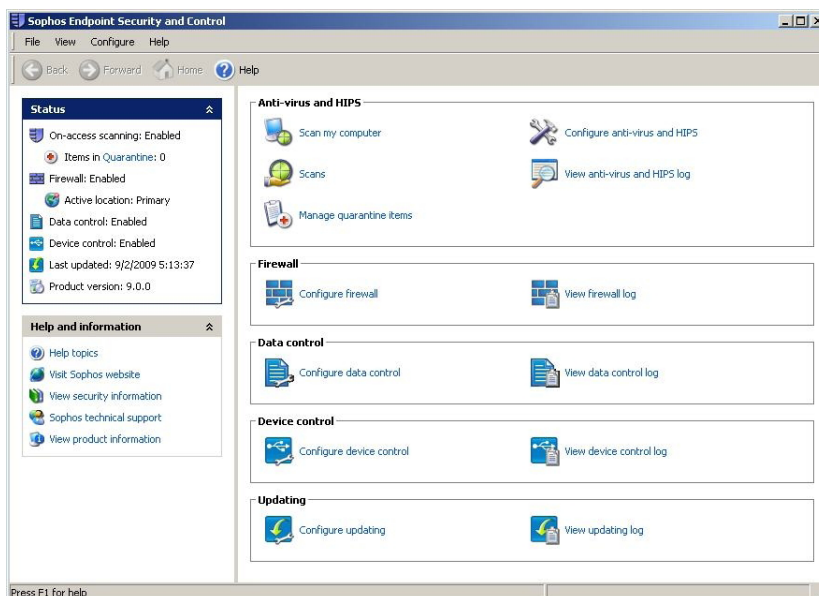


Sophos Endpoint Security and Control für Windows sorgt mit seinen vielfach ausgezeichneten Schutzverfahren für mehr Sicherheit in Umgebungen mit tausenden Windows-Desktops, -Laptops und -Servern. Nur ein Endpoint-Client erkennt Viren, Spyware und Adware, verdächtige Dateien, verdächtiges Verhalten und potenziell unerwünschte Anwendungen (PUAs), überwacht außerdem den Transfer sensibler und vertraulicher Daten und kontrolliert den Einsatz von Wechselmedien und nicht zugelassenen Anwendungen wie VoIP, IM, P2P und Spielen. Einzelprodukte werden somit überflüssig.

Ausgezeichneter Schutz vor unterschiedlichsten Bedrohungen in nur einem Produkt

- Die Sophos Virus Detection Engine schützt Windows-Server, -Desktopcomputer, -Laptops und -Handhelds vor Viren, Spyware und Adware, verdächtigen Dateien und Verhaltensmustern, potenziell unerwünschten Anwendungen, Wechselmedien sowie vor nicht zugelassener VoIP-, IM-, P2P- und Spielesoftware.
- Unser zentraler Client setzt zum Schutz vor neuen und unbekanntem Bedrohungen eine Kombination zahlreicher Verfahren ein. Ein Host Intrusion Prevention-System (HIPS) analysiert Code vor und während seiner Ausführung. Live-Anti-Virus gleicht verdächtige Dateien mit der umfassenden Reputationsdatenbank der SophosLabs ab.
- Die in den Agent integrierte Live-URL-Filterung sorgt dafür, dass auch mobile User vor Infektionen durch Malware hostende Websites geschützt werden. Ein automatischer Live-Abgleich mit der SophosLabs Datenbank (enthält Daten zu Millionen missbrauchter Websites) verhindert sämtliche Zugriffe auf schädliche URLs.
- Legitime Software-Anwendungen wie VoIP, P2P, IM, Mediaplayer und Spiele können für verschiedene Computergruppen gesperrt oder zugelassen werden. Dieser Prozess wird zentral über ActivePolicies™ in der Sophos Enterprise Console™ geregelt.
- Durch flexible und eingehende Kontrollen von Wechselmedien können ausgewählte Geräte zugelassen, die Verschlüsselung von Geräten vorgeschrieben oder nur Lesezugriff gewährt werden. Außerdem besteht die Möglichkeit, drahtlose Verbindungen wie Modems (einschließlich 3G-Versionen) zu kontrollieren.
- Die vollständig integrierte Funktion zur Inhaltsüberwachung für Speichermedien und Anwendungen, welche auf eine Reihe regelmäßig aktualisierter Datendefinitionen aus den SophosLabs zurückgreift, kontrolliert die Übertragung sensibler Daten und dämmt so das Risiko für versehentliche Datenverluste ein.



