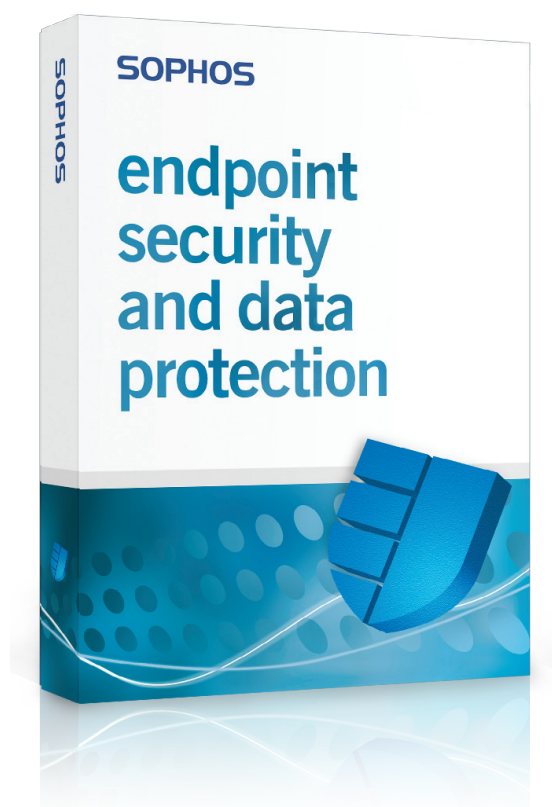


# Sophos Endpoint Security and Data Protection: Reviewer's Guide

**SOPHOS**





## WILLKOMMEN

Willkommen beim Reviewer's Guide zu Sophos Endpoint Security and Data Protection – der vollständig integrierten, skalierbaren Endpoint Security-Lösung von Sophos. Das vorliegende Dokument macht Sie mit den Software-Elementen von Sophos Endpoint Security and Data Protection vertraut: Management-Konsole, Anti-Virus, Client Firewall, Data Control, Device Control, Application Control, Verschlüsselung und Network Access Control.

Dieser Guide soll Ihnen einen Überblick über die umfassenden Funktionen von Sophos Endpoint Security and Data Protection verschaffen. Er vermittelt Ihnen einen Einblick in den Beitrag, den Sophos Endpoint Security and Data Protection mit dem derzeit kostengünstigsten und zuverlässigsten Schutz vor bekannten und unbekanntem Bedrohungen sowie Datenverlusten für Ihr Unternehmen leisten kann. Sie können sich auf andere wichtige Aufgabenbereiche konzentrieren und so Kontinuität und Effizienz Ihrer Abläufe optimieren.

Bei Fragen zu Preisen und Kaufoptionen in Bezug auf Sophos Endpoint Security and Data Protection wenden Sie sich bitte an Ihren Sophos Account Manager. Auf unserer Homepage erfahren Sie, wer für Ihren Standort zuständig ist:

[www.sophos.de/companyinfo/contacting](http://www.sophos.de/companyinfo/contacting)

Eine Testversion können Sie über folgende Adresse anfordern:

[www.sophos.de/products/enterprise/free-trials/](http://www.sophos.de/products/enterprise/free-trials/)

Die Installations-Anleitung finden Sie unter:

[www.sophos.de/support/docs](http://www.sophos.de/support/docs)

## INHALT

<b>1 UMFASSENDE SCHUTZ FÜR ENDPOINTS</b>	<b>5</b>
Übersicht zu Sophos Endpoint Security and Data Protection	
<b>2 EINE EINZIGE, ZENTRALE UND AUTOMATISIERTE KONSOLE</b>	<b>8</b>
Übersicht zur Sophos Enterprise Console	
<b>3 SCHUTZ FÜR WINDOWS-SYSTEME</b>	<b>24</b>
Übersicht zu Sophos Endpoint Security and Control, Sophos Client Firewall, Sophos NAC und SafeGuard Disk Encryption	
<b>4 SCHUTZ FÜR NICHT-WINDOWS-SYSTEME</b>	<b>30</b>
Übersicht zu Sophos Anti-Virus für Mac OS X, Linux und UNIX	
<b>ANHÄNGE</b>	
<b>I ENDPOINT SECURITY AND DATA PROTECTION TESTEN</b>	<b>33</b>
Empfohlenes Testnetzwerk	
<b>II DER EICAR-TESTVIRUS</b>	<b>36</b>
<b>III ANDERE PRODUKTE UND SERVICES VON SOPHOS</b>	<b>37</b>

## SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

# 1 UMFASSENDE SCHUTZ FÜR ENDPOINTS

## ÜBERSICHT ZU SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

Sophos gestaltet die Sicherung Ihrer Desktops, Laptops, Handhelds und Fileserver vor bekannten und unbekanntem Bedrohungen jetzt noch einfacher und schützt Ihr Unternehmen vor versehentlichen Datenverlusten.

### Umfassender Schutz

Dank des kombinierten Sophos Anti-Virus-Agent zum Schutz vor Malware jeglicher Art entfällt der Bedarf an zahlreichen Einzelprodukten zum Abwenden verschiedenartiger Bedrohungen. Mit nur einem Scan schützen Sie Ihr Unternehmen vor Viren, Spyware, Adware, Rootkits und potenziell unerwünschten Anwendungen (PUAs). Gleichzeitig können Sie die Installation und Verwendung nicht autorisierter Software (z.B. VoIP, Instant Messaging und Peer-to-Peer-Dateifreigabe [P2P]) sowie den Einsatz von Wechselmedien und drahtlosen Netzwerkprotokollen kontrollieren und die Übertragung sensibler Daten überwachen. Mit unserer lückenlosen Festplattenverschlüsselung für Computer und unseren Verschlüsselungsoptionen für Daten auf Wechselmedien beugen Sie Datenverlusten vor und sorgen für einen sicheren Informationsaustausch mit Dritten.

### Vereinfachte, automatisierte Konsole

Die automatisierte Sophos Enterprise Console ist der zentrale Punkt, über den Installationen, Updates und Reports des Endpoint-Schutzes für Ihre gesamte IT-Umgebung vorgenommen werden können. Eine Konsole kann zehntausende Windows-, Mac-, Linux- und UNIX-Computer verwalten. Durch die Vereinfachung und Automatisierung des Schutzes werden Kosten eingespart. Es sind weniger Arbeitsschritte erforderlich und Ihr gesamtes Netzwerk wird überschaubarer. Zusätzlich haben Sie durch unsere rollenbasierte Administration die Möglichkeit, bestimmte Aufgaben an User zu delegieren und so Ihren eigenen Arbeitsaufwand zu reduzieren, ohne die übergreifende Kontrolle der Sicherheitsrichtlinien aus der Hand geben zu müssen.

### Eine Lösung für sämtliche Plattformen

Mit der Lizenz für Endpoint Security and Data Protection erwerben Sie Zugriff auf Software für den Schutz von mehr als 25 Plattformen – eine in der Branche unübertroffene Abdeckung – darunter Windows, Mac OS X, Linux, UNIX, NetWare, NetApp Storage Systems und Windows Mobile.

## Lückenloser Datenschutz

Eine ideale Kombination verschiedener Technologien stellt sicher, dass Ihre Daten vor versehentlichen Verlusten geschützt sind. Der in den Endpoint Agent integrierte DLP-Inhaltsscan überwacht Übertragungen sensibler Daten auf Wechselmedien und in Internet-Anwendungen wie E-Mail-Programme, Internet-Browser und Instant Messaging. Durch Einsatz eingehender Kontrollen für Wechselmedien haben Sie die Entscheidungsgewalt darüber, welche Geräte zugelassen werden, ob nur verschlüsselte Geräte verwendet werden dürfen oder aber nur Lesezugriff gewährt wird. Unsere zuverlässige Festplattenverschlüsselung sichert zudem Ihre Daten auf mobilen Computern und verhindert, dass gespeicherte Informationen bei Verlust eines Laptops in die falschen Hände geraten.

## Integriertes Know-how

Das Fachwissen der SophosLabs™ über Malware, Spam und das Internet sorgt dafür, dass Sie den schnellsten und besten Schutz erhalten. Einzigartige Verfahren wie Behavioral Genotype® Protection in Kombination mit schnellen und kompakten Updates von Virenkennungen stoppen neue und unbekannte Malware und sorgen dafür, dass Sophos Symantec und McAfee in unabhängigen Tests immer wieder übertrifft.



## Endpoint-Compliance

Sophos Endpoint Security and Data Protection sorgt durch den Einsatz von Sophos NAC zur Überprüfung und Kontrolle aller Endpoints für lückenlose Endpoint-Compliance. Sophos NAC überprüft, ob der Virenschutz und andere Sicherheitsanwendungen aktiv und aktuell sind und ob Betriebssysteme über die nötigen Patches verfügen und ordnungsgemäß aktualisiert wurden. Indem anfällige Computer vor Gewähren von Netzwerkzugriff in die Quarantäne verschoben oder auf den aktuellen Sicherheitsstand gebracht werden, verringert sich das Risiko einer Malware-Infektion. Sophos NAC schützt über die gesamte Dauer der User-Sitzung und führt in regelmäßigen Abständen Prüfungen durch.

Gründe	Vorteile von Sophos
Vertrauenswürdiger Anbieter	Mit über 20 Jahren Erfahrung beim Schutz von Unternehmen vor bekannten und unbekanntem Bedrohungen ist es für uns ein leichtes, schnell auf entstehende Bedrohungen reagieren zu können – ganz gleich, wie komplex diese auch sein mögen.
Einfaches und intelligentes Konzept	Die Sophos Enterprise Console ermöglicht eine kosteneffiziente, zentrale und intuitive Verwaltung zahlreicher Plattformen und sorgt so für netzwerkübergreifende Einsicht und Kontrolle.
Schnelle Reaktion	Die SophosLabs begegnen neuen Bedrohungen durch ständige Wachsamkeit. Experten analysieren neue Malware in allen Zeitzonen und stellen schnelle, kompakte Updates bereit.
Hervorragender Support	Unser technischer Support wird von einem global agierenden Team aus Sophos Experten rund um die Uhr an 365 Tagen im Jahr bereitgestellt. Unsere Support-Techniker verfügen über praktische und eingehende Erfahrung und sind Grund dafür, dass Sophos den branchenweit höchsten Grad an Kundenzufriedenheit verzeichnen kann.
Einfache Lizenzstruktur	Über ein einziges Lizenz-Abonnement erhalten Sie regelmäßig automatische Updates und Upgrades für sämtliche Neuveröffentlichungen sowie rund um die Uhr verfügbaren Support durch hausinterne Sophos Experten – ganz ohne versteckte Kosten.
Reine Unternehmensorientierung	Sophos verkauft nur an Unternehmenskunden. So können wir Planung, Support und Forschung auf die Anforderungen von Unternehmen statt auf Endverbraucher konzentrieren.

Tabelle 1: Warum Kunden Sophos vertrauen

## Test der Hauptfunktionen

Vor Durchführung eines Tests sollten Sie folgende Punkte beachten und als Grundlage für einen Vergleich mit Konkurrenzprodukten verwenden:

- Können Sie den Schutz für all Ihre Plattformen von einer einzigen Management-Konsole verwalten?
- Wie viele Installationsvorgänge sind nötig, um eine einheitliche Endpoint-Schutz-Abdeckung zu gewährleisten – Anti-Virus, Anti-Spyware, Firewall, HIPS, Application Control, Device Control, Data Control und Network Access Control?
- Wie einfach lässt sich das Produkt im Unternehmen installieren und einsetzen? Kann zur Beschleunigung dieses Prozesses Active Directory (AD) eingesetzt werden?
- Kann eine Synchronisierung mit AD vorgenommen werden und können neue Computer bei Zugriff auf das Netzwerk automatisch mit Schutzupdates versorgt werden?
- Wie einfach lässt sich der durch verwaltete und unverwaltete Computer erfolgende Netzwerkzugriff überprüfen und kontrollieren?
- Bietet die Management-Konsole ein Dashboard mit Echtzeitinformationen zum Status und zu Benachrichtigungen?
- Wie leicht ist das Produkt zu verwalten? Wie viele Schritte und wie viel Zeit werden zur Erledigung üblicher Verwaltungsaufgaben wie dem Abändern und Zuweisen von Richtlinien zu Gruppen benötigt?
- Wie wirksam sind die proaktiven Erkennungs-/HIPS-Verfahren und welcher Konfigurationsaufwand muss für wirksamen Schutz betrieben werden?
- Kann der Endpoint Agent den Transfer sensibler Daten auf Wechselmedien oder Internet-Anwendungen (z.B. E-Mail, Internet-Browser und Instant Messaging) überwachen?
- Wie einfach ist es, die Verwendung von Wechselmedien zu kontrollieren und welche unterschiedlichen Enforcement-Optionen stehen bereit?
- Wie einfach kann ein User daran gehindert werden, legitime Anwendungen wie IM, P2P, VoIP und Spiele, deren Einsatz auf Ihrem Unternehmensnetzwerk Sie unterbinden möchten, zu downloaden und zu installieren? Wie viel Arbeitsaufwand ist mit der Aktualisierung von Anwendungslisten verbunden?
- Wie viel Speicherbedarf benötigt der Client und wie häufig und in welcher Größe werden die Schutzupdates eingespielt?
- Stehen fachkundige technische Support-Experten regional, rund um die Uhr und ohne Aufpreis zur Verfügung?

## SOPHOS ENTERPRISE CONSOLE

## 2 EINE EINZIGE, ZENTRALE UND AUTOMATISIERTE KONSOLE

### ÜBERSICHT ZUR SOPHOS ENTERPRISE CONSOLE

Die Sophos Enterprise Console ermöglicht eine einfachere und geschicktere Verwaltung Ihres Endpoint-Schutzes auf Basis von Richtlinien. Mit ihr können Sie Tausende von Windows-, Mac-, Linux- und UNIX-User über eine einzige Konsole verwalten.

