SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Konfigurationsanleitung – Sophos Central Edition

Inhalt

1 Einleitung

Diese Anleitung beschreibt die Konfiguration von Sophos für Virtual Environments.

Dabei wird vorausgesetzt, dass Sie Sophos Central für die Verwaltung Ihrer Sicherheitssoftware verwenden.

Wenn Sie Sophos Enterprise Console verwenden, lesen Sie stattdessen in der Konfigurationsanleitung für Enterprise Console nach.

2 Konfigurieren von Richtlinien

Sie können Sophos für Virtual Environments mithilfe von Sophos Central Richtlinien konfigurieren.

Sie können nur den Richtlinientyp Threat Protection verwenden, aber Sie können nach Bedarf mehrere Richtlinien erstellen.

Standardmäßig wendet Sophos Central eine Threat Protection Basisrichtlinie auf alle Ihre VM-Sicherheitssysteme an. Die Einstellungen in der Richtlinie werden dann für die VM-Gastsysteme verwendet.

Diese Einstellungen bieten:

- Erkennung bekannter Malware.
- Überprüfungen in der Cloud zur Erkennung der aktuellsten Malware, die Sophos bekannt ist.
- Proaktive Erkennung von Malware, die zum ersten Mal erkannt wird.
- Automatische Bereinigung von Malware.

Details finden Sie in der Sophos Central Hilfe.

Sie können die Basisrichtlinie anpassen oder weitere Richtlinien erstellen, um verschiedene Einstellungen auf verschiedene VM-Sicherheitssysteme anzuwenden.

Richtlinie erstellen oder bearbeiten

So erstellen oder bearbeiten Sie eine Threat Protection-Richtlinie:

1. Öffnen Sie Sophos Central und gehen Sie zu **Server-Schutz > Richtlinien**.
2. Klicken Sie auf eine **Threat Protection** Richtlinie oder klicken Sie **Richtlinie hinzufügen**, um eine neue zu erstellen.
3. Wählen Sie auf der Registerkarte **Server** die VM-Sicherheitssysteme, denen Sie die Richtlinie zuweisen wollen.
4. Geben Sie auf der Registerkarte **Einstellungen** die gewünschten Einstellungen ein.

   Details zu den Optionen, die Sie für VM-Sicherheitssysteme verwenden können, finden Sie in den folgenden Abschnitten.

Live Protection

Verdächtige Dateien werden durch Abgleich mit aktuellen Malware-Daten in der SophosLabs-Datenbank überprüft.

Option	Unterstützt?
Live-Schutz verwenden	Ja
Beispiele von Malware automatisch an SophosLabs senden	Nein

Echtzeit-Scans

Für **Echtzeit-Scans** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Aktivieren oder Deaktivieren	Ja
Lokal scannen oder lokal und remote scannen	Ja
Beim Lesen	Nein
Beim Schreiben	Nein

Echtzeit-Scans - Internet

Für **Echtzeit-Scans - Internet** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Laufende Downloads scannen	Nein
Zugriff auf schädliche Websites blockieren	Nein
Nach Dateien mit geringer Reputation suchen	Nein

Beseitigung

Für **Beseitigung** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Automatische Bereinigung von Malware	Ja

Echtzeit-Scans - Optionen

Für **Echtzeit-Scans - Optionen** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Aktivitäten bekannter Anwendungen automatisch ausschließen	Nein
Erkennung schädlichen Verhaltens (HIPS)	Nein

Geplante Scans

Für **Geplante Scans** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Geplanten Scan aktivieren	Ja

Laufzeitschutz

Für **Laufzeitschutz** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Netzwerkdatenverkehr zu Command-and-Control-Servern erkennen	Nein

Option	Unterstützt?
Dokumente vor Ransomware schützen (CryptoGuard)	Nein
Sophos Security Heartbeat aktivieren	Nein

Scan-Ausschlüsse

Für **Scan-Ausschlüsse** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Globale Scan-Ausschlüsse Um diese zu bearbeiten, gehen Sie zu **Einstellungen > Globale Scan-Ausschlüsse**.	Ja
Richtlinie Scan-Ausschlüsse (Windows und Linux)	Ja
Richtlinie Heartbeat-Ausschlüsse (nur Windows)	Nein
DNS-Server ausschließen (nur Windows)	Nein

Desktop-Benachrichtigungen

Für **Desktop-Benachrichtigungen** stehen folgende Optionen zur Auswahl.

