SOPHOS

Cybersecurity made simple.

Sophos Endpoint für Mac

Hilfe

Inhalt

1 Sophos Endpoint

Hinweis
Unter Umständen stehen Ihnen nicht alle in dieser Hilfe beschriebenen Funktionen zur Verfügung. Das hängt von Ihrer Lizenz ab.

Sophos Endpoint wird zentral über die Sophos Central Admin konfiguriert und verwaltet.

Folgende Aufgaben können auf dem Mac ausgeführt werden:

- Status (Seite 2) des Mac abfragen.
- Eine Datei scannen (Seite 8) oder Mac scannen (Seite 8), um nach Bedrohungen zu suchen.
- Ereignisse (Seite 3): Details zu Ereignissen auf dem Mac anzeigen, wie z. B. erkannte Bedrohungen.
- Entfernen eines Threat (Seite 8).
- Sicherheitseinstellungen ändern (Seite 8). Sie können zum Beispiel für die Fehlersuche und -behebung Funktionen deaktivieren.
- Jetzt aktualisieren (Seite 9).
- Fehlersuche (Seite 9).

Hinweis
Zum Entfernen von Bedrohungen oder zum Ändern der Einstellungen müssen Sie sich als Administrator anmelden (**Admin-Login**) und das Manipulationsschutz-Kennwort eingeben.

2 Status

Hinweis
Unter Umständen stehen Ihnen nicht alle hier beschriebenen Funktionen zur Verfügung. Das hängt von Ihrer Lizenz ab.

Auf der Seite **Status** können Sie:

- Den Sicherheitsstatus des Mac abfragen.
- Den Mac auf Bedrohungen überprüfen.
- Die installierten Funktionen und ihren Sicherheitsstatus sehen.

Hinweis
Unter dem Link **Info** können Sie die Viren-Definitionen aktualisieren oder Fehler beheben.

Sicherheitsstatus

Ein Symbol oben auf der Seite zeigt den Status an.

 Grün. Es liegen keine Warnhinweise oder nur solche mit niedriger Priorität vor.

 Rot. Es liegen Warnhinweise mit hoher Priorität vor.

 Gelb. Es liegen Warnhinweise mit mittlerer Priorität vor.

 Grau. Der Status ist unbekannt.

Darunter werden alle installierten Funktionen mit ihrem individuellen Sicherheitsstatus angezeigt.

Mac scannen

Klicken Sie auf **Jetzt scannen**, um alle Dateien auf dem Mac auf Bedrohungen zu überprüfen.

Hinweis
Wenn eine Bedrohung erkannt wird, ist die Option **Jetzt scannen** nicht verfügbar. Sie können stattdessen auf **Details anzeigen** klicken, um weitere Informationen zur Bedrohung anzuzeigen.

Nach Abschluss des Scans wird eine Zusammenfassung der Scanergebnisse angezeigt. Wenn Bedrohungen festgestellt wurden, können Sie auf **Details anzeigen** oder **Zu den Ereignissen** klicken, um Details anzuzeigen.

3 Ereignisse

Hinweis
Unter Umständen stehen Ihnen nicht alle hier beschriebenen Funktionen zur Verfügung. Das hängt von Ihrer Lizenz ab.

Auf der Seite **Ereignisse** werden Ereignisse auf dem Mac angezeigt, wie z. B. erkannte Bedrohungen.

Sie können Ereignisse filtern, z. B. um nur Ereignisse anzuzeigen, die Ihr Eingreifen erfordern, oder nach bestimmten Arten von Ereignissen suchen.

Die Liste „Ereignisse“

Die Liste „Ereignisse“ enthält folgende Informationen:

- Schweregrad. Ein Symbol gibt an, ob das Ereignis hohe oder mittlere Priorität hat oder ob es sich um eine Benachrichtigung handelt.
- Quelle. Ein Symbol gibt an, welche Sophos-Funktion das Ereignis gemeldet hat.
- Datum und Uhrzeit des Eintritts des Ereignisses.
- Beschreibung des Ereignisses.
- Link zu Maßnahmen, die Sie ergreifen können (sofern nötig). Wird nur angezeigt, wenn Sie sich als Administrator angemeldet haben.

Um Details zu einem Ereignis anzuzeigen, klicken Sie in der Liste auf den entsprechenden Eintrag.

Sie können hier dieselben Aktionen auswählen wie in der Sophos Central Admin-Konsole. Sehen Sie sich die Liste auf der Seite **Warnhinweise** in der Sophos Central Hilfe an.

Malware und PUAs

Malware ist eine allgemeine Bezeichnung für schädliche Software. Dazu gehören Viren, Würmer, Trojaner und Spyware.