Problemlose Verwaltung und Handhabung von Richtlinien für das gesamte Netzwerk, Skalierbarkeit und zentrale, gezielte Bereinigung mit dieser Konsole sorgen für enorme Einsparungen bei den wiederkehrenden Kosten. Sicherheitslösungen sind oft zu komplex und mit einem übermäßigen Verwaltungsaufwand verbunden. Die Enterprise Console verfolgt ein einfaches, integriertes Konzept und ermöglicht so ein schnelles Vorgehen gegen neue und potenzielle Bedrohungen. In diesem Abschnitt lernen Sie wichtige Funktionen der Enterprise Console sowie die damit verbundenen Vorteile kennen.

#### EINMALIGE INSTALLATION

### Endpoint-Schutz und Entfernung von alten Sicherheitslösungen

Mit Endpoint Security and Data Protection können Sie über nur eine Konsole Virenschutz, Client Firewall und Network Access Control-Komponenten (NAC) auf Endpoint-Computern installieren und verwalten. Um Ihnen auch den Wechsel von Ihrer bestehenden Lösung zu Endpoint Security and Data Protection noch einfacher zu gestalten, haben Sie ab sofort die Möglichkeit, Ihre alte Sicherheitssoftware während der Installation zu entfernen.

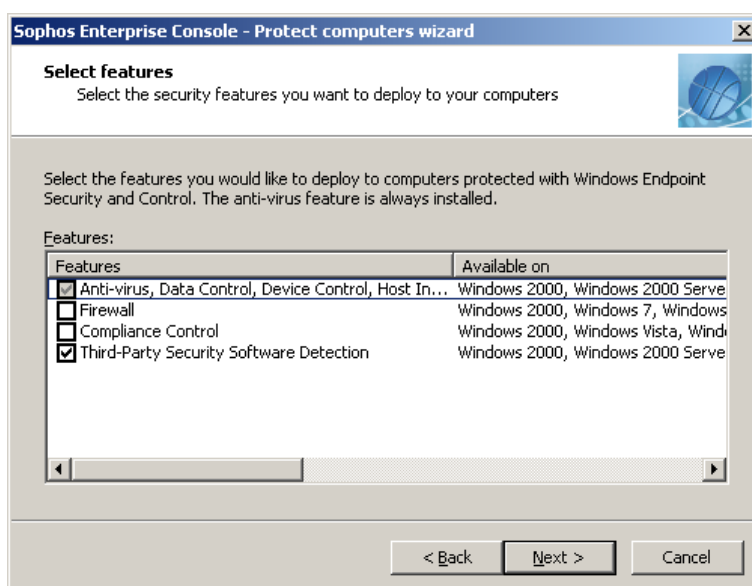


Abbildung 1: Einmalige Installation

## INTEGRATION UND SYNCHRONISIERUNG VON ACTIVE DIRECTORY

### Schnelle Installation und automatischer Schutz

Sophos Endpoint Security and Data Protection erleichtert die Suche nach Computern im Netzwerk durch die Replikation der Active Directory-Gruppen und der Client-Struktur in die Enterprise Console.

Nach der Replikation können Sie Active Directory und die Enterprise Console synchronisieren, damit Änderungen bei Active Directory automatisch auch in die Enterprise Console übernommen werden. So sind neue Clients sofort bei der Integration ins Netzwerk geschützt. Die Enterprise Console überprüft Active Directory standardmäßig jede Stunde auf Änderungen.

Falls Sie Active Directory nicht verwenden, stehen zwei Alternativen für die schnelle Erfassung von Computern zur Verfügung:

- Integrierte Netzwerksuche
- Suche anhand von IP-/Subnetzbereich

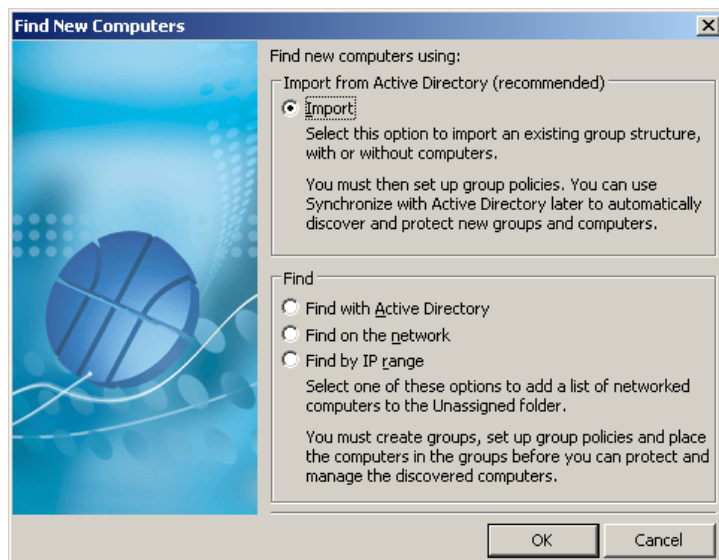


Abbildung 2: Schnelle Suche nach neuen Computern

## DASHBOARD

### Mehr Übersichtlichkeit und automatische Benachrichtigungen

Wird ein Virus, Spyware, Adware, verdächtiges Element oder eine potenziell unerwünschte Anwendung entdeckt, wird automatisch eine Benachrichtigung generiert, welche auf dem Dashboard zur Anzeige gebracht wird.

Das Infektionsrisiko im Netzwerk wird auf dem Dashboard der Enterprise Console angezeigt, das Benachrichtigungen von Windows-, Mac-, Linux- und UNIX-Computern erhält und den Status in Blau (OK), Gelb (Warnung) oder Rot (Kritisch) darstellt.

Mit nur einem Mausklick können Sie:

- Filter anwenden, um die Computer hervorzuheben, deren Virenschutz veraltet ist oder bei denen Malware erfasst wurde, um eine Übersicht über die Bereiche im Netzwerk zu erhalten, die Ihr Eingreifen erfordern.
- Schwellenwerte ändern, bei deren Erreichen sich die Farbe der Statusanzeige auf dem Dashboard ändert.

- automatische Benachrichtigungen aktivieren, wenn die von Ihnen festgelegten Schwellenwerte fast erreicht sind.

Dank dieser Funktionen erhalten Sie Benachrichtigungen über potenzielle Sicherheitsprobleme, ohne sich erst bei der Konsole anmelden zu müssen.

Malware-Benachrichtigungen werden standardmäßig auch auf jedem Computer angezeigt, auf dem Malware, PUAs oder nicht erlaubte Anwendungen erfasst wurden. Sie selbst oder bestimmte User können per E-Mail und SNMP benachrichtigt werden, wenn Viren, PUAs oder Fehler auf einem Computer der Gruppe vorliegen. Für jeden auf dem Computer erfassten Virus wird eine Verknüpfung zum entsprechenden Eintrag im Virenverzeichnis auf der Sophos Website angezeigt.

## Verfolgen kritischer Ereignisse

Wenn ein Application Control-, Firewall-, Data Control- oder Device Control-Ereignis auf einem Endpoint-Computer registriert wird (z.B. wenn eine Anwendung von der Firewall blockiert wird), wird dieses an die Enterprise Console gemeldet und kann im entsprechenden Ereignisfenster eingesehen werden.

## Übersichtliches Dashboard

Die leichte Einsehbarkeit der Problembereiche ist ein großer Vorteil, und beim Überschreiten der Sicherheits-Schwellenwerte werden automatische E-Mail-Benachrichtigungen verschickt.

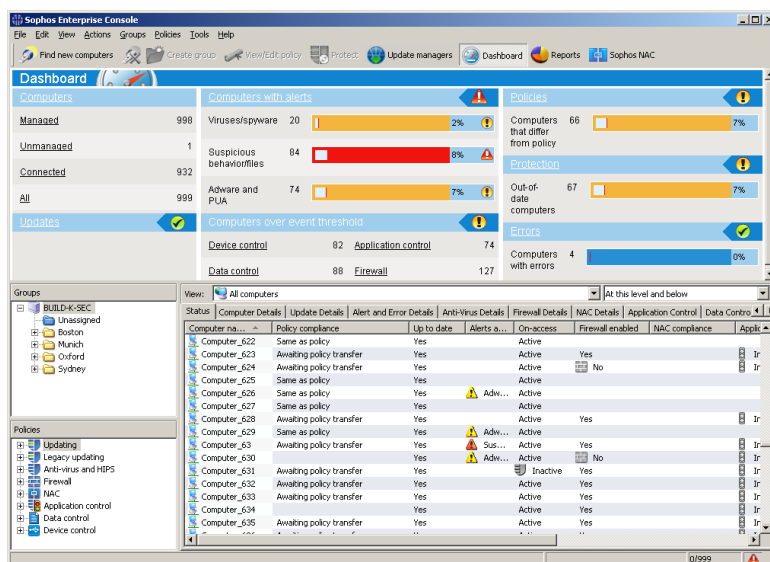


Abbildung 3: Security Dashboard der Sophos Enterprise Console

Mit dem Ereignisfenster können Ereignisse im Netzwerk schnell und einfach nachverfolgt werden. Durch das Setzen von Filtern besteht ferner die Möglichkeit, Listen ausgewählter Ereignisse zu generieren (z.B. eine Liste aller Data Control-Ereignisse für einen bestimmten User innerhalb der letzten sieben Tage).

Die Anzahl an Computern mit Ereignissen über einen spezifischen Schwellenwert innerhalb der letzten sieben Tage wird im Dashboard angezeigt. Außerdem besteht die Möglichkeit, Benachrichtigungen an ausgewählte Empfänger zu versenden, sobald ein Ereignis auftritt.

## SMART VIEWS

### Gezielte Bereinigung

Die Bereinigung eines großen Netzwerks nach einem Angriff kann äußerst kostspielig und zeitaufwändig sein. Die Enterprise Console ermöglicht die zentrale Bereinigung per Remote-Zugriff auf Dateien, Registrierungseinträge und laufende Prozesse. Smart Views bietet dem Administrator an einer einzelnen Konsole einen kompletten Überblick über den Sicherheitsstatus aller Computer im Netzwerk und ermöglicht die Bestimmung und Bereinigung genau der Computer, bei denen ein Handlungsbedarf besteht, z.B. bei Richtlinienverstößen oder wenn der Virenschutz aktualisiert werden muss.

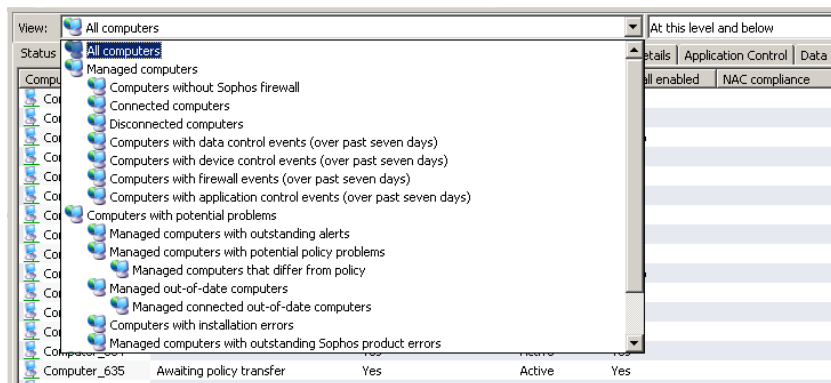


Abbildung 4: Smart Views

## SOPHOS UPDATE MANAGER

### Schnelle, von zentraler Stelle aus verwaltete Updates

Der Sophos Update Manager stellt sicher, dass das Netzwerk dank automatischer Updates der Sophos Sicherheitssoftware stets bestens geschützt ist. Ein Update Manager wird gemeinsam mit der Enterprise Console installiert und über diese verwaltet.

Nach erfolgreicher Konfiguration übernimmt der Update Manager folgende Aufgaben:

- Er verbindet sich in zeitgesteuerten Abständen mit einem Archiv zur Datenverteilung direkt bei Sophos oder in Ihrem eigenen Netzwerk.
- Er lädt relevante Updates der Sicherheitssoftware herunter, die der Administrator im Rahmen seiner Lizenzierung abonniert hat.
- Er platziert die aktualisierte Software zur Installation auf Endpoint-Computern in einer oder mehreren Netzwerkfreigaben.

Das Update der Endpoints erfolgt dann automatisch über die Netzwerkfreigaben und in Einklang mit der geltenden Update-Richtlinie.

## ACTIVEPOLICIES

### Vereinfachte Einrichtung und Durchsetzung von Richtlinien

Mit Sophos ActivePolicies™ können Sie Richtlinien unabhängig von Benutzergruppen schnell und intuitiv im gesamten Netzwerk einsetzen. Somit kann eine Richtlinie gleichzeitig auf mehrere Gruppen übertragen werden. ActivePolicies erleichtern Ihnen das Enforcement von Richtlinien in sieben Hauptbereichen.

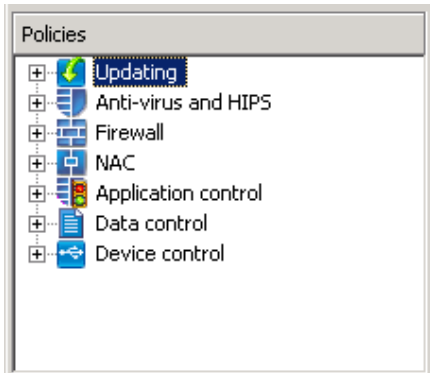


Abbildung 5: ActivePolicies

### Aktualisieren von Richtlinien

Über die Enterprise Console sorgen Sie dafür, dass Ihre Computer stets über den neusten Schutz verfügen. Update-Zeitpunkte für bestimmte Teile des Netzwerks sowie Standorte, mit denen Computer sich für Updates verbinden, sind individuell konfigurierbar. Diese Funktion ist besonders hilfreich, wenn sich Ihre Unternehmensnetzwerke über mehrere Zeitzonen erstrecken oder Mitarbeiter zu unterschiedlichen Zeiten an ihren Computern arbeiten – insbesondere bei der Verbindungsherstellung ortsferner Laptops zum Netzwerk. Dank Überwachung der automatischen Update-Einstellungen wird Ihr Netzwerk nur minimal belastet.

