

Sophos für Microsoft SharePoint

Sophos für Microsoft SharePoint schützt Ihre unternehmenskritischen Daten und gemeinschaftlich genutzten Umgebungen mit vielfach ausgezeichnetem Echtzeit-Schutz. Es stoppt Viren, Spyware, Adware, verdächtige Dateien und potenziell unerwünschte Anwendungen (PUAs). Um der Verbreitung sensibler oder unangemessener Inhalte vorzubeugen, setzt die Software außerdem differenzierte Funktionen zur Inhaltsfilterung ein.

Das Komplettpaket aus Bedrohungsschutz und Inhaltskontrolle

- On-Access-, On-Demand- und zeitgesteuerte Inhaltsscans stellen den Schutz Ihrer Daten selbst vor neuesten Bedrohungen sicher. Gleichzeitig wird für eine signifikante Kostenreduktion sowie für maximale Transparenz beim Enduser gesorgt.
- Unsere Software enthält ein Host Intrusion Prevention-System (HIPS) zur Abwehr von Zero-Day-Bedrohungen. Echtzeit-Erkennungsverfahren vor Ausführung von Code identifizieren unbekannte Malware sowie verdächtige Dateien und Verhaltensmuster.
- Eine technisch ausgefeilte Richtlinien-Engine zur Inhaltsfilterung unterbindet die Verbreitung unangemessener und sensibler Inhalte auf Basis von Dateinamen, -typen bzw. Ausdrücken und Stichwörtern, die sich in einer Datei befinden.
- Über unseren benutzerfreundlichen und voll integrierten Quarantäne-Manager können Malware, potenziell unerwünschte Anwendungen, verdächtige Dateien und kontrollierte Inhalte zugelassen, gelöscht oder desinfiziert werden.

Vereinfachte und automatisierte Verwaltung

- Unsere benutzerfreundliche webbasierte Management-Konsole macht die Sicherung Ihrer SharePoint-Umgebung zum Kinderspiel. Kernstück der Verwaltung ist unser Echtzeit-Dashboard, das mit „Point-and-Click“-Richtlinienanpassungen, effizienten Quarantäne-Verwaltungsoptionen sowie zuverlässigen und individuelle Reportingfunktionen kaum Wünsche offen lässt.
- Ihre gesamte SharePoint-Serverfarm kann über nur eine zentrale Management-Konsole verwaltet werden. Vereinfachte Kontrollen setzen Richtlinienanpassungen automatisch um und konsolidieren Reports nahtlos.
- Unsere umfassenden und individuell gestaltbaren Reporting-Funktionen liefern sofortigen Einblick in Bedrohungsaktivitäten, Performance der Inhaltsfilterung und Quarantäne-Status. Detaillierte Protokolle mit Suchfunktion ermöglichen eine lückenlose Prozess-Nachverfolgung.



Vorteile

- » Schutz Ihrer unternehmenskritischen Daten vor Viren, Spyware, Adware, verdächtigen Dateien und potenziell unerwünschten Anwendungen
- » Erkennen unbekannter Malware, verdächtigter Dateien und Verhaltensmuster durch integrierte Intrusion Prevention-Verfahren, die Schädlinge bereits vor Code-Ausführung aktiv bekämpfen
- » Kontrollierte Verbreitung unangemessener oder sensibler Inhalte durch ausgefeilte Richtlinienkontrollen zur Inhaltsfilterung
- » Vereinfachte Verwaltung von Einzelserversn bzw. ganzen Serverfarmen über unsere einzigartige aufgabenbasierte Management-Konsole nach dem Prinzip „Mit 3 Mausklicks zum Ziel“
- » Umfassende Reporting-Funktionen für sofortigen Einblick in Bedrohungsaktivitäten, Performance der Inhaltsfilterung und Quarantäne-Status
- » Detaillierte Protokolle mit Suchfunktion zur lückenlosen Prozess-Nachverfolgung
- » Integrierter Quarantäne-Manager zum Löschen, Desinfizieren und Zulassen von Dateien
- » Automatische Updates mit dem neuesten Schutz aus den SophosLabs™, unserem globalen Netzwerk aus Bedrohungsanalysecentern
- » Scans bei Zugriff, bei Bedarf oder zu festgelegten Zeiten für optimalen Schutz bei maximaler Flexibilität
- » Support und persönliche Unterstützung rund um die Uhr und während der gesamten Lizenzdauer