Vorteile

- » Mit multifunktionalem Endpoint-Client keinerlei Bedarf für weitere Einzelprodukte
- » Automatische Blockierung unbekannter Malware mit Behavioral Genotype® Protection durch Code-Analyse noch vor Ausführung
- » Integrierter Inhaltsscan zur Verhinderung versehentlicher Datenverluste
- » Identifizierung unbekannter Malware, verdächtiger Dateien und Verhaltensmuster dank integrierter Funktionen zur Bedrohungserkennung noch vor Code-Ausführung sowie übergreifendem Einsatz von Intrusion Prevention-Verfahren (Laufzeit) und Live-Schutz (Sophos Live Protection)
- » Zum Schutz vor allerneuesten Bedrohungen Abgleich von URLs und verdächtigen Dateien mit der Reputationsdatenbank der SophosLabs
- » Kontrolle legitimer Software-Anwendungen wie VoIP und IM
- » Verwaltung des Einsatzes von Wechselmedien, optischen Medienlaufwerken und drahtlosen Netzwerkprotokollen
- » Individuell konfigurierbare, rollenbasierte Administrationsfunktionen zur sorgfältigen Kontrolle von Administrator-Privilegien
- » Schnelle Erstellung von Virenschutz- und HIPS-Richtlinien sowie deren Anwendung auf zahlreiche Gruppen
- » Zentrale Systembereinigung von Dateien, Registrierungseinträgen und laufenden Prozessen
- » Integrierter Quarantäne-Manager zum Löschen, Desinfizieren und Zulassen von Dateien
- » Automatische Updates mit dem neuesten Schutz aus den SophosLabs™, unserem globalen Netzwerk aus Bedrohungsanalysecentern
- » Zugriffs-, bedarfs- und zeitgesteuertes Scanning mit Decision Caching™ zur ausschließlichen Prüfung geänderter Dateien
- » Support und persönliche Unterstützung rund um die Uhr und während der gesamten Lizenzdauer

Automatische, vereinfachte, zentrale Verwaltung von einer einzigen Konsole aus

- Das Dashboard zeigt den Sicherheitsstatus und Sicherheitsrisiken in Echtzeit an. Vor Erreichen der festgelegten Schwellenwerte werden automatisch Benachrichtigungen per E-Mail versendet.
- Die Synchronisation mit Microsoft Active Directory stellt sicher, dass die Installation schnell erfolgt und neue Computer im Netzwerk automatisch geschützt sind.
- Mit integrierter Data, Application und Device Control entstehen keinerlei Zusatzkosten für Installation und Verwaltung. Richtlinien für Computer-Gruppen können ganz nach den individuellen Sicherheitsanforderungen bestimmter Standorte oder Abteilungen konfiguriert werden.
- Durch Einsatz individuell konfigurierbarer, rollenbasierter Administrationsfunktionen können ausgewählte User mit Verwaltungsaufgaben betraut werden, ohne volle Administrationsrechte einräumen zu müssen.
- Eine einzige ActivePolicy, die sowohl Virenschutz als auch HIPS einbezieht, ermöglicht die schnelle Erstellung und gleichzeitige Anwendung von Sicherheitseinstellungen für diverse Computer und Gruppen.
- Kleine und regelmäßig aktualisierte Schutzupdates werden automatisch heruntergeladen und netzwerkübergreifend installiert.
- Endpoints können in einem Durchgang vollständig desinfiziert werden. Registrierungseinträge, laufende Prozesse und sogar Dateien auf der Festplatte werden im Bedarfsfall entfernt.
- Informationen zur Sicherheit und Verwaltung werden über individuell anpassbare, grafische Reports bereitgestellt, die zeitgesteuert abgerufen und per E-Mail direkt an ausgewählte Empfänger versendet werden können.