Ferner haben Sie die Möglichkeit, Einstellungen für Ihr Software-Abonnement individuell zu konfigurieren. So können Sie genau festlegen, welche Versionen der Endpoint-Software von Sophos für jede einzelne Plattform heruntergeladen werden. Das Standard-Abonnement beinhaltet die neueste Software für Windows 2000 und neuere Versionen.

Durch Bandbreitenregulierung verhindern Sie, dass Computer die gesamte Bandbreite für Updates nutzen, wenn andere Vorgänge erforderlich sind, z.B. das Abrufen von E-Mails.

### Richtlinien für Virenschutz und HIPS – Schutz vor Viren, Spyware, PUAs und Übergriffen

Mit der Implementierung unseres Virenschutzes erhalten Sie ohne zeitaufwändige Installation und Konfiguration ein vollwertiges Host Intrusion Prevention System (HIPS). Malware, verdächtige Dateien und Verhaltensmuster werden dank Laufzeitverhaltensanalyse, Pufferüberlaufschutz und proaktivem Schutz noch vor der Ausführung von Code erkannt.

Im Rahmen der Richtlinie können Sie eine Vielzahl von Optionen für Scans des gesamten Netzwerks einrichten. So lassen sich die Anforderungen für zugriffs-, zeit- oder bedarfsgesteuerte Internet-Scans festlegen und sogar Dateitypen ausschließen, die kein Sicherheitsrisiko darstellen. Standardmäßig gilt für alle Computer die folgende Standard-Richtlinie:

- Scannen von Dateien, die für Malware anfällig sind
- Zugriffsverweigerung auf Dateien, die Viren, Spyware usw. enthalten
- Anzeigen von Benachrichtigungen auf Computern, auf denen Viren oder PUAs erkannt wurden

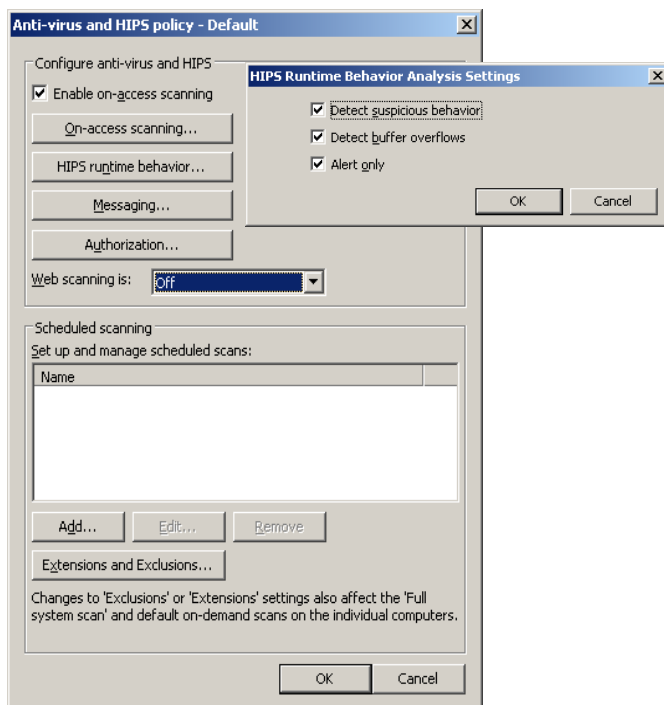


Abbildung 6: Konfiguration von Virenschutz und HIPS-Richtlinie

### Richtlinien zur Kontrolle von Anwendungen

Anwendungen wie VoIP, IM und P2P führen in Unternehmen vermehrt zu Problemen mit den Sicherheitsanforderungen, der Einhaltung von Gesetzen und der Arbeitsleistung. IT-Abteilungen müssen daher die unbefugte Installation und Verwendung derartiger Software unterbinden. Sophos integriert die Erkennung so genannter Controlled Applications in die Überprüfung auf Malware und PUAs. Damit entfällt die Notwendigkeit, spezielle Einzelprodukte anzuschaffen und zu implementieren.

Standardmäßig sind sämtliche Controlled Applications zugelassen. Mit der Enterprise Console haben Sie jedoch die Möglichkeit, Richtlinien für Endpoint-Computer-Gruppen ganz nach den individuellen Sicherheitsanforderungen bestimmter Standorte oder Abteilungen zu konfigurieren. Beispielsweise kann VoIP für unternehmensinterne Computer ausgeschaltet, für externe Computer jedoch zugelassen werden. Zum Sperren einer Anwendung brauchen Sie diese nur in die Spalte für gesperrte Software zu verschieben.

Die Liste der Controlled Applications wird von Sophos zur Verfügung gestellt und regelmäßig aktualisiert. Ein eigenständige Ergänzung der Liste mit neuen Anwendungen ist nicht möglich. Sie können jedoch eine Anfrage an Sophos senden, wenn Sie ein Hinzufügen einer neuen legitimen Anwendung zur Kontrolle in Ihrem Netzwerk wünschen.

Eine komplette Auflistung der kontrollierbaren Anwendungen finden Sie hier: <http://www.sophos.de/security/analyses/controlled-applications/>

### Folgende Anwendungen können u.a. blockiert werden:

- VoIP
- Instant Messaging
- Peer-to-Peer-Software
- Distributed Computing-Projekte
- Suchmaschinen-Symbolleisten
- Mediaplayer
- Internet-Browser
- Spiele (Windows- und Multiplayer-Spiele)
- Virtualisierungsanwendungen
- Remote-Verwaltungstools
- Mapping-Anwendungen
- E-Mail-Clients
- Online-Speicher
- Verschlüsselungstools

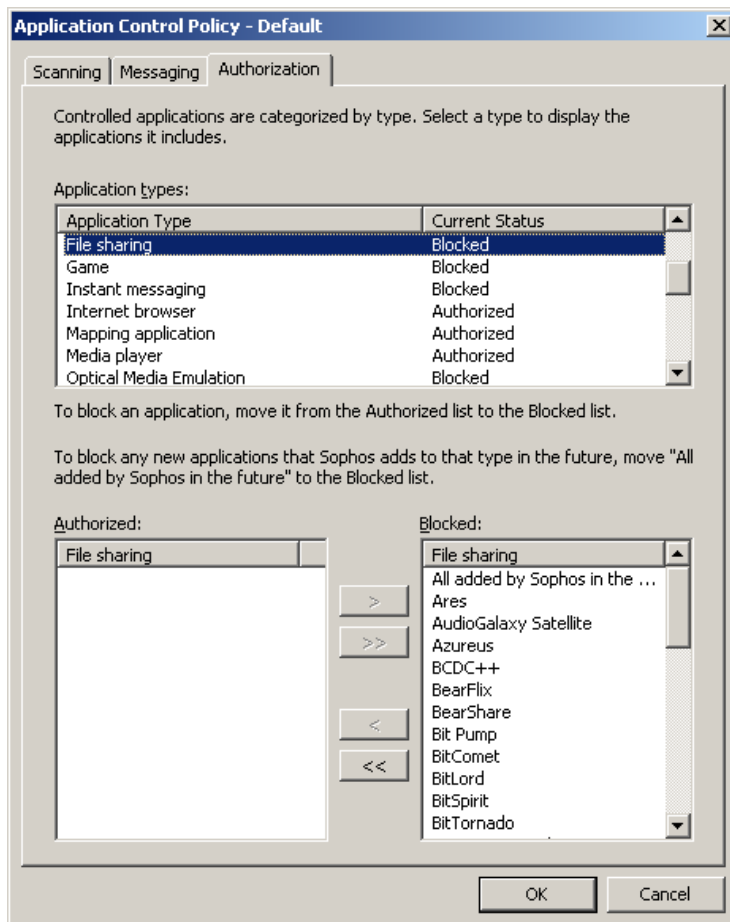


Abbildung 7: Application Control – unkomplizierte Kontrolle unerwünschter Software

### Richtlinien zur Kontrolle von Geräten

Device Control kann die Gefahr für versehentliche Datenverluste erheblich eindämmen und ein unbefugtes Einbinden von Software und Malware von außerhalb des Netzwerks unterbinden.

Integriert in Ihren Sophos Endpoint Agent ermöglicht Device Control die Kontrolle drei unterschiedlicher Gerätetypen:

- Speicherung: Wechselmedien (USB-Sticks, PC-Kartenleser und externe Festplatten), optische Medienlaufwerke (CD-ROM/DVD/Blu-Ray-Laufwerke), Diskettenlaufwerke, sichere Wechselmedien
- Netzwerk: Modems; drahtlos (Wi-Fi-Schnittstellen, 802.11-Standard)
- Short Range: Bluetooth-Schnittstellen; Infrarot (IrDA-Infrarot-Schnittstellen)

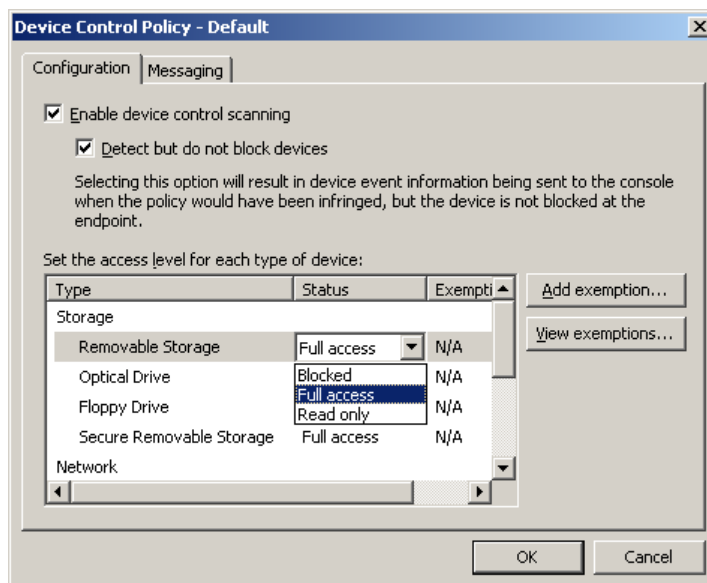


Abbildung 8: Device Control – granulare Kontrolle für Wechselmedien

Standardmäßig ist Device Control deaktiviert, d.h. alle Geräte sind erlaubt. Zur Erst-Deaktivierung von Device Control empfiehlt Sophos folgendes Vorgehen:

- Wählen Sie die zu kontrollierenden Gerätetypen.
- Erkennen Sie Geräte, ohne diese zu blockieren.
- Entscheiden Sie auf Grundlage der Device Control-Ereignisse, welche Gerätetypen gesperrt werden und welche Ausnahmen ggf. gelten sollen.
- Erkennen und sperren Sie Geräte oder gewähren Sie lediglich Lese-Zugriff auf Speichermedien.

Für jeden Gerätetyp können Ausnahmen auf Modell-Basis oder aber auf Einzelgerät-Basis vorgenommen werden. So kann z.B ein USB-Stick, der zur IT-Abteilung gehört, von der Richtlinie zur Blockierung von Wechselmedien ausgenommen werden.

Ausnahmen können einfach über das Device Control-Ereignisfenster der Sophos Enterprise Console vorgenommen werden. So können Ereignisse, die auf Basis der Device Control-Richtlinie generiert wurden, schnell gefiltert und geprüft sowie Geräte durch eine Ausnahme von der Richtlinie zugelassen werden.

Sie können auch das Risiko für die Erstellung von Netzwerkbrücken zwischen Ihrem Unternehmensnetzwerk und anderen Netzwerken erheblich eindämmen. Der Modus zur Blockierung von Netzwerkbrücken ist sowohl für drahtlose als auch für Modem-Geräte verfügbar. Der Modus blockiert Netzwerkbrücken, indem er drahtlose und Modem-Netzwerkadapter deaktiviert, sobald ein Endpoint mit einem physikalischen Netzwerk verbunden wird (meist über eine Ethernet-Verbindung). Sobald der Endpoint vom physikalischen Netzwerk getrennt wird, werden die drahtlosen oder Modem-Netzwerkadapter nahtlos reaktiviert.

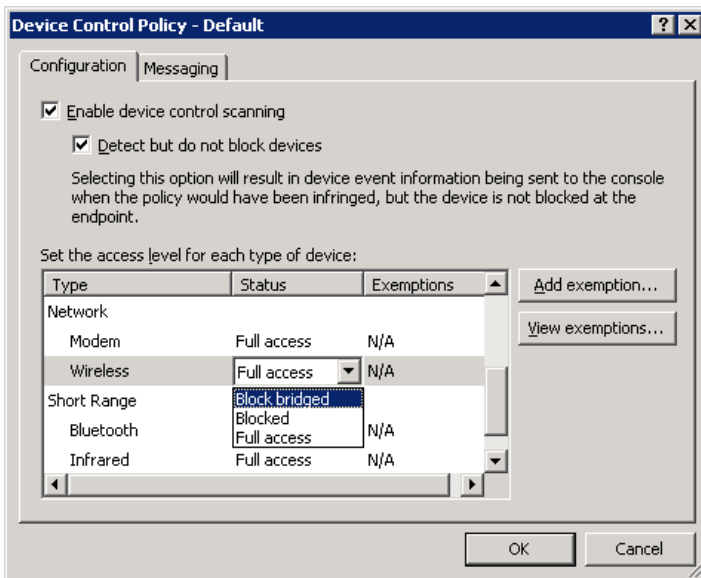


Abbildung 9: Device Control – Netzwerkbrücken verhindern

### Richtlinie zur Datenkontrolle

Die Implementierung einer Standalone-Lösung zur Verhinderung von Datenverlusten (DLP) kann zeitintensiv und kostspielig sein und außerdem signifikanten Einfluss auf die System-Performance Ihrer Endpoint-Computer nehmen. Sophos schafft diese Probleme durch Integration eines Scans auf sensible Daten in den Endpoint Agent aus der Welt und gestaltet so die Konfiguration, den Einsatz und die Verwaltung von DLP-Technologie kinderleicht.

