SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Konfigurationsanleitung für Benutzen von Sophos Central

Inhalt

1 Einleitung

Diese Anleitung beschreibt die Konfiguration von Sophos for 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 Sophos Enterprise Console nach.

2 Konfigurieren von Richtlinien

Sie können Sophos for Virtual Environments mithilfe von Sophos CentralRichtlinien 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 Security VMs 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.

Zugehörige Aufgaben

Richtlinie erstellen oder bearbeiten (Seite 2)
Sie können Sophos for Virtual Environments mithilfe von Sophos CentralRichtlinien konfigurieren.

Verwandte Referenzinformationen

Richtlinieneinstellungen (Seite 2)
Die Optionen, die Sie für Security VMs verwenden können

2.1 Richtlinie erstellen oder bearbeiten

Sie können Sophos for Virtual Environments mithilfe von Sophos CentralRichtlinien konfigurieren.

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

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 Security VMs, denen Sie die Richtlinie zuweisen wollen.
4. Geben Sie auf der Registerkarte **Einstellungen** die gewünschten Einstellungen ein.

2.2 Richtlinieneinstellungen

Die Optionen, die Sie für Security VMs verwenden können

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

Option	Unterstützt?
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
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 6) beschriebenen Schritte, ob das VM-Gastsystem geschützt ist.

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

   Hinweis
   Sollte dies nicht der Fall sein, lesen Sie unter Probleme mit Echtzeit-Scans lösen (Seite 7) nach.

3.2 Testen der Echtzeit-Scanfunktion

Prüfen Sie, ob Echtzeit-Scans auf einem Sophos Security VM funktionieren.

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 Security VM die Datei. Der Zugriff wird nur erlaubt, wenn die Datei keine Bedrohung darstellt. Wenn Sie ein Programm ausführen, scannt das Sophos Security VM 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 Security VM geschützt werden.

So prüfen Sie, ob ein Sophos Security VM Dateien beim Zugriff scannt:

1. Gehen Sie zu http://2016.eicar.org/86-0-Intended-use.html und verwenden Sie die EICAR-Testdatei.
2. 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.
3. Versuchen, Sie auf einem VM-Gastsystem auf die Datei zuzugreifen.
4. Sie sich bei Sophos Central an.
   - Wenn Sie die automatische Bereinigung aktiviert haben, gehen Sie zur Seite **Server** und klicken Sie auf das Sophos Security VM, 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 Security VM 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 7) 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 Security VM geltenden Serverrichtlinie aktiviert sind:
   a) Gehen Sie in Sophos Central zur Seite **Server**, suchen Sie nach dem Sophos Security VM 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 Security VM konform mit der Richtlinie ist.
2. Stellen Sie sicher, dass das VM-Gastsystem geschützt ist. Gehen Sie zum Host des Sophos Security VM und schauen Sie in der Protokolldatei nach. Für weitere Informationen siehe Anzeigen geschützter VM-Gastsysteme (Seite 8).
3. Stellen Sie sicher, dass im Windows Sicherheitscenter das VM-Gastsystem als von Sophos for 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 for 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 8). Dies können Sie in Sophos Central tun.
- Anzeigen geschützter VM-Gastsysteme (Seite 8).

"Verbundene" VM-Gastsysteme haben den Sophos-Agent installiert und können sich mit dem Sophos Security VM 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 Security VM verbunden sind.

1. Sie sich bei Sophos Central an.
2. Gehen Sie zu **Server-Schutz > Server**.
3. Suchen Sie in der Liste nach dem Sophos Security VM 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 Security VM geschützt sind.

1. Gehen Sie zu dem Sophos Security VM. 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 Security VM 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 Security VM die VM-Gastsysteme schützt.

5 Überprüfen von VM-Gastsystemen

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

Das Sophos Security VM 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 Security VM 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 Security VM verwalteten VM-Gastsysteme überprüft sind.

- So können Sie je nach Bedarf eine vollständige Überprüfung aller VM-Gastsysteme durchführen:
  a) Sie sich bei Sophos Central an.
  b) Gehen Sie zur Seite **Server**.
  c) Suchen Sie nach dem Sophos Security VM und klicken Sie darauf, um die Seite mit den Details aufzurufen.
  d) Klicken Sie im linken Fensterbereich auf **Jetzt scannen**.
- So führen Sie eine vollständige Überprüfung aller VM-Gastsysteme zu festen Zeiten aus:
  a) Sie sich bei Sophos Central an.
  b) Gehen Sie zur Seite **Server**.
  c) Suchen Sie nach dem Sophos Security VM und klicken Sie darauf, um die Seite mit den Details aufzurufen.
  d) Suchen Sie auf der Registerkarte **Zusammenfassung** unter **Zusammenfassung** nach der geltenden Threat Protection-Richtlinie. Klicken Sie zum Bearbeiten auf die Richtlinie.
  e) 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 Security VM 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 Security VM 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 Security VM.
- 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 12).

Was der Benutzer auf dem VM-Gastsystem angezeigt bekommt

Wenn das Sophos Security VM eine Bedrohung erkennt, wenn ein Benutzer versucht, auf eine Datei zuzugreifen, wird der Zugriff auf diese Datei vom VM-Gastsystem blockiert. Wenn die für den Zugriff verwendete Anwendung dies tun kann, wird der Benutzer informiert, dass auf die Datei nicht mehr zugegriffen werden kann.