Option	Unterstützt?
Desktop-Benachrichtigungen für Threat Protection aktivieren	Nein

3 Überprüfen, ob VM-Gastsysteme geschützt sind

In diesem Abschnitt erfahren Sie, wie Sie überprüfen, ob Ihre VM-Gastsysteme geschützt sind. Sie haben folgende Möglichkeiten:

- Überprüfen der Schutzeinstellungen auf einem VM-Gastsystem.
- Testen der Echtzeit-Scan-Funktion auf einem VM-Gastsystem.
- Probleme mit Echtzeit-Scans lösen.

3.1 Überprüfen der Schutzeinstellungen

So überprüfen Sie, ob ein VM-Gastsystem geschützt ist:

1. Gehen Sie zu dem VM-Gastsystem und suchen Sie nach **Sicherheit und Wartung** im Startmenü. Falls Sie diese Option nicht finden, suchen Sie nach **Info-Center**.

   Achtung
   Wenn Sie keine dieser Optionen finden, gibt es für das VM-Gastsystem kein Windows Sicherheitscenter. Überprüfen Sie mithilfe der unter Testen der Echtzeit-Scanfunktion (Seite 5) beschriebenen Schritte, ob das VM-Gastsystem geschützt ist.

2. Klicken Sie auf den Dropdown-Pfeil neben **Sicherheit**. Es sollte angezeigt werden, dass Sophos für Virtual Environments aktiviert ist.

   Hinweis
   Sollte dies nicht der Fall sein, lesen Sie unter Probleme mit Echtzeit-Scans lösen (Seite 6) nach.

3.2 Testen der Echtzeit-Scanfunktion

Echtzeit-Scans sind der Hauptmechanismus zum Schutz vor Threats. Bei jedem Versuch, eine Datei zu öffnen, zu verschieben oder umzubenennen oder in eine Datei zu schreiben, scannt das Sophos VM-Sicherheitssystem die Datei. Der Zugriff wird nur erlaubt, wenn die Datei keine Bedrohung darstellt. Wenn Sie ein Programm ausführen, scannt das Sophos VM-Sicherheitssystem die exe-Datei und alle anderen Dateien, die von ihr geladen werden.

Wichtig
Stellen Sie sicher, dass Sophos Endpoint für Windows *nicht* auf Gastsystemen installiert ist, die mit einem Sophos VM-Sicherheitssystem geschützt werden.

So prüfen Sie, ob ein VM-Sicherheitssystem Dateien bei Zugriff scannt:

1. Rufen Sie eicar.org/86-0-Intended-use.html auf. Kopieren Sie die EICAR-Testzeichenfolge in eine neue Datei. Geben Sie der Datei einen Namen mit der Erweiterung „.com“ und speichern Sie sie auf einem der VM-Gastsysteme.
2. Versuchen, Sie auf einem VM-Gastsystem auf die Datei zuzugreifen.
3. Melden Sie sich bei Sophos Central an.
    - **Wenn Sie die automatische Bereinigung aktiviert haben**, gehen Sie zur Seite **Server** und klicken Sie auf das Sophos VM-Sicherheitssystem, um die Details aufzurufen. Auf der Registerkarte **Ereignisse** sollte zu sehen sein, dass die EICAR-Datei erkannt und entfernt wurde.
    - **Wenn Sie die automatische Bereinigung nicht aktiviert haben,** schauen Sie auf der Seite **Warnhinweise** nach. Im Info-Center sollte ein Warnhinweis für das Sophos VM-Sicherheitssystem angezeigt werden. Die EICAR-Datei wurde erkannt, aber nicht entfernt.

Wenn die EICAR-Datei nicht erkannt wurde, lesen Sie unter Probleme mit Echtzeit-Scans lösen (Seite 6) nach. Falls die EICAR-Datei nicht entfernt wurde, löschen Sie sie einfach.