Potenziell unerwünschte Anwendungen (PUA) sind harmlose Programme, wie z. B. Dialer, Remote-Administrationstools und Hacking-Tools, die aber im Allgemeinen als nicht geeignet für den Einsatz im Unternehmen betrachtet werden.

Web-Bedrohungen

Zu Web-Bedrohungen zählen schädliche Websites und risikobehaftete Downloads.

Einige Websites werden außerdem generell als ungeeignet für den Einsatz im Unternehmen betrachtet, wie zum Beispiel Pornoseiten oder soziale Medien. Sie können diese blockieren.

Gesteuerte Elemente

Diese Kategorie umfasst:

- Anwendungen, die keine Sicherheitsbedrohung darstellen, die Sie jedoch für nicht geeignet für den Einsatz im Unternehmen halten.
- Peripheriegeräte und Wechselmedien.
- Risikobehaftete Downloads oder Websites, die für das Geschäftsumfeld nicht geeignet sind.
- Dateien, die sensible Informationen (wie personenbezogene oder finanzielle Daten) enthalten, die nicht in die Hände Unbefugter gelangen sollen.

Schädlicher Datenverkehr

Schädlicher Datenverkehr bezeichnet Datenverkehr zwischen Computern, der auf einen möglichen Versuch einer Übernahme der Kontrolle über den Mac hinweist (ein sogenannter Command-and-Control-Angriff).

Ransomware

Ransomware ist erpresserische Software. Sie versperrt Ihnen den Zugriff auf Ihre eigenen Dateien – bis Sie ein Lösegeld bezahlen.

4 Erkennungen

Sie können den Mac auf Bedrohungen scannen und die von Sophos erkannten Bedrohungen anzeigen.

Computer scannen

Klicken Sie auf **Jetzt scannen**, um alle Dateien auf dem Mac auf Bedrohungen zu überprüfen.

Nach Abschluss des Scans wird eine Zusammenfassung der Überprüfung angezeigt. Wenn Bedrohungen festgestellt wurden, können Sie auf der Seite **Ereignisse** Details dazu aufrufen.

Malware- und PUA-Ereignisverlauf

Zeigt den Verlauf der erkannten Malware und PUAs an. Klicken Sie auf den Pfeil, um Details auf der Seite **Ereignisse** anzuzeigen.

Erkennungsverlauf

Zeigt an, wie viele Bedrohungen eines bestimmten Typs erkannt wurden. Wenn Sie auf einen Typ klicken, werden Details zu den erkannten Bedrohungen des betreffenden Typs auf der Seite **Ereignisse** angezeigt.

Übersicht zurücksetzen

Klicken Sie auf **Übersicht zurücksetzen**, um die auf der Seite **Erkennungen** angezeigte Historien-Anzahl auf Null zu setzen.

5 Einstellungen

Hinweis
Unter Umständen stehen Ihnen nicht alle hier beschriebenen Funktionen zur Verfügung. Das hängt von Ihrer Lizenz ab.

Die Seite **Einstellungen** ist nur verfügbar, wenn Sie den **Admin-Login** verwenden und das Manipulationsschutz-Kennwort eingeben (das Sie vom Sophos Central-Administrator erhalten).

Sie können die Sicherheitseinstellungen auf diesem Mac vorübergehend ändern.

Dies kann für die Fehlersuche und -behebung erforderlich sein. Sie können z. B. eine Funktion deaktivieren, um festzustellen, ob Probleme auf dem Mac durch sie verursacht werden.

Einstellungen ändern

Aktivieren Sie das Häkchen bei **Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen**.

Sie können jetzt Änderungen auf dieser Seite vornehmen. Die Änderungen setzen vorübergehend die Richtlinie außer Kraft, die Sie (oder ein anderer Administrator) über die Sophos Central Admin-Konsole angewendet haben.

Nach vier Stunden ändern sich die Einstellungen automatisch wieder in die zentral durchgesetzten Richtlinieneinstellungen.

Hinweis
Sie können die Einstellungen aber auch früher wieder zurückändern. Für einzelne Funktionen ist dies nicht möglich. Sie müssen die Option **Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen** deaktivieren. Dies wird für alle Funktionen übernommen.

Echtzeit-Scans

Beim Echtzeit-Scan werden Elemente gescannt, wenn Benutzer versuchen, auf sie zuzugreifen. Zugriff wird nur erlaubt, wenn diese unbedenklich sind. Sie können folgende Optionen auswählen:

- **Dateien**. Hier werden lokale Dateien und (sofern in der Richtlinie ausgewählt) Netzwerkfreigaben gescannt.
- **Internet**. Hier werden Internetressourcen gescannt. Es können laufende Downloads gescannt werden, der Zugriff auf schädliche Websites kann blockiert werden und es können Websites mit niedriger Reputation erkannt werden.