Sie können die Übertragung von Dateien auf ausgewählte Speichermedien (z.B. Wechselmedien oder optische Laufwerke) oder mittels bestimmter Internet-Anwendungen (z.B. E-Mail-Clients, Internet-Browser oder Instant Messaging) kontrollieren und überwachen, ohne eine zusätzliche Lösung oder einen weiteren Endpoint Agent implementieren zu müssen.

Sophos stellt eine Reihe vordefinierter Regeln zur Datenkontrolle bereit, die nationale Identifikationsnummern und Vertraulichkeits-Dokumentenkenzeichnungen abdecken. Es steht Ihnen frei, entweder diese Standardregeln zu verwenden oder aber die Regeln an Ihre individuellen Bedürfnisse anpassen.

Es existieren zwei Arten von Regeln zur Datenkontrolle:

- **Dateiregel:** Legt die Maßnahme fest, welche ergriffen wird, wenn ein User versucht, eine Datei mit einem bestimmten Dateinamen oder von einem bestimmten Dateityp (True File Type-Kategorie, z.B. eine Tabellenkalkulation) an einen im Vorfeld definierten Zielort zu übertragen (z.B. Blockieren des Transfers von Datenbanken auf Wechselmedien).
- **Inhaltsregel:** Enthält eine oder mehrere Datendefinitionen und legt fest, welche Maßnahmen ergriffen werden, wenn ein User versucht, Daten, die allen Regeldefinitionen entsprechen, an einen vorgegebenen Zielort zu übertragen.

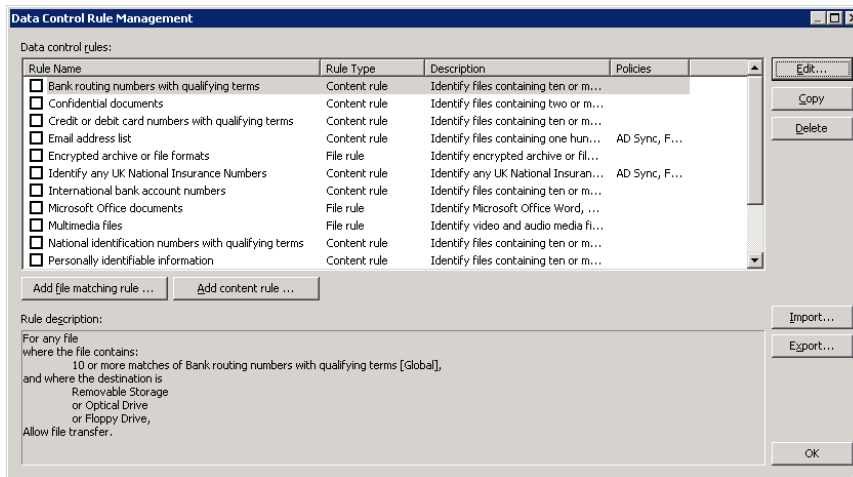


Abbildung 10: Data Control – vorkonfigurierte Regeln für Richtlinien

Um die Richtlinienerstellung zu vereinfachen, pflegen die SophosLabs eine umfassende Library globaler Definitionen sensibler Daten (Content Control Lists), welche u.a. personenbezogene Daten wie Kreditkartendaten, Sozialversicherungsnummern, Anschriften oder E-Mail-Adressen abdeckt.

Um eine fehlerfreie Erkennung zu gewährleisten, bedienen sich diese Definitionen zahlreicher Verfahren. Die Definitionen werden von den SophosLabs regelmäßig aktualisiert und neue Definitionen werden im Rahmen der monatlichen Endpoint-Datenupdates eingespielt.

Auch die Erstellung eigener unternehmensspezifischer Listen ist möglich. Sie haben ferner die Möglichkeit, eigene, speziell auf die Bedürfnisse Ihres Unternehmens abgestimmte Listen zu erstellen, die z.B. Ihre Kundennummern und eigene Vertraulichkeits-Dokumentenkenzeichnungen einschließen können.

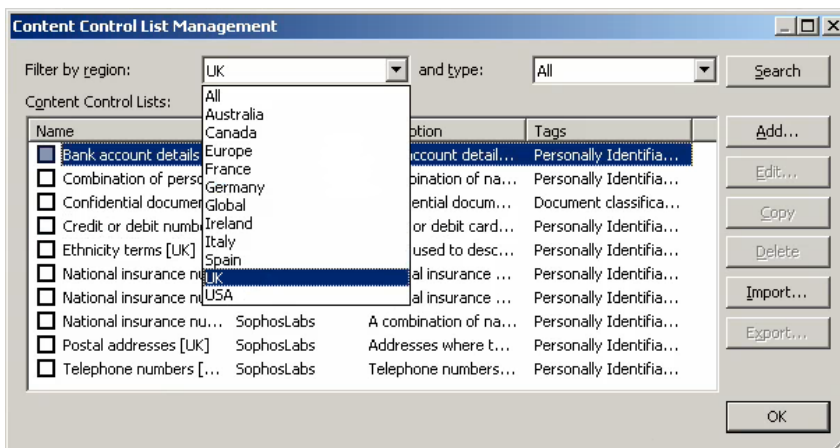


Abbildung 11: Data Control – Listen zur Inhaltskontrolle

Beim Greifen einer Regel zur Datenkontrolle können folgende Maßnahmen getroffen werden:

- Dateiübertragung zulassen und Ereignis protokollieren
- Dateiübertragung nach Zustimmung durch den User zulassen und Ereignis protokollieren
- Übertragung blockieren und Ereignis protokollieren

Im Rahmen der Standardeinstellungen erscheint eine Benachrichtigung auf dem Computerdesktop, sobald eine Regel greift und ein Datentransfer blockiert bzw. ein Zustimmung seitens des Users für den Datentransfer erforderlich ist. Ein Hinzufügen eigener, individuell gestalteter Nachrichten für die User-Zustimmung oder die Blockierung eines Datentransfers ist problemlos möglich.

Die Maßnahme „Übertragung nach User-Zustimmung zulassen“ kann auch dazu verwendet werden, um bei Usern ein Bewusstsein dafür zu schaffen, dass ihre Datenübertragung ggf. gegen geltende Unternehmensrichtlinien verstößt, ohne diese Vorgänge komplett zu unterbinden und im Zweifelsfall Arbeitsschritte des Users gänzlich zu blockieren. Die Entscheidung des Endusers wird einem Audit unterzogen und kann zu einem späteren Zeitpunkt überprüft werden.

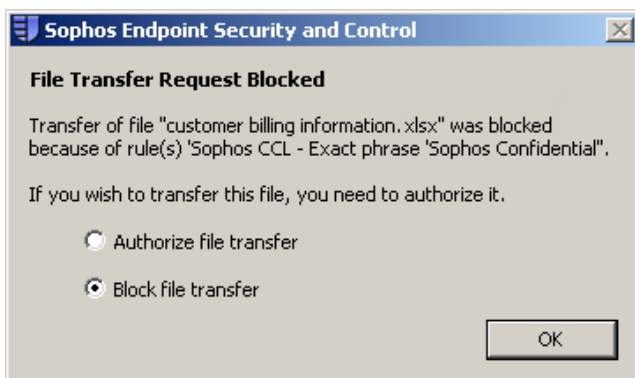


Abbildung 12: Data Control – Autorisierungsmeldung an Enduser

Wenn ein Data Control-Ereignis auftritt, z.B. eine Datei mit sensiblen Daten auf einen USB-Stick kopiert wird, wird dieses Ereignis an die Enterprise Console geschickt und kann im Data Control-Ereignisfenster eingesehen werden. Die Anzahl an Computern mit Data Control-Ereignissen über einem bestimmten Schwellenwert innerhalb der letzten sieben Tage wird ebenfalls auf dem Dashboard angezeigt.

### Firewall-Richtlinien

Standardmäßig ist die Sophos Client Firewall für alle Computer in allen Gruppen aktiviert und blockiert sämtlichen nicht zwingend erforderlichen Datenverkehr. Im Lieferumfang ist ein Satz vordefinierter Sicherheitsrichtlinien enthalten. Sie können diese Richtlinien problemlos an Ihre Anforderungen anpassen. Jeder Aspekt der Firewall-Konfiguration kann zentral verwaltet werden (mehr Informationen zur Sophos Client Firewall in Abschnitt 3).

Um grundlegende Informationen über alle im Netzwerk verwendeten Anwendungen vor dem Rollout einer „echten“ Richtlinie zu erhalten, kann die Firewall netzwerkübergreifend im „Nur melden“-Modus eingesetzt werden. Die so erhobenen Daten werden zurück an die Konsole gemeldet und können in Folge der Erstellung von Richtlinien dienen, die die Produktivität Ihrer User nicht beeinflussen.

Um einen lückenlosen Schutz mobiler Computer innerhalb und außerhalb des Büros zu gewährleisten, ist die Konfiguration unterschiedlicher standortspezifischer Sicherheitsrichtlinien möglich. Der Standort des mobilen Computers wird entweder über DNS oder die Gateway-MAC-Adresse ermittelt.

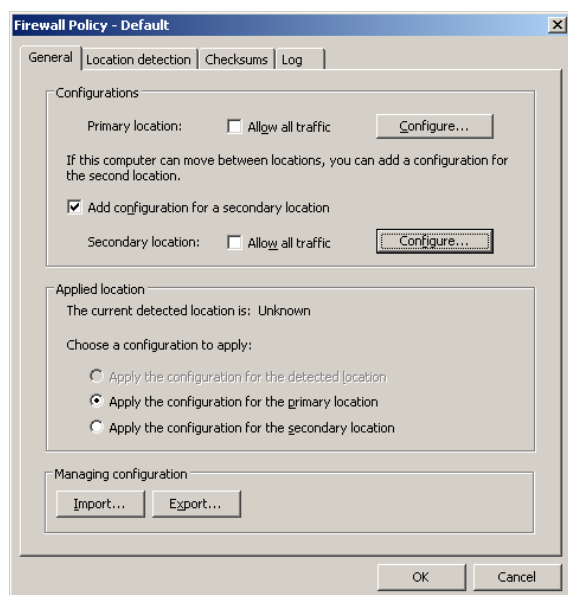


Abbildung 13: Standortspezifische Firewall

### Network Access Control-Richtlinien

Die Kontrolle von NAC-Richtlinien erfolgt mithilfe des NAC Manager, welcher über die NAC-Menüschaftfläche im oberen Bereich der Konsole oder durch Doppelklicken einer NAC-Richtlinie gestartet wird.

Endpoint Security and Data Protection verfügt über vorkonfigurierte Richtlinien für verwaltete und unverwaltete Computer. Der NAC Manager stellt ergänzende Funktionen zur Überarbeitung von Richtlinien, zum Reporting, zur Zugriffskontrolle sowie zur Systemkonfiguration bereit und ist in vier Hauptnavigationsbereiche unterteilt: Verwalten, Durchsetzen, Benachrichtigen und Systemkonfiguration.

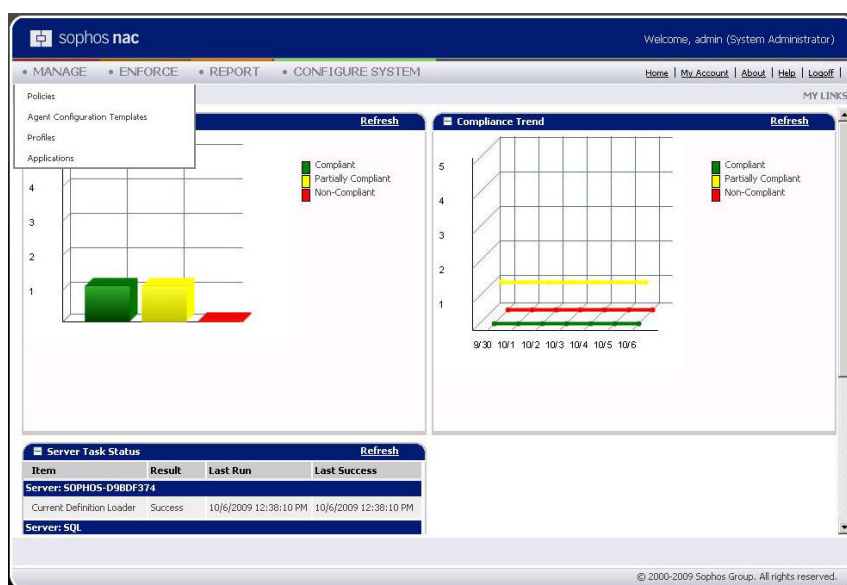


Abbildung 14: Die NAC-Management-Benutzeroberfläche verschafft übersichtlich Einblick in den Compliance-Status des Netzwerks

- Verwalten – hier können Richtlinien überarbeitet und sowohl Richtlinien als auch Computer verwaltet werden.
- Durchsetzen – ermöglicht die Kontrolle des Netzwerkzugriffs durch Einsatz von Access Templates und Ausnahmen.
- Berichten – eine Reihe von Reports, mit denen Compliance- und Netzwerkzugriffsprobleme gelöst werden können.
- Konfigurieren – verschafft Kontrolle über Komponenten, die zur Systemverwaltung, Konfiguration und für Server-Einstellungen benötigt werden.