3.3 Probleme mit Echtzeit-Scans lösen

Wenn Echtzeit-Scans nicht funktionieren:

1. Stellen Sie sicher, dass Echtzeit-Scans in der für das Sophos VM-Sicherheitssystem geltenden Serverrichtlinie aktiviert sind:
    a) Gehen Sie in Sophos Central zur Seite **Server**, suchen Sie nach dem Sophos VM-Sicherheitssystem und klicken Sie darauf, um die Details aufzurufen.
    b) Auf der Registerkarte **Zusammenfassung** sehen Sie unter **Zusammenfassung**, welche Threat Protection-Richtlinie auf den Server angewendet wird. Klicken Sie auf den Namen der Richtlinie.
    c) Gehen Sie in der Richtlinie zum Bereich **Echtzeit-Scans**. Stellen Sie sicher, dass **Scannen** aktiviert ist.
    d) Vergewissern Sie sich, dass das Sophos VM-Sicherheitssystem konform mit der Richtlinie ist.
2. Stellen Sie sicher, dass das VM-Gastsystem geschützt ist. Gehen Sie zum Host des Sophos VM-Sicherheitssystem und schauen Sie in der Protokolldatei nach. Details finden Sie unter "Anzeigen geschützter VM-Gastsysteme" in der Sophos for Virtual Environments Konfigurationsanleitung.
3. Stellen Sie sicher, dass im Windows Sicherheitscenter das VM-Gastsystem als von Sophos für Virtual Environments geschützt angezeigt wird.
4. Vergewissern Sie sich, dass keine Neustarts durch Microsoft-Updates ausstehen. Diese können verhindern, dass die Installation des Sophos Guest VM Agent abgeschlossen werden kann.
5. Vergewissern Sie sich, dass keine anderen Virenschutzprodukte installiert sind. Vergewissern Sie sich auf Serverplattformen, auf denen es kein Sicherheitscenter gibt, das Windows Defender nicht aktiv ist. Denken Sie daran, dass Sie mit Sophos für Virtual Environments keine VM-Gastsysteme schützen können, auf denen andere Virenschutzprodukte ausgeführt werden.
6. Wenn On-Access-Scans weiterhin nicht funktionieren, wenden Sie sich bitte an den technischen Support von Sophos.

4 Anzeigen von VM-Gastsystemen

Sie können Details zu allen VM-Gastsystemen wie folgt ansehen:

- Anzeigen verbundener VM-Gastsysteme (Seite 7). Dies können Sie in Sophos Central tun.
- Anzeigen geschützter VM-Gastsysteme (Seite 7).

"Verbundene" VM-Gastsysteme haben den Sophos-Agent installiert und können sich mit dem VM-Sicherheitssystem verbinden.

In der Regel ist ein verbundenes VM-Gastsystem auch geschützt. Wurde der Agent jedoch gerade erst installiert oder liegt ein Problem vor, hat unter Umständen noch keine Überprüfung auf Bedrohungen stattgefunden.

4.1 Anzeigen verbundener VM-Gastsysteme

So können Sie alle VM-Gastsysteme anzeigen, die mit einem Sophos VM-Sicherheitssystem verbunden sind.

1. Melden Sie sich an Sophos Central an.
2. Gehen Sie zu **Server-Schutz > Server**.
3. Suchen Sie in der Liste nach dem Sophos VM-Sicherheitssystem und klicken Sie darauf, um die Details anzusehen.
4. Suchen Sie auf der Registerkarte **Zusammenfassung** unter **Status Virtual Environments Verbundene VM-Gastsysteme**. Klicken Sie auf die angezeigte Zahl.

   Hinweis
   Sind keine VM-Gastsysteme eingeschaltet oder werden darauf noch Agents installiert, werden keine VM-Gastsysteme angezeigt.

5. Sie sehen eine Liste von VM-Namen und IP-Adressen.

   Sie können die Liste nach einem bestimmten VM-Gastsystem durchsuchen oder mithilfe des Filters Desktop- oder Server-VM-Gastsysteme anzeigen.

4.2 Anzeigen geschützter VM-Gastsysteme

Sie können alle VM-Gastsysteme anzeigen, die durch ein Sophos VM-Sicherheitssystem geschützt sind.

1. Gehen Sie zu dem Sophos VM-Sicherheitssystem. Sie benötigen dazu den Windows Explorer und die IP-Adresse.
2. Doppelklicken Sie auf die Freigabe **Protokolle**.
3. Geben Sie bei Aufforderung Ihre Anmeldedaten ein:
   - Der Benutzername lautet „sophos“.
   - Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos VM-Sicherheitssystem festgelegt haben.
4. Öffnen Sie **ProtectedGVMs.log**, um die geschützten VM-Gastsysteme anzuzeigen.