Kontrolle über Benutzer

- **Peripheral Control**. Hiermit können Sie den Zugriff auf Peripheriegeräte und Wechselmedien kontrollieren.
- **Application Control**. Hiermit können Sie Anwendungen erkennen und sperren, die zwar kein Sicherheitsrisiko darstellen, die Sie jedoch nicht für geeignet für den Einsatz im Unternehmen halten.

- **Web Control**. Die Funktion schützt vor risikobehafteten Downloads, steuert, welche Websites Benutzer besuchen dürfen, und verhindert Datenverlust.

Laufzeitschutz

Der Laufzeitschutz schützt vor Bedrohungen, indem verdächtiges oder schädliches Verhalten bzw. Datenverkehr auf Macs erkannt wird. Sie können folgende Optionen auswählen:

- **Erkennung schädlichen Datenverkehrs**. Erkennung von Datenverkehr zwischen einem Mac und einem Server, der auf einen möglichen Versuch hinweist, die Kontrolle über den Mac zu übernehmen.
- **Ransomware-Erkennung (CryptoGuard)**. Schutz vor Malware, die den Zugriff auf Dateien unterbindet und für deren Freigabe Lösegeld fordert.

6 Hinweise zur Vorgehensweise

6.1 Eine Datei scannen

So scannen Sie einzelne Dateien:

Rechtsklicken Sie im Finder auf die Datei und wählen Sie **Mit Sophos Endpoint scannen**.

Es wird der Dialog **Finder-Objektscan** mit dem Scan-Fortschritt und den Ergebnissen angezeigt.

6.2 Mac scannen

So scannen Sie alle Dateien auf dem Mac:

1. Wechseln Sie zur Seite **Status** oder zur Seite **Erkennungen**.
2. Klicken Sie Auf **Jetzt Scannen**.
   Nach Abschluss des Scans wird eine Zusammenfassung der Überprüfung angezeigt.
3. Wenn Bedrohungen festgestellt wurden, können Sie auf der Seite **Ereignisse** Details dazu aufrufen.

6.3 Entfernen eines Threat

So entfernen Sie eine erkannte Bedrohung:

1. Klicken Sie auf **Admin-Login** und geben Sie das Manipulationsschutz-Kennwort ein (das Sie vom Sophos Central-Administrator erhalten).
   Der Link **Einstellungen** in der Menüleiste ist jetzt aktiv.
2. Rufen Sie die Seite **Ereignisse** auf, um Details zu der festgestellten Bedrohung anzuzeigen.
3. Suchen Sie den Aktionslink neben den Bedrohungsdetails.

Sie können hier dieselben Aktionen auswählen wie in der Sophos Central Admin-Konsole. Schauen Sie sich die Liste auf der Seite **Warnhinweise** in der Sophos Central Hilfe an.

6.4 Sicherheitseinstellungen ändern

So ändern Sie Sicherheitseinstellungen:

1. Klicken Sie auf **Admin-Login** und geben Sie das Manipulationsschutz-Kennwort ein (das Sie vom Sophos Central-Administrator erhalten).
   Der Link **Einstellungen** in der Menüleiste ist jetzt aktiv.
2. Rufen Sie die Seite **Einstellungen** auf.
3. Aktivieren Sie das Häkchen bei **Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen**.
4. Mithilfe der Regler auf der Seite können Sie Sicherheitsfunktionen aktivieren bzw. deaktivieren.

Nach vier Stunden ändern sich die Einstellungen automatisch wieder in die zentral durchgesetzten Richtlinieneinstellungen.

Hinweis
Sie können die Einstellungen aber auch früher wieder zurückändern. Für einzelne Funktionen ist dies nicht möglich. Sie müssen die Option **Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen** deaktivieren. Dies wird für alle Funktionen übernommen.

6.5 Jetzt aktualisieren

So nehmen Sie die Aktualisierung vor:

1. Klicken Sie auf **Info**.
2. Klicken Sie auf **Jetzt aktualisieren**.

6.6 Fehlersuche

So beheben Sie Probleme:

1. Klicken Sie auf **Info**.
2. Klicken Sie auf **Diagnosetool ausführen**, um Daten zu dem Problem zu sammeln.

Sie können auch auf **Community Forum** klicken, um weitere Informationen zu erhalten.

6.7 Den Mac verschlüsseln

Mit der Funktion „Device Encryption“ wird die Festplatte des Macs mit der FileVault 2-Technologie verschlüsselt. Wenn Ihr Administrator **Device Encryption** aktiviert, wird der Dialog **Sophos Device Encryption** angezeigt.