Nach dem Login erhalten Sie sofort einen Überblick über die Gesamt-Compliance in Ihrem Unternehmen. Das aktuelle Compliance-Diagramm verschafft einen sofortigen Überblick darüber, wie viele Computer mit Ihren Sicherheitsrichtlinien konform, teilweise konform und nicht konform sind. Ein zweites Diagramm zeigt den neuesten Compliance-Trend.

### *Vordefinierte Richtlinien für verwaltete und nicht verwaltete Computer*

Richtlinien geben Ihnen die Möglichkeit, den Zugriff bestimmter Gruppen auf Netzwerkressourcen auf Basis der Sicherheitsüberprüfung jedes einzelnen User-Computers zu kontrollieren. Diese legen außerdem den Compliance-Status des Computers, angezeigte Nachrichten und auszuführende Korrektur- und Enforcement-Maßnahmen fest.

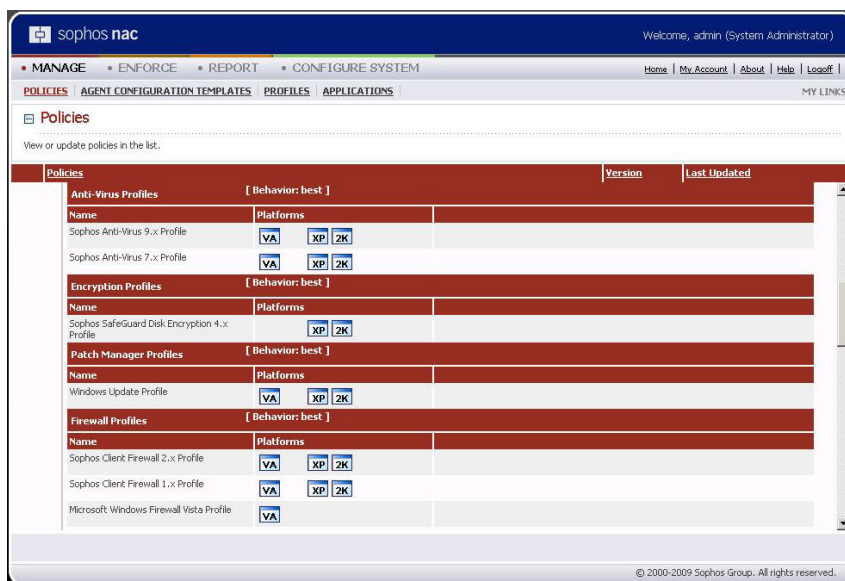


Abbildung 15: Vorkonfigurierte Richtlinien zur Überprüfung des Compliance-Status

Es stehen drei vordefinierte NAC-Richtlinien zur Verfügung:

- **Standard** – Die Standard-Richtlinie dient der schnellen Überprüfung und Kontrolle verwalteter Clients. Sie kommt bei allen neuen Enterprise Console-Gruppen und jedem Client ohne Richtlinienzuordnung bzw. Client, der die ihm zugeordnete Richtlinie nicht finden kann, zum Einsatz. Die Standard-Richtlinie verfügt standardmäßig über Sophos Anti-Virus, Sophos SafeGuard Encryption, Sophos Client Firewall, Microsoft/Windows Update und MS Windows Firewall XP SP2/Vista.
- **Verwaltet** – Die verwaltete Richtlinie ist identisch mit der Standard-Richtlinie. So können Sie an einer dieser Richtlinien Änderungen vornehmen und Sie vor dem Zuordnen zu Ihren Computern testen.
- **Unverwaltet** – Die unverwaltete Richtlinie wird Computern zugeordnet, die nur temporär auf das Netzwerk zugreifen und über den temporären Java-Agent geprüft werden. Sie ist zur Überprüfung einer Reihe von Fremdanbieter-Sicherheitslösungen vordefiniert, zu denen gängige Spywareschutz- und Virenschutz-Produkte sowie Firewall-Anwendungen und Windows oder Microsoft Update zählen. Zu den unterstützten Anbietern gehören u.a. Sophos, Microsoft, Trend Micro, McAfee, Symantec/Norton, F-Secure, Panda, Spybot und Ad-Aware.

## Wichtiger Hinweis

Für einen vollständigen Test der NAC-Funktionen downloaden und installieren Sie bitte die NAC-Manager-Komponente unter [www.sophos.de/downloads/](http://www.sophos.de/downloads/) (mit Ihren Test-Zugangsdaten haben Sie Zugriff auf diesen Bereich).

## MESSAGE RELAYS

### Große Skalierbarkeit

Sophos Endpoint Security and Data Protection ist für hohe Skalierbarkeit konzipiert und ermöglicht Ihnen die Verwaltung zehntausender Computer von einer einzelnen Konsole aus. Noch größere Skalierbarkeit erzielen wir mit Message Relays, durch die Computer im Netzwerk als Relay für die Enterprise Console fungieren. Diese Funktion reduziert den Datenverkehr im Netzwerk, entlastet die Management-Server und ermöglicht in großen Unternehmen die Verwaltung zehntausender Computer.

## REPORTS

### Angepasste und zeitgesteuerte Reports

Bei Bedarf generierbare, integrierte und netzwerkübergreifende Reports sind für die Aufrechterhaltung der Sicherheit unerlässlich. Die Enterprise Console stellt daher eine Reihe von Reports mit grafischen und Textinformationen zu zahlreichen Aspekten Ihres Sicherheitsstatus im Netzwerk bereit. Diese können entweder in Standard-Konfiguration verwendet oder problemlos individuell konfiguriert werden. Zu den Standard-Reports zählen:

- Benachrichtigungen nach Elementname
- Benachrichtigungen nach Standort
- Benachrichtigungen nach Zeit
- Benachrichtigungs-Chronik
- Zusammenfassung aller Benachrichtigungen
- Mangelnde Compliance mit Endpoint-Richtlinien
- Verwalteter Endpoint-Schutz
- Update-Hierarchie
- Ereignisse nach User

Reports können in Tabellen- oder Diagrammformat (auch Tortendiagramm) generiert und in zahlreiche Dateiformate exportiert werden: PDF (Acrobat), HTML, MS Excel, MS Word, RTF, CSV, XML.

Über den Report Manager können Reports auf Basis bestehender Vorlagen erstellt, Konfigurationsänderungen existierender Reports vorgenommen sowie Reports zeitgesteuert abgerufen (einmalig, täglich, wöchentlich, monatlich) und automatisch per E-Mail an ausgewählte Empfänger versendet werden.

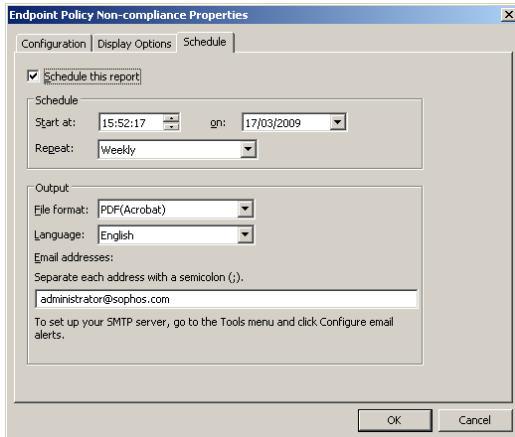


Abbildung 16: Zeitsteuerung von Reports

Über zusätzliche Reports erhalten Sie Zugriff auf Informationen zu sämtlichen Computern. Durch Doppelklicken auf den Computernamen erscheint ein Dialogfeld mit Details wie z.B. IP-Adresse, Benutzername und Datum des letzten Scans.

## ROLLENBASIERTE ADMINISTRATION

### Delegierung von Verwaltungsaufgaben zur Reduzierung der Arbeitsbelastung

Durch die geschickte Kombination aus konfigurierbaren Rollen, Rechten und Untergruppen in Endpoint Security and Data Protection kann die Verwaltung Ihrer gesamten IT-Umgebung äußerst flexibel gestaltet werden.

Funktionen zur rollenbasierten Administration ermöglichen die Konfiguration des Zugriffs auf die Enterprise Console, so dass bestimmte Verwaltungsaufgaben an Abteilungen bzw. Einzelpersonen auf Basis vorkonfigurierter oder individuell erstellter Rollen delegiert werden können. Ein Help Desk Engineer kann z.B. Computer aktualisieren oder bereinigen, jedoch im Gegensatz zu einem Administrator keine Richtlinien konfigurieren.

Zur Konfiguration des Zugriffs müssen Sie lediglich die erforderlichen Rollen einrichten, diese mit ausgewählten Rechten ausstatten und sie in Folge Windows-Usern und -Gruppen zuweisen.

Es existieren vier vordefinierte Rollen:

**Systemadministrator** – eine vordefinierte Rolle mit vollen Rechten zur Verwaltung der Sophos Sicherheitssoftware im Netzwerk und zur Verwaltung von Rollen in der Enterprise Console. Die Rolle des Systemadministrators kann nicht bearbeitet oder gelöscht werden.

**Administrator** – eine vordefinierte Rolle, die die Verwaltung der Sophos Sicherheitssoftware im Netzwerk umfasst, jedoch keine Rollen in der Enterprise Console verwalten kann. Die Rolle des Administrators kann umbenannt, bearbeitet oder gelöscht werden.

**Helpdesk** – eine vordefinierte Rolle, die lediglich Bearbeitungsrechte umfasst (z.B. Bereinigung oder Update von Computern). Die Helpdesk-Rolle kann umbenannt, bearbeitet oder gelöscht werden.

**Gast** – eine vordefinierte Rolle mit reinem Lesezugriff auf die Enterprise Console. Die Gast-Rolle kann umbenannt, bearbeitet oder gelöscht werden.

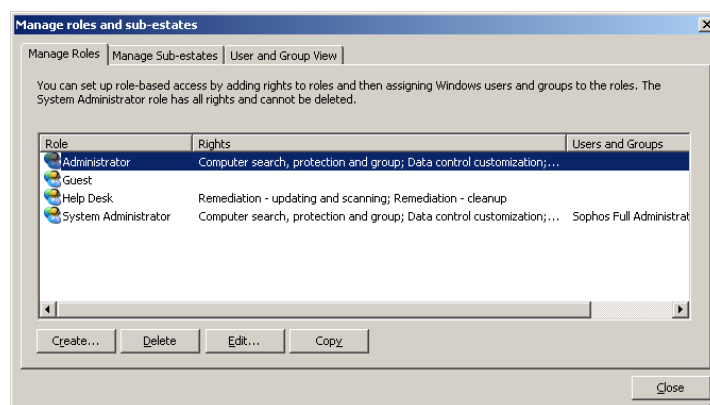


Abbildung 17: Verwaltung der rollenbasierten Administration

### Verwaltung von Untergruppen

Durch die Unterteilung Ihrer IT-Umgebung in Untergruppen können bestimmte Aktionen auf Computern und in Gruppen auf ausgewählte Userkreise beschränkt werden.

Der Zugriff auf Untergruppen kann durch die Zuweisung von Windows-Usern und -Gruppen kontrolliert werden. User haben lediglich Einsicht in für Ihre Untergruppe relevante Computer und Gruppen.

Auch Reports sind Untergruppen-spezifisch. Sämtliche Richtlinien gelten nur für die Untergruppe, in der sie erstellt wurden; ein Administrator kann keine Änderungen an Richtlinien außerhalb seiner Untergruppe vornehmen.

Administratoren können ausschließlich Reports für ihre eigene Untergruppe konfigurieren und generieren. Ein vollwertiger Systemadministrator wiederum kann Reports für die gesamte IT-Umgebung generieren.

### SKALIERBARER DATENSPEICHER

#### Integration in Microsoft SQL Server

Die Enterprise Console lässt sich zum Speichern von Managementinformationen standardmäßig in MSDE (Microsoft SQL Server Desktop Engine) einbinden. In großen Unternehmen empfiehlt sich der Einsatz des Microsoft SQL Server, wodurch sich zusätzliche Funktionen eröffnen und eine höhere Skalierbarkeit in großen Netzwerken möglich ist.

## 3 SCHUTZ FÜR WINDOWS-SYSTEME

Sophos Endpoint Security and Data Protection schützt Ihr Windows-Netzwerk mit Sophos Endpoint Security and Control für Windows, Sophos NAC, SafeGuard Disk Encryption und der Sophos Client Firewall.

### SOPHOS ENDPOINT SECURITY AND CONTROL FÜR WINDOWS

Sophos ist für Unternehmensnetzwerke konzipiert und bietet neben Schutz vor Malware auch ein Host Intrusion Prevention System (HIPS) sowie die Überwachung von Wechselmedien, unerwünschten Anwendungen und der Übertragung sensibler Daten.