Hinweis: Die Datei ProtectedGVMs.log wird erst ab dem Moment angezeigt, ab dem das Sophos VM-Sicherheitssystem die VM-Gastsysteme schützt.

5 Überprüfen von VM-Gastsystemen

Das Sophos VM-Sicherheitssystem überprüft Dateien immer beim Zugriff, d. h. wenn sie geöffnet und geschlossen werden.

Das Sophos VM-Sicherheitssystem kann zudem einen vollständigen Scan aller VM-Gastsysteme durchführen. Sie können entweder einen Scan sofort oder zu bestimmten Zeiten ausführen.

Bei der vollständigen Überprüfung werden Threats erkannt, aber nicht entfernt.

Hinweis
Das Sophos VM-Sicherheitssystem plant Scans zeitlich so, dass der Host nicht zu sehr ausgelastet wird. Standardmäßig werden zwei VM-Gastsysteme gleichzeitig überprüft. Daher kann es etwas dauern, bis alle vom Sophos VM-Sicherheitssystem verwalteten VM-Gastsysteme überprüft sind.

VM-Gastsysteme je nach Bedarf überprüfen

So können Sie je nach Bedarf eine vollständige Überprüfung aller VM-Gastsysteme durchführen:

1. Melden Sie sich bei Sophos Central an.
2. Gehen Sie zur Seite **Server**.
3. Suchen Sie nach dem Sophos Security VM und klicken Sie darauf, um die Seite mit den Details aufzurufen.
4. Klicken Sie im linken Fensterbereich auf **Jetzt scannen**.

VM-Gastsysteme zu bestimmten Zeiten überprüfen

So führen Sie eine vollständige Überprüfung aller VM-Gastsysteme zu festen Zeiten aus:

1. Melden Sie sich bei Sophos Central an.
2. Gehen Sie zur Seite **Server**.
3. Suchen Sie nach dem Sophos Security VM und klicken Sie darauf, um die Seite mit den Details aufzurufen.
4. Suchen Sie auf der Registerkarte **Zusammenfassung** unter **Zusammenfassung** nach der geltenden Threat Protection-Richtlinie. Klicken Sie zum Bearbeiten auf die Richtlinie.
5. Gehen Sie in der Richtlinie zum Bereich **Geplante Scans**. Aktivieren Sie die Scans und geben Sie an, zu welchen Zeiten der Scan ausgeführt werden soll.

6 Was geschieht, wenn ein Threat erkannt wird?

Wenn das Sophos VM-Sicherheitssystem einen Threat auf einem VM-Gastsystem erkennt, wird:

- Der Threat blockiert.
- Versucht, den Threat automatisch zu entfernen.
- Ein Alert an Sophos Central gesendet, sofern Sie tätig werden müssen.

Hinweis
Das Sophos VM-Sicherheitssystem entfernt nicht automatisch Threats, die bei einem vollständigen Scan aller VM-Gastsysteme erkannt werden.

Was Sie in Sophos Central sehen

Sophos Central:

- Zeigt den Threat an, der blockiert wurde. Nähere Informationen finden Sie auf der Registerkarte **Ereignisse** auf der Seite mit dem Details zum Sophos VM-Sicherheitssystem.
- Anzeige eines Warnhinweises auf der Seite **Warnhinweise**. Angezeigt werden Informationen, um was für einen Threat es sich handelt, auf welchem VM-System er sich befindet und ob er entfernt werden kann.
- Entfernt den Warnhinweis, wenn die automatische Bereinigung erfolgreich war.

Wenn die automatische Bereinigung nicht verfügbar ist oder nicht erfolgreich war, werden Sie mit einem Warnhinweis auf der Seite **Warnhinweise** zu einer manuellen Bereinigung aufgefordert.

Weitere Informationen zur Bereinigung finden Sie unter Entfernen eines Threat (Seite 11).

Was der Benutzer auf dem VM-Gastsystem angezeigt bekommt

Erkennt das Sophos VM-Sicherheitssystem beim Versuch des Benutzers, auf eine Datei zuzugreifen, einen Threat, wird unter Umständen eine Meldung auf dem VM-Gastsystem angezeigt, die den Benutzer darüber informiert, dass kein Zugriff auf die Datei möglich ist. Dies hängt von der jeweiligen Anwendung ab, über die auf die Datei zugegriffen wird.

