteren Scan aus, um auf andere infizierte Dateien zu prüfen.
4. Überprüfen Sie die bereinigten Dateien, um deren ordnungsgemäße Funktionsweise sicherzustellen.

Verwalten der Einstellungen für den Viren- und Spyware-Schutz

Verwalten isolierter Dateien

Verwalten isolierter Dateien

Erkennt der Client einen Virus in einer Datei, versucht er standardmäßig, diesen zu entfernen. Wenn der Virus nicht entfernt werden kann, wird die Datei in die Quarantäne auf Ihrem Computer verschoben. Wenn Symantec Endpoint Protection ein Sicherheitsrisiko in einer Datei erkennt, verschiebt es die Datei zuerst in die Quarantäne. Anschließend repariert der Client alle Nebenwirkungen des Risikos.

Wenn Sie Ihre Virendefinitionen aktualisieren, überprüft der Client automatisch den Quarantänebereich. Sie können die Objekte im Quarantänebereich erneut scannen. Mit den neuesten Definitionen können die isolierten Dateien evtl. bereinigt oder repariert werden.

So verwalten Sie isolierte Dateien:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Aktivität > Sicherheitsverlauf > Quarantäne**.
2. Wählen Sie die zu verwaltende Datei und anschließend die entsprechende Option aus:

Reparieren	Wählen Sie diese Option, um eine isolierte Datei zu reparieren versuchen. Stellen Sie sicher, dass Ihre Virendefinitionen aktueller sind als das Datum, an dem die Datei isoliert wurde.
Löschen	Wählen Sie diese Option, um alle nicht mehr benötigten Dateien aus der Quarantäne zu löschen.
Wiederherstellen	Wenn Sie sicher sind, dass die Datei keinen Virus enthält, können Sie sie in ihrem ursprünglichen Verzeichnis auf dem Computer wiederherstellen. Mit dieser Option wird die Datei nicht gescannt oder zu reparieren versucht.

Reagieren auf Meldungen über erkannte Infektionen und Risiken

Aktivieren bzw. Deaktivieren des Sendens von Sicherheitsinformationen an Symantec

Symantec Endpoint Protection kann pseudonymisierte Informationen zu erkannten Bedrohungen an Symantec senden. Symantec verwendet diese Informationen, um Ihre Clientcomputer vor neuen, gezielten und mutierenden Bedrohungen zu schützen. Von Ihnen übermittelte Daten verbessern Symantecs Fähigkeit, auf Bedrohungen zu reagieren und den Schutz für Computer anzupassen.

Die von Symantec erfassten Telemetriedaten enthalten möglicherweise pseudonyme Elemente, die nicht direkt identifizierbar sind. Symantec benötigt zum Identifizieren einzelner Benutzer keine Telemetriedaten.

Standardmäßig sendet der Clientcomputer Informationen über Erkennungen an Symantec. Sie können diese Einstellung zwar deaktivieren, Symantec empfiehlt allerdings, sie aktiviert zu lassen.

Es wurden nur Informationen zu erkannten Viren gesendet.

NOTE
Symantec empfiehlt, dass Sie diese Option aktiviert lassen.

So aktivieren bzw. deaktivieren Sie das Senden von pseudonymisierten Sicherheitsinformationen an Symantec:

Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Product Settings**, und aktivieren oder deaktivieren Sie die Option **Security Info Submission**.

Einrichten geplanter Scans

Ausführen eines manuellen Scans

Verwalten von Intrusion Prevention

Die Standardeinstellungen für den Angriffsschutz schützen den Mac-Client. Wenn Sie den Schutz jedoch selbst verwalten möchten, können Sie den Angriffsschutz im Rahmen des Netzwerkbedrohungsschutzes anpassen.

Table 8: Verwalten von Intrusion Prevention

Schritte	Beschreibung
Schritt 1: Informationen zu Intrusion Prevention	Informationen dazu, wie der Angriffsschutz Netzwerkangriffe erkennt und blockiert. Funktionsweise des Netzwerkbedrohungsschutzes für Mac
Schritt 2: Download der neuesten IPS-Signaturen	Standardmäßig werden die neuesten Signaturen auf den Client heruntergeladen. Möglicherweise wollen Sie die Signaturen jedoch sofort herunterladen. Sofortiges Aktualisieren des Content in Symantec Endpoint Protection
Schritt 3: Aktivieren und Deaktivieren des Angriffsschutzes	Sie müssen den Angriffsschutz eventuell zur Fehlerbehebung oder wenn auf Clientcomputern zu viele Falschmeldungen erzeugt werden, deaktivieren. Üblicherweise sollten Sie den Angriffsschutz nicht deaktivieren müssen. Aktivieren bzw. Deaktivieren des Netzwerkbedrohungsschutzes
Schritt 4: Weitere Informationen finden Sie unter: So aktivieren Sie Angriffsschutz-Benachrichtigungen	Sie können Symantec Endpoint Protection so konfigurieren, dass eine Benachrichtigung angezeigt wird, wenn ein Angriff erkannt wird. Aktivieren bzw. Deaktivieren der Netzwerkbedrohungsschutz-Meldungen