Ein einziger Endpoint Agent macht Einzelprodukte überflüssig, da er folgende Features beinhaltet:

- Virenschutz und HIPS (sperrt Viren, Spyware, Adware, PUAs, verdächtige Dateien und verdächtiges Verhalten)
- Application Control (verhindert die Installation und Nutzung unerlaubter Anwendungen)
- Device Control (verwaltet die Verwendung von Wechselmedien und drahtlosen Netzwerkprotokollen)
- Data Control (scannt auf Übertragungen sensibler Daten von Endpoints)
- Client Firewall (schützt vor Hacker-Angriffen und nicht autorisierter Anwendungskommunikation)

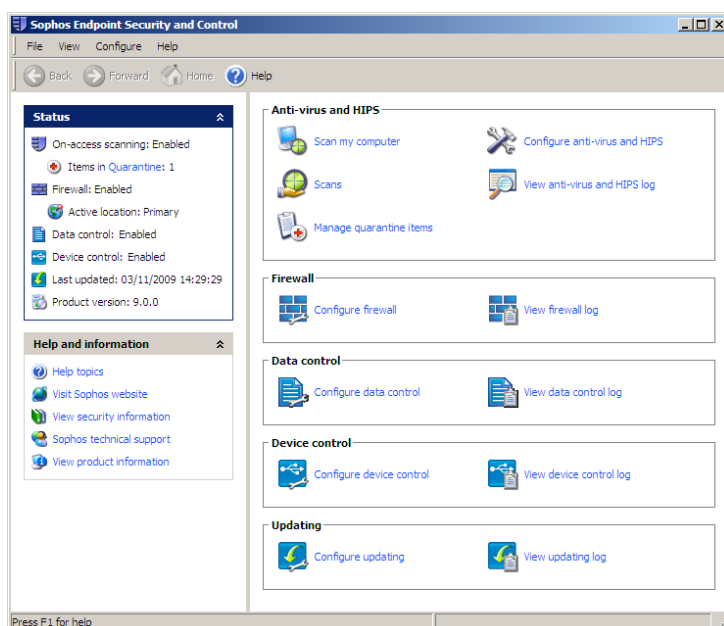


Abbildung 18: Durch Einsatz nur eines Endpoint Agent geringerer Einfluss auf die System-Performance

## Unbefugte Zugriffe

Sophos Endpoint Security and Control für Windows umfasst ein vollständiges Host Intrusion Prevention System (HIPS) für proaktiven Schutz ohne die komplizierte Installation oder Konfiguration eines weiteren Produkts. Durch den Einsatz proaktiver Erkennungsalgorithmen ist Ihr Netzwerk vor zielgerichteten gemischten Zero-Day-Bedrohungen geschützt:

- **Genotype®-Verfahren** bietet Zero-Day-Schutz, indem es Virenfamilien und -varianten bereits erkennt und blockiert, bevor eine spezifische Erkennung überhaupt verfügbar ist.
- **Behavioral Genotype® Protection** schützt automatisch vor neuen gezielten Bedrohungen, indem das Verhalten vor dem Ausführen von Code analysiert wird.
- **Das integrierte HIPS-Verfahren** erkennt verdächtige Dateien vor deren Ausführung, analysiert verdächtiges Verhalten und Laufzeitfehler sowie schützt vor Pufferüberläufen, damit Malware, verdächtige Dateien und verdächtiges Verhalten rechtzeitig aufgedeckt werden können.

## Schnelleres Scanning mit Decision Caching

Decision Caching™ – der leistungsstarke On-Access-Scan von Sophos Endpoint Security and Control für Windows – optimiert die Performance durch gezieltes Scannen nur neuer oder geänderter Dateien. Intelligent File Recognition scannt ausschließlich Dateien, die Malware enthalten könnten. Remote-User können bedarfsgesteuerte Scans einzelner Dateien oder Computer durchführen lassen, bevor sie die Verbindung zum Hauptnetzwerk herstellen. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen.

## Quarantäne-Manager

Der Quarantäne-Manager regelt das Verschieben oder Löschen infizierter Dateien sowie das individuelle Sperren von PUAs und Controlled Applications.

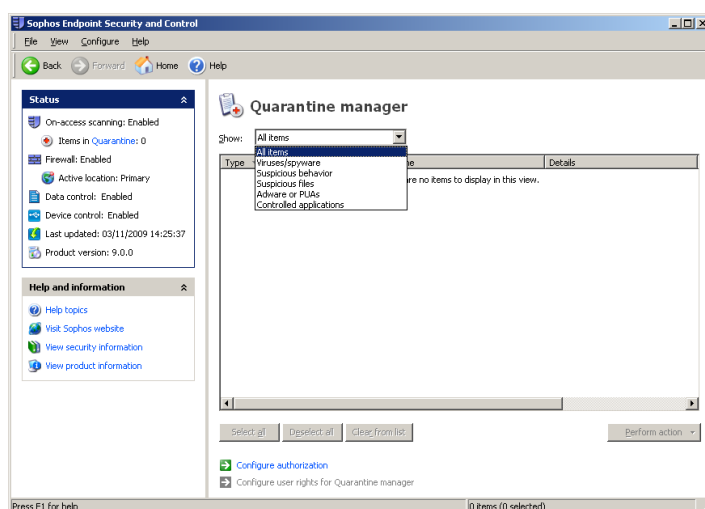


Abbildung 19 : Quarantäne-Manager

## Application Control

Einige Anwendungen können die Effektivität verbessern, andere lenken Mitarbeiter von der Arbeit ab, vergeuden kostbare Netzwerkressourcen und bremsen die Systemgeschwindigkeit. Angriffe durch P2P- und IM-basierte Malware nehmen rapide zu. Gleichzeitig machen gesetzliche Vorschriften die Verwaltung und den Schutz von Daten unerlässlich und die Kontrolle nicht autorisierter Anwendungen gewinnt an Bedeutung.

Durch die Integration von Application Control in den Endpoint Agent ermöglicht Sophos eine selektive Anwendungszulassung bzw. -sperrung – zentral oder auf Desktop-Ebene. Dank Aktivierung von ActivePolicies in der Sophos Enterprise Console können Anwendungen für verschiedene Computergruppen gesperrt oder zugelassen werden (siehe Abschnitt 2). So können Sie VoIP z.B. für Computer im Unternehmen deaktivieren und für Remote-Computer zulassen.

## Device Control

Mit unserem Device Control-Feature dämmen Sie Risiken für Datenverluste und Malwareinfektionen ein, indem Sie Wechselmedien und drahtlose Netzwerkprotokolle lückenlos kontrollieren.

Integriert in den zentralen Endpoint Agent dient das Feature als Port-Agnostiker und unterstützt sämtliche Ports, an die Geräte angeschlossen werden (u.a. USB-, FireWire-, SATA- und PCMCIA-Schnittstellen).

Die Device Control-Richtlinie kann zunächst im „Nur Benachrichtigen“-Modus eingesetzt werden. So erhalten Sie ohne Geräteblockierung einen Überblick über in Ihrer IT-Umgebung verwendete Geräte und können in Folge Kontrollrichtlinien für ausgewählte Gruppen konfigurieren und einsetzen.

Jeder Gerätetyp kann wahlweise zugelassen (Standard-Einstellung) oder gesperrt werden. Speichermedien kann auch der Modus „Nur lesen“ zugeordnet werden. In diesem Fall können Daten zwar vom Medium gelesen, aber nicht auf dieses geschrieben werden. Diese Option erweist sich vor allem für USB-Sticks und CD-/DVD-Laufwerke als nützlich.

Bei Netzwerkbrücken unterbindet der „Brücken blockieren“-Modus Netzwerkbrücken und deaktiviert drahtlose Computerschnittstellen, sobald ein Computer sich physikalisch mit dem Netzwerk verbindet (z.B. über ein Ethernet-Kabel). Bei Entfernen des Kabels wird die drahtlose Schnittstelle wieder aktiviert.

## Data Control

Sophos integriert als erster Anbieter einen DLP-Scan in den Endpoint Agent und reduziert so die Systembelastung und den Arbeitsaufwand erheblich, da nur ein Agent auf sensible Daten und Malware scannt sowie konfiguriert, implementiert und verwaltet werden muss.

Der DLP-Scan ermöglicht Ihnen die Überwachung von Übertragungen sensibler Daten (z.B. personenbezogene Daten oder vertrauliche Unternehmensinterna) auf Wechselmedien oder in Internetanwendungen und beugt so versehentlichen Datenverlusten vor.

Durch vordefinierte Regeln zur Datenkontrolle wird die Erstellung von Richtlinien erheblich vereinfacht, da Standardrichtlinien ohne jede Zeitverzögerung direkt nach Implementierung der Software zum Einsatz gebracht werden können. Auch die Anpassung der Richtlinien auf individuelle Bedürfnisse ist problemlos möglich.

Die SophosLabs pflegen zudem eine umfassende Library globaler Definitionen sensibler Daten (Content Control Lists), welche u.a. personenbezogene Daten wie Kreditkartendaten, Sozialversicherungsnummern, Anschriften oder E-Mail-Adressen abdeckt und so einen noch schnelleren Schutz Ihrer sensiblen Daten ermöglicht.

Sie haben ferner die Möglichkeit, eigene, speziell auf die Bedürfnisse Ihres Unternehmens abgestimmte Listen zu erstellen, die z.B. Ihre Kundennummern und eigene Vertraulichkeits-Dokumentenkenzeichnungen einschließen können.

## SOPHOS NAC

### Überprüfung und Kontrolle aller Windows-Endpoints

Bei Computern, die versuchen, auf das Netzwerk zuzugreifen, wird mit Sophos NAC auf Basis der vordefinierten Sicherheitsrichtlinien eine Compliance-Überprüfung durchgeführt. Diese Funktion zur Gewährleistung der Endpoint-Compliance stellt durch folgende Maßnahmen sicher, dass sämtliche Computer ausreichend geschützt sind:

- Überprüfen von Virenschutz und anderen Sicherheitsanwendungen auf korrekte Konfiguration und Aktualität
- Überprüfen der Microsoft Windows Service Packs auf Aktualität
- Prüfen der Aktivierung von Microsoft Windows und/oder Microsoft Update
- Einsetzen gesonderter Richtlinien, die für verwaltete, Gastcomputer und Computer von Geschäftspartnern konfiguriert werden können

### Enforcement-Optionen zur Kontrolle des Netzwerkzugriffs

Sophos NAC setzt zur Kontrolle verwalteter Computer ein agent-basiertes Enforcement ein und kooperiert mit Microsoft DHCP, um Netzwerkzugriff durch unverwaltete/nicht autorisierte Computer zu unterbinden. Die Endpoint-Überprüfung übernehmen:

- der Sophos NAC Compliance Quarantine Agent (befindet sich auf dem Client) und
- der temporäre Sophos NAC Compliance Agent (downloadbare Java-Komponente)

Der Sophos NAC Compliance Quarantine Agent, welcher über die Sophos Enterprise Console eingesetzt wird, überprüft und kontrolliert verwaltete Computer sowohl vor und während des Netzwerkzugriffs und in von Ihnen festgelegten Intervallen. Dieser Agent schützt das Netzwerk durch Selbst-Quarantäne für nicht richtlinienkonforme Computer.

Der temporäre Sophos NAC Compliance Agent führt die gleiche Prüfung vor dem Netzwerkzugriff unverwalteter LAN-Computer durch. Dieser wurde speziell für User entwickelt, die selbst keinen Agent auf dem Endpoint installiert haben bzw. keinen Agent installieren können, aber dennoch auf ausgewählte Netzwerkressourcen zugreifen müssen (z.B. Gäste oder Subunternehmer). Unter Verwendung der bestehenden Microsoft DHCP-Infrastruktur eines Unternehmens setzt Sophos NAC Microsoft DHCP zum Schutz des Netzwerks vor LAN-gebundenen Computern ein und lässt das über Sophos NAC erfolgende Verschieben von nicht richtlinienkonformen und nicht autorisierten Computern in die Quarantäne zu.

## SOPHOS CLIENT FIREWALL

Die Sophos Client Firewall ist in den Endpoint Agent integriert. So werden Einsatz, Konfiguration, Update und Verwaltung über die Enterprise Console vereinfacht. Die Firewall sperrt Computer proaktiv und schützt so vor bekannten und unbekanntem Bedrohungen wie Internet-Würmern, Hacker-Angriffen und ungenehmigter Anwendungskommunikation. Durch den Einsatz von Funktionen zur Verhinderung des Missbrauchs von Anwendungen und des Identitätswechsels bietet Sophos Client Firewall besseren Schutz als das simple Sperren von Ports, wie es bei Firewalls anderer Sicherheitsanbieter üblich ist.

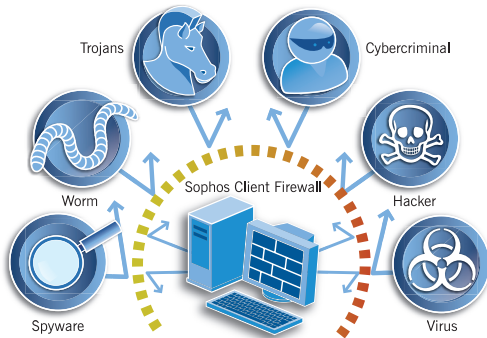


Abbildung 20: Zero-Day-Schutz

### Proaktiver Zero-Day-Schutz vor bekannten und unbekanntem Bedrohungen

Die Sophos Client Firewall schützt z.B. anfällige Computer vor neuen Bedrohungen in der Gefahrenzeit zwischen dem Auftreten einer neuen Bedrohung und der Entwicklung eines Schutzes. Sie sichert die Computer eines Unternehmens gegen komplexe Bedrohungen, die sich schnell verbreiten, und erstickt Malware-Infektionen gewissermaßen im Keim, also noch bevor sie den geregelten Arbeitsablauf stören.

### Proaktive Sicherheit

Die Sophos Client Firewall bietet Schutz vor Netzwerk- und Internet-Würmern sowie vor Hackern und verhindert durch gezielte Beschränkung der Zugriffsrechte, dass ungeschützte Computer eine Verbindung zum Netzwerk herstellen – im Büro ebenso wie auf Laptops, die eine Verbindung über drahtlose Hotspots und DSL-Verbindungen im Hotel herstellen.

### Überwachen und Sperren von Ports zur Abwehr von Bedrohungen

Die Sophos Client Firewall wehrt bekannte und unbekanntem Bedrohungen ab, indem sie aktive Ports überwacht und inaktive Ports sperrt. Dadurch werden Internet-Würmer und Hacker-Angriffe wirksam gestoppt.

### Stealth-Technologie verhindert unbefugte Zugriffe

Cyberkriminelle wie z.B. Hacker machen sich Port-Scanning zunutze, um Computer mit offenen Ports ausfindig zu machen und anzugreifen. Zu diesem Zweck senden sie Verbindungsanfragen über das Internet. Die Stealth-Technologie von Sophos unterbindet Antworten auf diese Anfragen und schirmt Computer so ab, dass sie von außerhalb inaktiv erscheinen. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen. Der Datenschutz wird dadurch gewährleistet, dass Hackern die Möglichkeit genommen wird, anfällige Computer ausfindig zu machen und anzugreifen.