Scheller, besserer und proaktiver Schutz dank innovativer Verfahren

- Mit Genotype® Virus Detection werden Virenfamilien proaktiv blockiert, noch bevor spezifische Virenkennungen verfügbar sind.
- Das HIPS-Verfahren von Sophos verwendet die bestehende Anti-Virus Engine, um Programme mit verdächtigem Verhalten noch vor Ausführung zu identifizieren.
- Das Behavioral Genotype®-Verfahren scannt nach zahlreichen spezifischen Verhaltensweisen und Eigenschaften und schützt proaktiv vor Zero-Day-Malware. So erkennt dieses Verfahren neue Bedrohungen bereits vor Code-Ausführung.
- Die integrierte Erkennung verdächtiger Dateien noch vor ihrer Ausführung wird mit Laufzeitverhaltensanalysen und Buffer Overflow-Schutz kombiniert, um Malware, verdächtige Dateien und verdächtiges Verhalten zu erkennen.
- Die Algorithmen der Behavioral Genotype Protection werden ständig mit einer umfassenden Library legitimer Anwendungen abgeglichen, damit die Erkennung stets auf dem neuesten Stand und somit zuverlässig ist.
- Decision Caching verbessert das zugriffsgesteuerte Scanning durch das ausschließliche Abfangen und Scannen neuer bzw. solcher Dateien, die seit dem letzten System-Zugriff geändert wurden.
- Schnelle Bedrohungsanalyse aus den SophosLabs und die schnellsten Updates der Branche werden bis zu alle 10 Minuten heruntergeladen.

Professionelle Beratung 24x7

- Unser rund um die Uhr verfügbarer Support und die SophosLabs, unser weltweites Netzwerk aus Bedrohungsanalysecentern, reagieren rasch auf neue und unbekannte Bedrohungen.

Sprachen

- Deutsch, Englisch, Französisch, Japanisch, Italienisch, Spanisch, Vereinfachtes und Traditionelles Chinesisch

Alle beschriebenen Funktionen sind in Sophos Endpoint Security and Control für Windows enthalten. Einige dieser Funktionen können jedoch abhängig von der erworbenen Lizenz deaktiviert sein. Mehr Informationen erhalten Sie unter www.sophos.de.

Systemanforderungen

Unterstützte Plattformen

- » Windows 7
- » Windows Vista*
- » Windows Server 2003**
- » Windows Server 2008*
- » Windows XP*
- » Windows 2000 Server
- » Windows 95/98 and NT4***
- » VMware ESX 3.0
- » VMware Workstation 5.0
- » VMware Server 1.0

Festplattenspeicher

- » Windows XP/2003/Vista/7: 120 MB
- » Windows 2000: 120 MB
- » Windows 95/98: 90 MB
- » Windows NT4: 90 MB

Empfohlener Arbeitsspeicher

- » Windows XP/2003/Vista/7: 256 MB
- » Windows 2000: 256 MB
- » Windows 95/98: 128 MB
- » Windows NT4: 256 MB

* Einschließlich AMD64

** Einschließlich Itanium

*** Adware- und PUA-Erkennung sowie Application Control und HIPS stehen auf diesen Plattformen nicht zur Verfügung.



Sophos Anti-Virus ist außerdem für diverse Nicht-Windows-Plattformen vom Gateway bis zum Endpoint erhältlich, z.B. für Windows, Macintosh, Linux, UNIX, NetWare und OpenVMS. Diese Lösungen werden auf separaten Datenblättern beschrieben.

Vollständige Details unter: www.sophos.de