Verwalten des Firewall-Schutzes für den macOS-Client

Die Symantec Endpoint Protection-Firewall für Mac bietet Firewall-Schutz, der vollständig in Symantec Endpoint Protection (Ereignisse, Richtlinien und Befehle) integriert ist. Die Symantec Endpoint Protection-Firewall ist nur auf verwalteten Clients verfügbar.

NOTE
Die Symantec Endpoint Protection-Firewall für Mac kann nicht in die Firewall des Betriebssystems integriert werden. Sie wird stattdessen parallel ausgeführt. Die Betriebssystem-Firewall prüft in der Anwendungsschicht, während die Symantec Endpoint Protection-Firewall in niedrigeren Schichten (IP und Transport) prüft.Die Symantec Endpoint Protection-Firewall für Mac bietet keine Peer-to-Peer-Blockierungsregeln, obwohl diese teilweise über benutzerdefinierten Firewall-Regeln erstellen könnten.

Table 9: Verwalten des Firewall-Schutzes

Schritte	Beschreibung
Schritt 1: Weitere Informationen zum Firewall-Schutz	Es wird beschrieben, wie der Firewall-Schutz den Datenverkehr überwacht und vor gängigen Angriffsvektoren schützt. Funktionsweise des Netzwerkbedrohungsschutzes für Mac
Schritt 2: Aktivieren oder Deaktivieren der Firewall	Sie müssen möglicherweise die Firewall zu Fehlerbehebungszwecken deaktivieren, beispielsweise wenn Datenverkehr blockiert wird, der zugelassen werden soll. Normalerweise sollten Sie die Firewall nicht deaktivieren. Aktivieren bzw. Deaktivieren des Netzwerkbedrohungsschutzes

So aktivieren oder deaktivieren Sie den Netzwerkbedrohungsschutz

Wenn Sie den Netzwerkbedrohungsschutz auf einem Computer deaktivieren, ist dieser weniger gut geschützt. Jedoch sollten Sie den Angriffsschutz deaktivieren, um Falschmeldungen zu verhindern, oder die Firewall deaktivieren, um Fehler beim blockierten Datenverkehr zu beheben. Angriffsschutz und Firewall sind Teil des Netzwerkbedrohungsschutzes.

Bei verwalteten Clients hängt die Kontrolle, die Sie über diese Einstellungen haben, davon ab, wie der Administrator den Client konfigurierte. Zusätzlich werden alle Änderungen, die Sie an diesen Einstellungen vornehmen, möglicherweise beim folgenden Heartbeat zurückgesetzt auf das, was die Richtlinie vorschreibt.

Für nicht verwaltete Clients ist die Firewall nicht verfügbar.

So aktivieren oder deaktivieren Sie den Netzwerkbedrohungsschutz:

1. Klicken Sie im Symantec Endpoint Protection-Client auf der Seite **Erweitert** auf **Netzwerkbedrohungsschutz**.
2. Um den Angriffsschutz zu aktivieren oder zu deaktivieren, schalten Sie den **Angriffsschutz** ein oder aus.
3. Um die Firewall zu aktivieren oder zu deaktivieren, schalten Sie die **Firewall** ein oder aus.
4. Um Benachrichtigungen für den Angriffsschutz und die Firewall zu aktivieren oder zu deaktivieren, klicken Sie auf das Einstellungssymbol **Vulnerability Protection** (Schwachstellenschutz), und aktivieren oder deaktivieren Sie im Dialogfeld die Option **Display Vulnerability Protection Notifications** (Benachrichtigungen für den Schwachstellenschutz anzeigen).
5. Klicken Sie auf **Fertig**.

Wenn Sie diese Komponenten deaktivieren, sollten Sie sie erneut so bald wie möglich wieder aktivieren um den optimalen Schutz für den Computer sicherzustellen.

Verwalten von Intrusion Prevention

Verwalten des Firewall-Schutzes für den macOS-Client


Symantec
A Division of Broadcom