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 Security VM 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 Deinstallieren des Sophos Security VM

Stellen Sie zuvor sicher, dass die VM-Gastsysteme weiterhin geschützt sind. Gehen Sie zu dem Sophos Security VM und rufen Sie Anzeigen geschützter VM-Gastsysteme (Seite 8) auf. Weisen Sie dann die VM-Gastsysteme einem anderen Sophos Security VM mit ähnlichen Richtlinieneinstellungen zu.

Um ein Sophos Security VM zu deinstallieren, muss es gelöscht werden.

So weisen Sie Ihre VM-Gastsysteme neu zu:

1. Deinstallieren Sie den Sophos Guest VM Agent (siehe Deinstallieren des Sophos Guest VM Agent).
2. Installieren Sie den Sophos Guest VM Agent mit der neuen IP-Adresse für das Sophos Security VM neu.

Sobald Sie die VM-Gastsysteme verschoben haben, können Sie das Sophos Security VM löschen. Verfahren Sie hierzu wie folgt:

3. Gehen Sie zu Ihrem Hypervisor.
4. Schalten Sie das Sophos Security VM aus.
5. Löschen Sie das VM-System.

9 Deinstallieren des Sophos Guest VM Agent

Sie können den Sophos Guest VM Agent über die Systemsteuerung löschen.

1. Öffnen Sie auf dem VM-Gastsystem die **Systemsteuerung**.
2. Klicken Sie auf **Programme und Funktionen**.
3. Wählen Sie die folgenden Funktionen aus und klicken Sie auf **Deinstallieren**:
   - Sophos for Virtual Environments
   - Sophos Guest VM Scanning Service
   - Sophos Virus Removal Tool.

10 Anhang: Security VMs für die Migration von VM-Gastsystemen hinzufügen

Sie können jederzeit weitere Security VMs hinzufügen, um migrierende VM-Gastsysteme zu schützen

Wenn Sie in Zukunft weitere Sophos Security VMs erstellen möchten, sollten Sie IP-Adressen für die Sophos Security VMs reservieren, die Sie wahrscheinlich hinzufügen werden. Erstellen Sie dazu eine vorab aufgefüllte Master-Version dieser Datei. Diese Datei sollte alle IP-Adressen der Sophos Security VMs enthalten, die Sie haben und die Sie in der Zukunft haben werden. Sie können diese Datei dann in jede Sophos Security VM kopieren, wenn Sie sie erstellen.

Wichtig
Sie müssen diese Schritte auf dem Sophos Security VM, das Sie hinzufügen möchten, und auf den vorhandenen Security VMs ausführen.

1. Öffnen Sie eine Konsole für das Sophos Security VM.
2. Melden Sie sich an:

   Der Benutzername lautet „sophos“.

   Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos Security VM festgelegt haben.
3. Öffnen Sie die Konfigurationsdatei additional_svms.txt zur Bearbeitung, indem Sie folgenden Befehl ausführen: `sudo vi /opt/sophos-svms/etc/additional_svms.txt`
4. Bearbeiten Sie die Datei um IP-Adressen der Security VMs hinzuzufügen oder zu entfernen, die zum Schutz von zu migrierenden VM-Gastsystemen zur Verfügung stehen. Geben Sie eine IP-Adresse pro Zeile ohne zusätzliche Trennzeichen an.

   a) Drücken Sie `i` um den Bearbeitungsmodus in vi zu öffnen.

   b) Schreiben Sie eine IP-Adresse pro Zeile und verwenden Sie keine Trennzeichen. Zum Beispiel:

      1.2.3.4
      5.6.7.8

   c) Sie müssen die IP-Adresse des Sophos Security VM, an das Sie derzeit angemeldet sind, nicht angeben.

   d) Drücken Sie `Esc` um den Bearbeitungsmodus in vi zu verlassen.

   e) Speichern und schließen Sie die Datei durch Eingeben von `:wq`.
5. Überprüfen Sie unter `/var/log/ssvm.log`, ob beim Verarbeiten der Liste mit den zusätzlichen Security VMs Fehler aufgetreten sind.

   Sind keine Fehler aufgetreten, wird die aktualisierte Liste an alle verbundenen VM-Gastsysteme gesendet, so dass sie durch die neuen Security VMs geschützt sind.

11 Anhang: Hinzufügen von CPUs für das Sophos Security VM

Wenn sich eine große Anzahl an VM-Gastsystemen auf einem Host befindet, müssen Sie sicherstellen, dass das Sophos Security VM über ausreichend Rechenleistung zum Scannen der Dateien beim Start verfügt.

Fügen Sie hierzu mehr CPUs für das Sophos Security VM hinzu. Dies können Sie jederzeit tun.

Je nach Art der Last kann durch das Hinzufügen von CPUs auch die Systemleistung insgesamt verbessert werden.

CPUs in VMware ESXi hinzufügen

Fügen Sie CPUs wie folgt hinzu:

1. Schalten Sie das Sophos Security VM aus.
2. Wählen Sie in vSphere Client das Sophos Security VM aus.
3. Wählen Sie **Edit SettingsHardwareCPUs.** Geben Sie dann die Anzahl der CPUs an.

CPUs in Microsoft Hyper-V hinzufügen

Fügen Sie CPUs wie folgt hinzu:

1. Klicken Sie auf **Start**, wählen Sie **Verwaltung** und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Ergebnisbereich unter **Virtuelle Computer** das Sophos Security VM aus.
3. Klicken Sie im Bereich **Aktion** unter dem Namen des virtuellen Computers auf **Einstellungen**.
4. Klicken Sie auf **Prozessor** und geben Sie die Anzahl von Prozessoren ein.

12 Technische Unterstützung

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- 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.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

13 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.