7 Entfernen eines Threat

In diesem Schritt wird das automatische und manuelle Entfernen von Threats beschrieben.

Informationen über eine Bedrohung und Hinweise zur Bereinigung finden Sie in Sophos Central auf der Seite **Warnhinweise**. Suchen Sie den Threat-Alert und klicken Sie auf den Threat-Namen.

Automatische Bereinigung

Das Sophos VM-Sicherheitssystem entfernt automatisch erkannte Bedrohungen.

Hinweis
Die automatische Bereinigung ist nicht möglich bei CDs, schreibgeschützten Dateisystemen und Medien oder auf Remote-Dateisystemen.

Manuelle Bereinigung

Sie können ein VM-Gastsystem manuell bereinigen.

Für eine manuelle Bereinigung muss das VM-Gastsystem wiederhergestellt werden. Beachten Sie, dass die möglicherweise Daten verlieren (Details siehe unten).

Wenden Sie eine der folgenden Methoden an:

- Löschen Sie das VM-Gastsystem und klonen Sie es erneut über das Vorlagenimage. Sie werden Ihre Daten verlieren.
- Stellen Sie auf dem VM-Gastsystem den letzten bekanntermaßen threatfreien Snapshot wieder her. Daten, die seit dem Erstellen des Snapshots hinzugefügt wurden, gehen verloren.

Ganz gleich, welche Methode Sie anwenden, führen Sie anschließend eine vollständige Überprüfung des VM-Gastsystems aus, um sicherzustellen, dass es virenfrei ist.

8 Anhang: VM-Sicherheitssysteme für die Migration von VM-Gastsystemen hinzufügen

Sie können jederzeit mehr VM-Sicherheitssysteme hinzufügen, um migrierende VM-Gastsysteme zu schützen

Wichtig
Sie müssen diese Schritte auf dem VM-Sicherheitssystem, das Sie hinzufügen möchten, und auf den vorhandenen VM-Sicherheitssystemen ausführen.

1. Öffnen Sie über SSH die Konfigurationsdatei additional_svms.txt zur Bearbeitung:
   /opt/sophos-svms/etc/additional_svms.txt
2. Bearbeiten Sie die IP-Adressen der VM-Sicherheitssysteme, die zum Schutz von VM-Gastsystemen zur Verfügung stehen.
   - Schreiben Sie eine IP-Adresse pro Zeile und verwenden Sie keine Trennzeichen. Zum Beispiel:
     1.2.3.4
     5.6.7.8
   - Sie müssen die IP-Adresse des Sophos VM-Sicherheitssystem, an das Sie derzeit angemeldet sind, nicht angeben.
3. Speichern und schließen Sie die Datei.
4. Überprüfen Sie unter /var/log/ssvm.log, ob beim Verarbeiten der Liste mit den zusätzlichen VM-Sicherheitssystemen Fehler aufgetreten sind.
   Sind keine Fehler aufgetreten, wird die aktualisierte Liste an alle verbundenen VM-Gastsysteme gesendet, so dass sie durch die neuen VM-Sicherheitssysteme geschützt sind.

9 Technischer Support

Sie können sich wie folgt an den technischen Support von Sophos wenden:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Begleitmaterial zu den Produkten finden Sie hier: www.sophos.com/de-de/support/documentation.aspx
- Öffnen Sie ein Service Ticket unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

10 Rechtliche Hinweise

Dritt-Lizenzen

Drittlizenzen für die Nutzung dieses Produkts finden Sie in folgendem Ordner im Sophos VM-Sicherheitssystem: `/usr/share/doc`.

Für einige Softwareprogramme wird Benutzern gemäß GNU General Public License (GPL) oder ähnlichen Lizenzen für kostenlose Software eine Lizenz oder Unterlizenz gewährt, die ihnen unter anderem das Recht geben, bestimmte Programme oder Teile von Programmen zu kopieren, zu verändern oder weiterzuverbreiten und Zugriff auf den Quellcode geben. Die GLP bestimmt, dass für unter der GLP lizenzierte Software, die an Benutzer in einem ausführbaren Binärformat verteilt wird, diesen Benutzern der Quellcode ebenfalls zur Verfügung gestellt werden muss. Für Software, die zusammen mit diesem Sophos-Produkt vertrieben wird, kann der Quellcode per E-Mail bei Sophos angefordert werden: savlinuxgpl@sophos.com.