## Erhöhter Schutz durch Standorterkennung

Die Sophos Client Firewall ermöglicht Ihnen die Konfiguration unterschiedlicher Richtlinien für verschiedene Standorte abhängig davon, wo Computer zum Einsatz kommen (z.B. im Büro und im Netzwerk oder außerhalb des Büros). Die Enterprise Console weist Computern daraufhin abhängig von ihrem Standort (im Netzwerk oder außerhalb) unterschiedliche Firewall-Einstellungen zu. Diese duale Standort-Konfiguration ist besonders beim Einsatz von mobilen Computern wie Laptops nützlich.

## Verhindern von Anwendungsmissbrauch und -maskierung

Durch Filter auf Anwendungsebene wird das Verhalten von Anwendungen überwacht. Nur Anwendungen, die Ihren Spezifikationen entsprechen, erhalten Zugang zum Internet oder Netzwerk. Die Sophos Client Firewall verhindert auch den Missbrauch von Anwendungen durch Hacker, indem unangemessene Aufrufe von Anwendungen oder Systemen sowie das Starten versteckter Prozesse überwacht werden. Durch die Prüfsummen-Methode wird verhindert, dass Spyware und andere Malware sich als legitime Anwendungen tarnen können. Dadurch wird der Diebstahl vertraulicher Daten über das Internet unterbunden.

## Stateful Inspection überwacht ein- und ausgehende Datenpakete

Die Sophos Client Firewall nutzt Stateful Inspection, um die Sicherheit zu erhöhen, indem Pakete verfolgt und nur legitime Pakete erlaubt werden. Um eine eingeschränkte Antwort-Kommunikation zu ermöglichen, werden Pakete nachverfolgt. Wenn z.B. ein ausgehendes Paket versendet wird, dürfen nur solche eingehenden Pakete die Firewall passieren, welche von dem Computer stammen, mit dem kommuniziert wurde (von dem entsprechenden Port).

## Zentrales Reporting, zentrale Protokollierung

Die Firewall stellt der Management-Konsole einen zentralen Report bereit. In diesem sind unbekannte Anwendungen, unbekannter Traffic, versteckte Prozesse und veränderte Speicherereignisse aufgeführt. So können Sie Risikobereiche schnell und einfach identifizieren. In der Protokollansicht der Firewall können Sie Daten zu jeder Verbindung, die von der Firewall zugelassen oder gesperrt wurde, einsehen, filtern und speichern.

## „Nur Überwachen“-Modus

Die Firewall kann in Ihrer gesamten IT-Umgebung auf Wunsch in einem „Nur Melden“-Modus betrieben werden. In diesem Fall deckt die Firewall alle Anwendungen auf, die im Netzwerk verwendet werden (unter Berücksichtigung sämtlicher LAN-Einstellungen). Die Ergebnisse werden zurück an die Enterprise Console gemeldet. So haben Sie die Möglichkeit, Informationen über unbekanntes Traffic zu sammeln und Firewall-Richtlinien auf Grundlage dieser ohne Einfluss auf die User-Produktivität zu verfeinern.

## Interaktives Arbeiten

Die Firewall kann im Lern-Modus (interactive) betrieben werden. In diesem Modus entscheidet der User, wie mit erkanntem Traffic verfahren werden soll. Bei Aktivierung dieses Modus blendet die Firewall auf dem Endpoint-Computer jedes Mal ein Pop-up-Fenster ein, sobald eine unbekanntes Anwendung oder Serviceleistung auf das Netzwerk zugreifen möchte. Der Lerndialog fragt den User, ob der Traffic erlaubt oder blockiert werden bzw. eine Regel für diese Art von Traffic erstellt werden soll.

SOPHOS ANTI-VIRUS FÜR MAC OS X, LINUX UND UNIX

## 4 SCHUTZ FÜR NICHT-WINDOWS-SYSTEME

### AUCH NICHT-WINDOWS-SYSTEME MÜSSEN GESCHÜTZT WERDEN

Der Schutz von Mac-, Linux-, UNIX- und anderen Systemen ist inzwischen unerlässlich. Selbst Nicht-Windows-Systeme können Windows-spezifische Viren bergen und verbreiten. Mac- und Linux-Viren sind nicht auszuschließen und gesetzliche Bestimmungen sehen den Schutz jedes Computers vor. All das bedeutet Mehrarbeit für Sie.

Sophos Anti-Virus für Mac OS X, Sophos Anti-Virus für Linux und Sophos Anti-Virus für UNIX sind leistungsstarke Lösungen mit intuitiven Bedienfunktionen, die speziell zum Schutz von Servern, Desktops und Laptops in Unternehmen entwickelt wurden.

### SOPHOS ANTI-VIRUS FÜR MAC OS X

Sophos Anti-Virus für Mac OS X erkennt Viren, Spyware, Trojaner und Würmer in Echtzeit und bei Bedarf sowie desinfiziert den Computer automatisch von Windows- und Mac-Malware. Sophos Anti-Virus für Mac OS X erfasst Viren selbst in komprimierten Attachments einschließlich rekursiver Archive.

#### Verwaltungskontrolle über Mac- oder Windows-Plattform

Sophos Anti-Virus für Mac kann entweder über den Sophos Update Manager für Mac oder die Sophos Enterprise Console (Windows) verwaltet werden. Um eine ordnungsgemäße Aktualisierung von Sophos Anti-Virus für Mac OS X sicherzustellen, genügt die Verwendung einer dieser Administrator-Oberflächen.

#### Zentrale Verwaltung

Über die Enterprise Console können Sie den Malware-Schutz für Windows-, Mac-, Linux- und UNIX-Systeme von einer zentralen Stelle im gesamten Netzwerk aus konfigurieren und verwalten. Für den Betrieb der Enterprise Console ist kein Windows-Computer erforderlich. Über die Konsole sind zahlreiche Verwaltungsfunktionen verfügbar.

Wenn Sie ein reines Mac-Netzwerk betreiben, können Updates und Konfiguration über den Sophos Update Manager für Mac von einem einzigen Mac-Computer abgewickelt werden. So können Sie automatische Updates aktivieren und bestimmen, wie Sie E-Mail-Benachrichtigungen erhalten möchten. Sie nehmen auch die Einstellungen für die Implementierung des Scanvorgangs von Desktops und Laptops vor und aktivieren die zentrale Konfiguration der Desktop-Einstellungen.

#### Automatische Updates aus den SophosLabs

Zur Verwaltung von Software- und Schutzupdates können Sie entweder die Sophos Enterprise Console oder aber den Sophos Update Manager für Mac OS X verwenden.

Sie können Adresse, Benutzernamen und Kennwort bereitstellen, damit Computer automatisch Updates mit den neuesten Virenkennungsdateien (IDEs) der SophosLabs durchführen können. Eigenständige Updates können auch über das zentrale Installationsverzeichnis (CID) erfolgen, das im Rahmen des Installationsvorgangs im Netzwerk eingerichtet wurde.

Externen und mobilen Usern können Sie die Möglichkeit zu Updates über das Netzwerk oder Internet vom Hauptserver, einem Backup oder direkt von Sophos einräumen.

### Automatische Reports über Virenvorfälle

Das Dashboard der Enterprise Console enthält Daten zum Infektionsrisiko. Im Fall einer Infektion werden automatische E-Mail-Benachrichtigungen verschickt, damit Sie umgehend Gegenmaßnahmen ergreifen können.

Mit dem Sophos Update Manager für Mac können Sie außerdem Benachrichtigungsoptionen wählen, die bei unmittelbaren Scans und On-Access-Scans greifen. Selbstverständlich können Sie den Empfänger der Nachricht auswählen. Benachrichtigungen bleiben gespeichert, wenn der Absender keine Verbindung hergestellt hat, und werden weitergeleitet, sobald der Absender die Netzwerkverbindung herstellt, damit keine Nachrichten verloren gehen.

### Minimale Scankosten

Sophos Anti-Virus erkennt bei On-Access- und On-Demand-Scans nicht infizierbare Dateitypen und verringert so die Systembelastung.

Sie können im Sophos Update Manager eine Reihe von Einstellungen vornehmen. So lassen sich beispielsweise bestimmte Dateien vom Scan ausschließen und Sie können auch festlegen, was im Fall einer erfassten Bedrohung (Desinfizieren oder Löschen) geschehen soll.

## SOPHOS ANTI-VIRUS FÜR LINUX

Sophos Anti-Virus für Linux bietet höchst zuverlässige, leistungsfähige On-Access-Scans für Linux-Desktops, -Laptops und -Server und unterstützt von vornherein eine große Auswahl von Linux-Distributionen.

### Zentrale Verwaltung

Linux-Systeme können über die Enterprise Console verwaltet werden. Das Dashboard zeigt das Infektionsrisiko an. Automatische E-Mail-Benachrichtigungen werden gesendet, wenn die von Ihnen festgelegten Schwellenwerte erreicht werden. Jeder Virenvorfall wird automatisch gemeldet. Das erleichtert die alltägliche Verwaltung.

### Schnelle Installation in reinen Linux-Netzwerken

Die Installation in reinen Linux-Umgebungen kann über den Red Hat Package Manager abgewickelt werden. Konfiguration und Updates können entweder extern über eine webbasierte Benutzeroberfläche oder über die Befehlszeile vorgenommen werden.

### Leistungsstark, stabil und zuverlässig

Für zusätzlichen Schutz sorgt Talpa, ein einzigartiges Modul aus dem Hause Sophos zum Abfangen von Dateien, das den Scan lokaler Festplatten, Medienlaufwerke, freigegebener Dateisysteme (wie NFS und Samba) und verteilter Dateisysteme je nach Zugriff, Bedarf oder Zeitplan ermöglicht. Zahlreiche Linux-Kernel werden unterstützt, darunter auch die neueren 64-Bit-Versionen. So können Sie, um optimalen Schutz zu erzielen, Versionen bei Bedarf ändern, aktualisieren und kompilieren.

## Automatische Updates

Schutz-Updates werden von der Enterprise Console, kaskadierenden Webservern oder direkt von Sophos automatisch heruntergeladen und verteilt. Somit sind alle Computer im Netzwerk, auch Remote-Laptops, stets umfassend geschützt.

## SOPHOS ANTI-VIRUS FÜR UNIX

Sophos Anti-Virus für UNIX bietet integrierte und plattformübergreifende Viren- und Spyware-Erkennung für Server, Desktops und Laptops mit UNIX-Betriebssystem. Die leistungsstarke Detection Engine scannt alle potenziellen Eintrittspunkte und bietet so lückenlosen Netzwerk-Schutz.

## Einfache Verwaltungsoptionen

Sophos Anti-Virus für UNIX kann für maximale Flexibilität sowohl über die Befehlszeile, als auch über die Enterprise Console (für Solaris 9 und 10 auf SPARC und Intel [i386] und HP-UX auf Itanium 2) verwaltet werden.

## Leistungsstarkes Scanning

Scanning und Desinfektion können zeit- und zugriffsgesteuert mit minimalen Auswirkungen auf die System-Performance erfolgen. Decision Caching™ sorgt dafür, dass nur Dateien gescannt werden, die geändert wurden, und bietet so einen schnelleren Scan praktisch ohne Einbußen bei der Systemgeschwindigkeit.

## Erkennung von Zero-Day-Bedrohungen noch vor Ausführung

Behavioral Genotype® Protection bietet die Vorteile eines Host Intrusion Prevention Systems (HIPS), indem es Programmcode noch vor der Ausführung analysiert und so automatisch vor unbekanntem Bedrohungen schützt.

## Automatisiertes und angepasstes Reporting

Jeder Virenvorfall wird automatisch an den Administrator gemeldet, wodurch tägliche Verwaltungsaufgaben vereinfacht werden.

## ANHANG I

## ENDPOINT SECURITY AND DATA PROTECTION TESTEN

Wir möchten Ihnen demonstrieren, dass Sophos Endpoint Security and Data Protection besseren Schutz für Ihr Netzwerk und besseren Support für Sie bietet als die Sicherheitslösungen anderer Anbieter. In diesem Anhang finden Sie Einzelheiten der zum Test unserer Software erforderlichen Dokumentation, Empfehlungen für die Testumgebung und eine umfassende Checkliste zu allen Aspekten unserer Software und unseres Supports.

### Startup-Anleitung und Benutzerhandbücher

Laden Sie bitte vor dem Test von Sophos Endpoint Security and Data Protection die Startup-Anleitung herunter. Die Adresse lautet:

[http://www.sophos.de/support/docs/Endpoint\\_Security\\_Control-all.html](http://www.sophos.de/support/docs/Endpoint_Security_Control-all.html)

### TESTUMGEBUNG

Sophos Anti-Virus unterstützt eine Vielzahl von Plattformen, darunter UNIX, Linux und NetWare. Ein Test der zentralen Managementfunktionen der Enterprise Console erfordert jedoch mindestens einen Windows-Computer. Ihre Testumgebung sollte möglichst Folgendes enthalten:

- Eine Management-Konsole, also einen Computer mit Windows 2000/XP/2003.
- Mindestens einen Client – wir empfehlen einen Windows 2000/XP/2003/Vista/7 Desktop-PC.

Außerdem benötigen Sie Zugang zum Internet. Ihre Testumgebung sollte möglichst auch Mac OS X-Computer, Linux- und UNIX-Plattformen sowie einen nicht vernetzten Computer zum Testen der Remote-Updates enthalten.

### Wichtiger Hinweis

Deinstallieren Sie bitte zunächst jegliche Virenschutzsoftware in Ihrem Testnetzwerk. Falls dabei Probleme auftreten, wenden Sie sich bitte an den technischen Support von Sophos (siehe [www.sophos.de/support/queries](http://www.sophos.de/support/queries)).