Schneller, besserer und proaktiver Schutz mit innovativen Verfahren

- Mit der Genotype® Virus Detection-Technologie werden Virenfamilien proaktiv blockiert, noch bevor spezifische Virenerkennungen verfügbar sind.
- Unser HIPS-Verfahren verwendet die bestehende Anti-Virus-Engine, um verdächtige Programme und potenzielle Malware noch vor Ausführung zu identifizieren.
- Unsere Behavioral Genotype®Protection scannt nach zahlreichen spezifischen Verhaltensweisen und Eigenschaften, um Zero-Day-Malware proaktiv zu stoppen. So erkennt dieses Verfahren neue Bedrohungen bereits vor Code-Ausführung.
- Damit die Erkennung stets auf dem neuesten Stand und somit zuverlässig ist, führen wir regelmäßig Gegenprüfungen unserer Verhaltensregeln in einer umfassenden Library legitimer Anwendungen durch.
- Die Scan-Engine blockiert potenziell unerwünschte Anwendungen (PUAs), die als schädlich bekannt sind, unter dem Verdacht der Schädlichkeit stehen, Adware beinhalten oder Ressourcen beanspruchen (z.B. Dienstprogramme, Symbolleisten und andere verdächtige Anwendungen).
- Kompakte Updates werden bis zu alle fünf Minuten veröffentlicht – ein Vorteil für Unternehmen, die schnellen Schutz ohne negativen Einfluss auf ihre Netzwerkressourcen wünschen.

Inhaltsfilterung und Data Loss Prevention für lückenlose Compliance

- Verhindert Datenverluste, schützt vor Haftbarkeitsansprüchen und stellt mit ausgefeilten Richtlinien zur Kontrolle von Dateitypen (z.B. ausführbare Dateien, Media-Dateien und Archive) und sensiblen Daten (z.B. Binärdateien, Quellcode, Datenbanken, Kontaktlisten und XML-Dateien) die produktive Nutzung der Infrastruktur sicher.
- Unterbindet Dateityp-Maskerading durch Einsatz von True File Type Anti-Spoofing-Technologie (z.B. Umbenennung einer MP3-Datei in eine DOC-Datei).
- Hält die unternehmensweite Compliance durch Einsatz benutzerfreundlicher Inhaltsrichtlinien aufrecht. Diese basieren auf vom Administrator definierten Stichwörtern, Ausdrücken bzw. regulären Ausdrücken, die sich in gängigen Dateitypen befinden, und kontrollieren die Verbreitung sensibler oder vertraulicher Daten.
- Filtert auf Basis unserer Liste anstößiger Begriffe/Ausdrücke Ihre Umgebung nach unangemessenen Inhalten und reduziert somit den anstößigen Sprachgebrauch.
- Verschiebt Dateiverstöße in die Quarantäne bzw. blockiert und/oder ersetzt diese mit Platzhaltertext.

Zuverlässiger Experten-Support

- Hochspezialisierte Analysten in unseren SophosLabs stellen proaktiven und schnellen Schutz vor bekannten und unbekanntem Bedrohungen bereit.
- Die in den SophosLabs verwendeten Verfahren, eine globale Übersicht über neue Bedrohungen und das Fachwissen über Schädlinge ermöglichen die Analyse und eine schnelle Reaktion rund um die Uhr: Die idealen Voraussetzungen für Ihr Unternehmen, um stets bestens vor zunehmend komplexen Bedrohungen geschützt zu sein.
- Unser rund um die Uhr verfügbarer, hauseigener Support-Service ist in jeder Lizenzierung als Standardleistung inbegriffen.
- Unsere Support-Experten bieten individuellen Support per E-Mail oder Telefon, oder aber Sie nutzen unsere webbasierte Support-Knowledgebase zur Beantwortung Ihrer Fragen.
- Sie möchten Sophos Anti-Virus testen? Besuchen Sie www.sophos.de/products.

Systemanforderungen

Unterstützte Plattformen

SharePoint

- » Microsoft SharePoint Services 3.0, 32 und 64 Bit, SP1 und SP2
- » Microsoft SharePoint Server 2007, 32 und 64 Bit, SP1 und SP2
- » Microsoft SharePoint Foundation 2010
- » Microsoft SharePoint Server 2010 (alle Editionen)
- » Microsoft Search Server 2008
- » Microsoft Search Server 2008 Express Edition
- » Microsoft Office Project Server 2007

Betriebssystem

- » Windows Server 2003, 32 und 64 Bit, SP2 (alle Editionen)
- » Windows Server 2003 R2, 32 und 64 Bit, SP2 (alle Editionen)
- » Windows Small Business Server 2003, SP2
- » Windows Small Business Server 2003 R2, SP2
- » Windows Server 2008, 32 und 64 Bit, SP1 und SP2 (alle Editionen)
- » Windows Small Business Server 2008, SP1 und SP2
- » Windows Server 2008 R2, SP0 und SP1 (alle Editionen*)
- » Windows Small Business Server 2011

SQL-Server

- » Microsoft SQL Server 2005, SP3 (alle Editionen)
- » Microsoft SQL Server 2008, SP1 und SP2 (alle Editionen)
- » Microsoft SQL Server 2008 R2 (alle Editionen)

Hardware

- » Festplattenspeicher: mind. 1 GB
- » Arbeitsspeicher: mind. 1 GB (besser mind. 2 GB)
- » CPU: mind. 1.5 GHz (besser mind. 2 GHz)

*Server Core-Editionen werden nicht unterstützt (da keine Unterstützung durch SharePoint besteht).