

Sophos E-Mail Security and Data Protection

Sophos E-Mail Security and Data Protection bietet umfassende Funktionen zum Bedrohungs- und Datenschutz für die gesamte E-Mail-Infrastruktur: Vom Gateway bis zum Workgroup-Server. Die Lösung beseitigt sowohl bekannte als auch neue Bedrohungen wie Spam, Phishing und Malware und verhindert außerdem Datenverluste und Compliance-Verstöße. Sie ermöglicht sicheren, produktiven internen und externen E-Mail-Verkehr ohne großen Administrations- und Useraufwand.

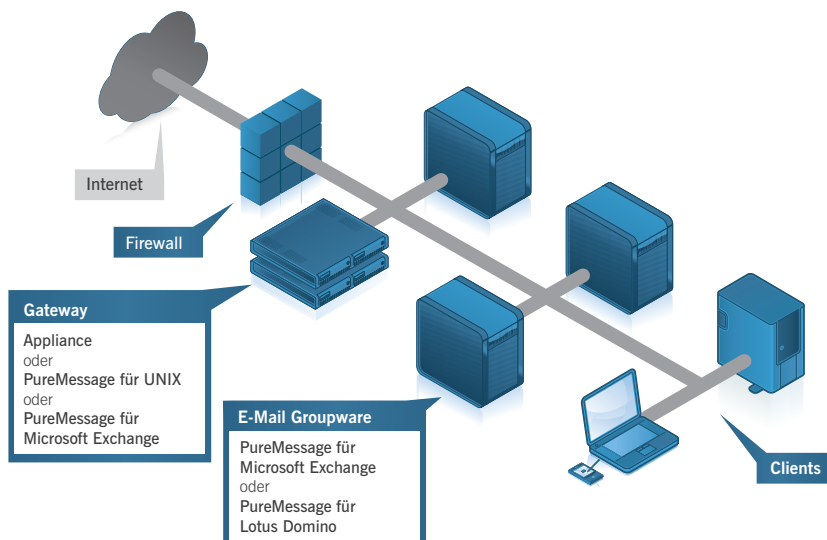
Umfassender Schutz vor Bedrohungen und Datenverlusten für Ihre E-Mail-Infrastruktur

Mit Sophos E-Mail Security and Data Protection verhindern Sie, dass unerwünschte und schädliche E-Mails in Ihren Posteingang oder vertrauliche Daten nach außen gelangen. Eine Lizenz umfasst vollautomatische Managed Appliances und benutzerfreundliche Software, die in Ihrer gesamten E-Mail-Infrastruktur durchgehend für Sicherheit sorgt:

- Unsere Managed Appliances und Softwarelösungen wehren am Gateway eingehende Bedrohungen wie Spam, Phishing-Angriffe, Spyware und Malware schnell und wirksam ab.
- Mit leistungsstarken Verschlüsselungsfunktionen sowie Inhalts- und Attachment-Kontrollen gehören Datenverluste der Vergangenheit an.
- Anhand konfigurierbarer Richtlinien legen Sie Nutzungsbedingungen für den E-Mail-Verkehr fest und sorgen für lückenlose Compliance mit Gesetzen, Richtlinien und Vorschriften.

Schnellerer und besserer Schutz

Das Fachwissen und die Erfahrung der SophosLabs™ im Bereich Malware, Spam, unerwünschte Anwendungen und Internet ermöglichen den schnellsten und besten Schutz vor Mischbedrohungen. Eine Kombination aus Behavioral Genotype® Protection und schnellen Updates von Virenkennungen sorgt dafür, dass neue und unbekannte Malware sowie Spam zuverlässig gestoppt werden.



Vorteile

- » Schutz der gesamten E-Mail-Infrastruktur: Vom Gateway bis zur Workgroup
- » Blockieren von Spam, Phishing, Malware und Sperren unerwünschter Anwendungen
- » Proaktiver Zero-Day-Schutz durch diverse Abwehrmechanismen
- » Leistungsstarke Verschlüsselungsfunktionen und Inhaltsfilterung zur gezielten Verhinderung von Verlusten sensibler Daten über den E-Mail-Verkehr
- » Überprüfung auf Updates alle fünf Minuten sowie automatisches Herunterladen und Installieren der Updates
- » Umfassender Echtzeit-Spamschutz
- » Als Hardware- oder Softwareversion erhältlich
- » Nahtlose Einbindung in Active Directory und andere LDAP-Systeme
- » Remote-Überwachung des Betriebsverhaltens von Hardware und Software auf allen Appliances, bei Bedarf inklusive Remote-Unterstützung
- » Leistungsstarke Reporting-Funktionen für bessere Berichterstattung über den E-Mail-Verkehr
- » Support, Updates und Upgrades sind rund um die Uhr an 365 Tagen im Jahr für die Dauer der Lizenz enthalten. Bei individuellem Support-Bedarf kann Sophos jederzeit kontaktiert werden.