## SYSTEMANFORDERUNGEN

Genauere Informationen auch unter  
[www.sophos.de/products/all-sysreqs.html](http://www.sophos.de/products/all-sysreqs.html)

### Systemanforderungen für die Sophos Enterprise Console

<b>Unterstützte Plattformen</b>	Windows 95/98/NT4/2000/XP/2003/ Vista/2008/7 Mac OS X Linux UNIX
<b>Hardware</b>	Mind. 2.0 GHz Pentium oder kompatibler
<b>Management-Server</b>	Windows Server 2008 Windows Server 2003 und R2 Windows 2000 Server VMWare ESX VMWare Workstation VMWare Server
<b>Sophos NAC Management-Server</b>	Windows Server 2008 32 Bit Windows Server 2003 und R2 32 Bit
<b>Remote-Konsole</b>	Windows Server 2008 Windows Server 2003 und R2 Vista Windows XP Professional Windows 2000 Professional oder Server VMWare ESX VMWare Workstation VMWare Server
<b>Festplattenspeicher</b>	Mind. 150 MB MSDE 2 GB SQL 2005 ohne Begrenzung SQL 2008 ohne Begrenzung SQL 2005 Express Edition 4 GB SQL 2008 Express Edition 4 GB SQL Server 2000 2 GB
<b>Arbeitsspeicher</b>	Mind. 512 MB Mind. 1 GB für Sophos NAC Manager

### Systemanforderungen Sophos NAC Compliance Agent

<b>Unterstützte Plattformen</b>	Windows 2000/XP/Vista
<b>Festplattenspeicher</b>	Mind. 20 MB
<b>Arbeitsspeicher</b>	Mind. 512 MB RAM

### Systemanforderungen Sophos SafeGuard Disk Encryption

<b>Unterstützte Plattformen</b>	Windows 7/Vista/XP
<b>Festplattenspeicher</b>	Mind. 300MB
<b>Arbeitsspeicher</b>	Windows 7/Vista – 1 GB empfohlen Windows XP – 512 MB empfohlen

### Systemanforderungen Sophos Endpoint Security and Control für Windows

Unterstützte Plattformen	
Windows 95/98/NT4/2000 und 2000 Pro/XP Home und Pro/2003/Vista/2008/7	
Windows Netbooks	
Windows XPe	
Windows Embedded Standard	
WePOS	
VMWare ESX	
VMWare Workstation	
VMWare Server	
Festplattenspeicher	
Windows 2000/XP/2003/Vista/2008/7	Mind. 120 MB
Windows Me/98/95/NT4	Mind. 90 MB
Arbeitsspeicher	
Windows 2000/XP/2003/Vista/2008/7	Mind. 256 MB
Windows Me/98/95	Mind. 64 MB
Windows NT4	Mind. 256 MB

### Systemanforderungen Sophos Client Firewall

<b>Unterstützte Plattformen</b>	Windows 2000 Pro/XP Home und Pro/Vista/7
<b>Festplattenspeicher</b>	Mind. 100 MB freier Speicher
<b>Arbeitsspeicher</b>	Mind. 320 MB RAM
<b>Prozessor</b>	Pentium-Klasse mit mind. 300 MHz

### Testumgebung für Sophos Anti-Virus für Mac OS X

Sie müssen ein Testnetzwerk aus Computern mit Mac OS X einrichten. Ein Computer muss als Server eingerichtet werden und das zentrale Installationsverzeichnis (CID) – den Installationsordner für Sophos Anti-Virus – enthalten, von dem aus die Installation im restlichen Netzwerk erfolgt. Im CID ist auch der Sophos Update Manager abgelegt, welcher Mac OS X-Computern im Netzwerk die aktuellen Virenkennungsdateien (IDEs) und Konfigurationseinstellungen bereitstellt.

### Systemanforderungen Sophos Anti-Virus für Mac OS X

<b>Unterstützte Plattformen</b>	Mac OS X 10.2 und höher
<b>Festplattenspeicher</b>	Mind. 90 MB freier Speicher
<b>Arbeitsspeicher</b>	Mind. 128 MB RAM
<b>Prozessor</b>	Intel- und PowerPC-basierte Macs

## ANHANG II

## DER EICAR-TESTVIRUS

### ÜBER DIE EICAR-TESTDATEI

Die EICAR\*-Testdatei kann gefahrlos in Virenschutztests eingesetzt werden. Sie ist kein Virus und enthält keinen Virencode. Es handelt sich um ein legitimes DOS-Programm und besteht ausschließlich aus ASCII-Zeichen, die gedruckt werden können. Die Datei ermöglicht Ihnen das gefahrlose Simulieren der Vorgänge nach der Erkennung schädlichen Codes durch Sophos Anti-Virus. Beim Versuch, die Datei auszuführen, wird sie wie ein echter Virus erkannt und es werden (anpassbare) Benachrichtigungen erstellt.

Die EICAR-Datei eignet sich auch zum Testen der verschiedenen, erstellbaren Reports.

Ein Exemplar der Testdatei können Sie auf [www.eicar.org](http://www.eicar.org) herunterladen.

### Hinweis

Die EICAR-Datei ist kein echter Virus und kann daher nicht durch Sophos Anti-Virus bereinigt werden. Löschen Sie die Datei bitte selbst.

## ANHANG III

## SONSTIGE PRODUKTE UND SERVICES VON SOPHOS

### Sophos Security and Data Protection

#### *Sophos E-Mail Security and Data Protection*

Sophos E-Mail Security and Control bietet eine Auswahl an Software-Lösungen und integrierten E-Mail-Appliances für ausgereiften und zuverlässigen Schutz vor Viren, Spyware, Trojanern, Spam, anstößigen Inhalten und Datenverlust.

#### *Sophos Web Security and Control*

Sophos Web Security and Control umfasst die zum Schutz vor Bedrohungen aus dem Internet erforderliche Software und eine voll integrierte Web Appliance. Sie bietet eine umfassende Infrastruktur für sicheres Browsing ohne den bislang für effektive Internet-Sicherheit erforderlichen Verwaltungsaufwand.

#### *Sophos NAC Advanced*

Sophos NAC Advanced ist eine Software-Lösung und kontrolliert, wer und was auf Ihr Netzwerk zugreift. Sophos NAC Advanced ist speziell auf Unternehmen ausgelegt, die ausgeklügeltere Richtlinienkontrolle benötigen, als ihnen die NAC-Funktionen von Endpoint Security and Data Protection bieten können.

#### *Sophos SafeGuard Enterprise*

SafeGuard Enterprise ist eine modulare Kontrollplattform zum Schutz von Unternehmensdaten, über die Sicherheitsrichtlinien für PCs und mobile Geräte in gemischten Umgebungen durchgesetzt werden können. Durch die zentrale Administration über nur eine Konsole gestaltet sich die Verwaltung einfach und für den Enduser transparent. SafeGuard Enterprise bietet durch eine geschickte Kombination aus Verschlüsselungsverfahren und Data Loss Prevention (DLP) eine mehrschichtiges Datenschutz-Konzept auf Endpoint-Ebene.

#### *SAV Interface*

Mit SAV Interface™ erhalten Software-Anbieter, OEMs, ISPs und ASPs die Möglichkeit, Sophos Malware-Erkennung in ihre eigenen, den Branchenstandards entsprechenden Firewalls, Gateways und ähnliche Lösungen zu integrieren.

#### *Sophos Small Business Solutions*

Sophos Small Business Solutions bieten vielfach ausgezeichneten und bewährten Schutz vor Viren, Spyware und Spam für Unternehmen mit wenigen oder keinen IT-Fachkräften.

## Sophos Alert Services

**Sophos ZombieAlert™ Service** warnt Ihr Unternehmen sofort, wenn Spammer Computer in Ihrem Netzwerk dazu missbrauchen, Spam-Mails zu versenden oder Denial-of-Service-Attacken durchzuführen.

[www.sophos.de/products/enterprise/alert-services/zombiealert.html](http://www.sophos.de/products/enterprise/alert-services/zombiealert.html)

**Sophos PhishAlert™ Service** warnt Sie nahezu in Echtzeit vor Phishing-Kampagnen, damit Sie die nötigen Schritte einleiten können, um eine falsche Website zu schließen und die Kunden Ihres Unternehmens zu schützen.

[www.sophos.com/products/enterprise/alert-services/phishalert.html](http://www.sophos.com/products/enterprise/alert-services/phishalert.html) (englisch)

**Sophos WebAlert™ Service** warnt Sie rechtzeitig, wenn Webseiten Ihrer Domain Ziel eines Hacker-Angriffs geworden sind oder Malware hosten.

[www.sophos.com/products/enterprise/alert-services/webalert.html](http://www.sophos.com/products/enterprise/alert-services/webalert.html) (englisch)

## Sophos Global Support Services

Für uns bedeutet Support mehr als die simple Bereitstellung von Updates oder die Unterstützung bei Installationen. Wir möchten unser Know-how mit Ihnen teilen und Ihnen so bestmöglichen Schutz bieten.

Wir schulen unsere hauseigenen Support-Teams speziell auf Sophos Lösungen und Drittanbieter-Technologien.

Wann auch immer Sie die Sophos Global Support Services kontaktieren, wird sich ein umfassend geschulter Sophos Mitarbeiter und kein Dispatcher in einem Übersee-Callcenter um Ihre Belange kümmern.

## Technischer Support

Wir verfügen über ein globales Team von Sophos Experten, die Ihnen rund um die Uhr bei der Installation, Konfiguration und Aufrüstung unserer Produkte behilflich sind und auch Ihre technischen Probleme löst.

Standard Support ist rund um die Uhr an 365 Tagen im Jahr im Rahmen aller befristeten Sophos Lizenzen und ohne Aufpreis verfügbar. Bei unbefristeten Lizenzen ist Standard Support als Zusatzleistung zu erwerben. Premium and Platinum Support mit speziellen Service-Level-Verträgen, im Rahmen derer wir Sie bei Nichteinhaltung zugesicherter Zielreaktionszeiten entschädigen, erhalten Sie nach Entrichtung einer Zusatzgebühr, die sich prozentual nach Ihren Lizenzgebühren richtet.

## Professional Services

Sophos Professional Services versorgen Sie mit dem Know-how zur Implementierung und Verwaltung Ihrer Schutzlösungen. Mit einer Reihe individueller und Standard-Services bieten wir Ihnen genau die Unterstützung, die Ihr Unternehmen benötigt. Im Rahmen der Professional Services erhalten Unternehmen wahlweise direkt vor Ort oder über eine Remote-Verbindung Hilfestellung und profitieren so maximal von ihrem Investment in Sophos.

## Technisches Training

Sophos Technical Training bietet weltweit Kurse und Workshops an, in denen Unternehmen den richtigen Umgang mit zunehmend komplexeren und immer neuen Bedrohungen erlernen. Es werden sowohl Kurse für die Bereiche Endpoint, E-Mail und Web Security, als auch individuelle Packages angeboten, die spezifischeren Anforderungen gerecht werden.

Weitere Informationen finden Sie auf [www.sophos.de/support/services](http://www.sophos.de/support/services)

## Kostenlose Tools

Sophos bietet eine Reihe von Tools an, mithilfe derer Schwachstellen und Bedrohungen eingedämmt werden können. Diese Tools können kostenlos heruntergeladen werden und befinden sich auf dem neuesten Stand der Informationstechnologie.

### *Sophos Computer Security Scan*

<http://www.sophos.de/products/free-tools/sophos-computer-security-scan.html>

Der kostenlose Sophos Computer Security Scan zeigt Ihnen die Bedrohungen, die der Sicherheitslösung Ihres Unternehmens entgangen sind. Der Scan erkennt Malware sowie unerwünschte Geräte und Anwendungen, welche Datenverluste verursachen können (z.B. Wechselmedien, Peer-to-Peer-Software, Spiele uvm.)

### *Kostenloser Endpoint Assessment Test*

[www.sophos.de/products/free-tools/sophos-endpoint-assessment-test/](http://www.sophos.de/products/free-tools/sophos-endpoint-assessment-test/)

Testen Sie mit unserem kostenlosen Endpoint Assessment Test Ihren Sicherheitsstatus. Überprüfen Sie einen ausgewählten Computer und finden Sie heraus, ob Betriebssystem-Patches fehlen und sämtliche Sicherheitsanwendungen aktuell und aktiviert sind.

### *Application Discovery Tool*

[www.sophos.de/products/enterprise/applicationdiscovery/eval](http://www.sophos.de/products/enterprise/applicationdiscovery/eval)

Laden Sie unser kostenloses Application Discovery Tool herunter, um Ihr Netzwerk auf unerwünschte Anwendungen zu überprüfen, die von Sophos kontrolliert werden können. Das Tool läuft neben der bereits bei Ihnen installierten Virenschutzsoftware.

### *Sophos Threat Detection Test*

[www.sophos.de/products/free-tools/sophos-threat-detection-test.html](http://www.sophos.de/products/free-tools/sophos-threat-detection-test.html)

Unser kostenloser Threat Detection Test stellt Ihren bestehenden Virenschutz auf die Probe. Dieses Tool scannt und findet Viren, Spyware und Adware sowie Zero-Day-Bedrohungen, die dem bestehenden Schutz u.U. entgangen sind. Zum Ausführen des Tests braucht Ihre verwendete Virenschutzsoftware weder deinstalliert noch deaktiviert zu werden.

### *Sophos Anti-Rootkit*

<http://www.sophos.de/products/free-tools/sophos-anti-rootkit.html>

Unsere kostenlose Sophos Anti-Rootkit-Software entfernt Rootkits zuverlässig. Dieses Tool scannt auf versteckte Rootkits sowie erkennt und entfernt diese durch Einsatz eines hochentwickelten Verfahrens zur Erkennung von Rootkits.

Mehr Informationen über kostenlose Sophos Tools unter <http://www.sophos.de/products/free-tools/>