1. Geben Sie im Dialog **Sophos Device Encryption** Ihr Kennwort für die Anmeldung ein und klicken Sie auf **Verschlüsseln**.
   Dadurch wird die Device Encryption aktiviert. Sie können aber auch auf **Später erinnern** klicken, wenn Sie den Prozess später starten möchten.
2. Ihr Wiederherstellungsschlüssel wird automatisch in Sophos Central gespeichert.

Sobald die Systemfestplatte verschlüsselt ist, werden automatisch interne Datenvolumes verschlüsselt. Verschlüsselte Festplatten werden beim Starten des Macs automatisch entsperrt. Wechselmedien wie USB-Laufwerke werden nicht verschlüsselt.

6.8 Zugriff auf den Mac, wenn Sie das Passwort vergessen haben

Wenn Sie sich bei Ihrem Mac nicht anmelden können, weil Sie Ihr Passwort für die Anmeldung vergessen haben, benötigen Sie einen Wiederherstellungsschlüssel.

Wenn Sie **Sophos Device Encryption** verwenden, ist der Schlüssel in Sophos Central gespeichert. Um Ihren Wiederherstellungsschlüssel abzurufen, haben Sie folgende Möglichkeiten:

- Melden Sie sich beim Sophos Self Service Portal an und folgen Sie den Anweisungen in der Sophos Central Hilfe.

- Bitten Sie Ihren Administrator, den Wiederherstellungsschlüssel für Sie abzurufen, wie unter FileVault-Wiederherstellung (Seite 10) beschrieben. Wenn Sie das Self-Service-Portal nicht nutzen können, ist dies die einzige Möglichkeit.

6.8.1 FileVault-Wiederherstellung

Führen Sie die folgenden Schritte aus, damit ein Administrator einen Wiederherstellungsschlüssel für Sie abruft.

1. Starten Sie Ihren Mac neu und warten Sie, bis die **Wiederherstellungsschlüssel-ID** angezeigt wird.
   Die **Wiederherstellungsschlüssel-ID** wird nur für kurze Zeit angezeigt. Um sie erneut anzuzeigen, müssen Sie den Mac neu starten.
2. Wenden Sie sich an Ihren Administrator und teilen Sie ihm die **Wiederherstellungsschlüssel-ID** mit.
   Ihr Administrator muss den Wiederherstellungsschlüssel für Ihren Mac in Sophos Central suchen und Ihnen den Schlüssel mitteilen.
3. Auf das Fragezeichen im Feld **Passwort** klicken.
   Eine Meldung wird angezeigt.
4. Auf den Pfeil neben der Meldung klicken, um zum Feld „Wiederherstellungsschlüssel“ zu wechseln.
5. Geben Sie den Wiederherstellungsschlüssel ein.
6. Den Anweisungen auf dem Bildschirm folgen, um ein neues Passwort zu erzeugen.
   Wenn Ihr Benutzerkonto aus Active Directory importiert wurde, klicken Sie im Dialog **Kennwort zurücksetzen** auf **Abbrechen** und bitten Sie Ihren Administrator, das Kennwort für Sie zurückzusetzen.
7. Benutzer müssen auf **Neuen Anmeldeschlüsselbund erstellen** klicken, falls sie dazu aufgefordert werden.

Sie haben dann wieder Zugriff auf Ihren Mac.

7 Warum wird meine Dateiübertragung blockiert?

Sie bekommen möglicherweise eine Meldung angezeigt, dass eine Dateiübertragung (z. B. Kopieren, Verschieben oder E-Mail-Versand von Dateien) blockiert wurde.

Das liegt daran, dass Ihr Unternehmen eine Richtlinie eingerichtet hat, mit der sichergestellt wird, dass Sie nicht aus Versehen sensible Informationen an Benutzer schicken, für die diese nicht bestimmt sind.

Es gibt zwei Arten von Meldungen:

Übertragung wurde blockiert

Wenn Sie die Meldung „Dateiübertragung blockiert“ erhalten, können Sie die Dateien nicht übertragen. Bei Ihrem Administrator erfahren Sie Näheres zu dieser Meldung.

Übertragung kann zugelassen werden

Wenn Sie die Meldung „Angeforderte Dateiübertragung blockiert“ erhalten, können Sie selbst entscheiden, ob die Dateien übertragen werden sollen. Bei Ihrem Administrator erfahren Sie Näheres zu dieser Meldung. Klicken Sie auf **Zulassen**, wenn Sie sich sicher sind, dass Sie den Vorgang ohne Bedenken fortsetzen können.

8 Weitere Hilfe

Sie können den technischen Support folgendermaßen anfordern:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com mit anderen Benutzern aus, die dasselbe Problem haben.
- Durchsuchen Sie die Wissensdatenbank des Sophos Support unter www.sophos.com/de-de/support.aspx.

9 Rechtliche Hinweise