Proaktiver Schutz vor Spam, Malware, Phishing und anderen E-Mail-Bedrohungen

Das Sender Genotype-Verfahren bietet lückenlosen Schutz vor neuen und unbekanntem Spam-Quellen, wodurch bis zu 90% des gesamten Spamaufkommens bereits vor einem Scan beseitigt werden.

Genotype® Detection blockiert Malware-Familien und Spamkampagnen proaktiv.

Abwehr von unerwünschten und unbefugten Zugriffen auf Ihr Gateway ist durch Behavioral Genotype® Protection (HIPS) gewährleistet. Diese Technologie erkennt neue Bedrohungen noch vor der Ausführung von Code und schützt so proaktiv vor Zero-Day-Malware.

Durch Einsatz zahlreicher Spamschutzverfahren wie Obfuscation Detection, URL-Tracking (Web-Adressen-Nachverfolgung), Heuristiken und Fingerprinting von Inhalten werden mehr als 99% Spam abgewehrt.

Ein umfassendes Echtzeit-System schützt durch Einsatz des Sophos SXL-Verfahrens vor neuesten Spamkampagnen.

Einfacher und wirksamer Schutz vor Datenverlusten

Die leistungsfähigen Tools von Sophos E-Mail Security and Data Protection schützen vor versehentlicher oder absichtlicher Weitergabe vertraulicher Informationen per E-Mail:

- Sophos' einzigartiges und einfaches Data Loss Prevention-Verfahren integriert das Scanning auf sensible Daten in die Threat Detection Engine (Endpoint und E-Mail Appliances). Mit vorgefertigten Datendefinitionen sorgt es für schnelles, einfaches und einheitliches Erstellen und Durchsetzen von Richtlinien zur Verhinderung von Datenverlusten.
- Betreffzeilen, Textkörper sowie Attachments von internen und ausgehenden E-Mails werden auf Stichwörter, individuelle Zeichenketten und Dateitypen überprüft.
- Für ausgehende E-Mails bestimmter Gruppen oder User ist die Einrichtung individueller Disclaimer möglich.
- Flexible Optionen zur Verschlüsselung von E-Mails, wie sie u.a. von unserer vielseitigen Standalone SafeGuard MailGateway Software-Appliance realisiert werden, stellen sicher, dass die Vertraulichkeit, Integrität und Authentizität Ihrer E-Mail-Kommunikation in jedem Fall gewahrt bleibt.
- Unsere zum Patent angemeldete SPX Encryption (erhältlich in unseren E-Mail- und Encryption-Appliance-Produkten) eröffnet Ihnen die Möglichkeit, auch verschlüsselten E-Mail-Kontakt mit Unternehmen und Usern zu pflegen, die selbst über keine Verschlüsselungsinfrastruktur verfügen. Die Realisierung erfolgt durch Einsatz der flächendeckend verfügbaren PDF-Technologie, welche die Prozessabwicklung für den User so einfach wie möglich gestaltet.
- Durch integrierte TLS-Verschlüsselung und Einbindungsmöglichkeiten in Verschlüsselungslösungen anderer Hersteller sind Ihren Verschlüsselungsoptionen zur Sicherung Ihres E-Mail-Traffics praktisch keine Grenzen gesetzt.

Software-Komponenten

Sophos Anti-Spam-Engine

Diese Engine bietet eine Reihe von Verfahren zur Erkennung neu entstehender Spamkampagnen: Sender Genotype, Prüfsummen, Heuristiken, URL-Erkennung und Entnahme von Bild- und Anhangsabdrücken.

Sophos Anti-Malware-Engine

Diese Engine erkennt und blockiert mit nur einem Scan alle Arten von Malware wie Spyware, Trojaner, Würmer, verdächtige Dateien und unerwünschte Anwendungen.

Sophos Management-Konsolen

Integrierte Konsolen mit Weboberfläche oder Microsoft Management Console, die sich leicht bedienen lassen und die Integration von Active Directory ermöglichen, sorgen für minimalen Zeitaufwand bei der Verwaltung.

Lösungen, die auf Ihre Arbeitsweise zugeschnitten sind

Ob Sie nun in einem Kleinunternehmen mit nur wenigen Mailboxen tätig sind oder in einem Großunternehmen mit komplexer Netzwerkstruktur und unzähligen Computern – für jede E-Mail-Infrastruktur bietet Sophos E-Mail Security and Data Protection eine passende Lösung. Unsere Produkte sind für diverse Plattformen erhältlich, können an beliebigen Punkten der E-Mail-Infrastruktur implementiert werden, vereinen Malware- und Spamschutz sowie ermöglichen anhand leistungsstarker Richtlinien das Enforcement allgemeiner Nutzungsbedingungen für den gesamten E-Mail-Verkehr: Ganz gleich, ob intern, eingehend oder ausgehend.

Hardware-Lösungen: Gateway

Sophos E-Mail Appliances

Die optimierten, leistungsstarken E-Mail Appliances von Sophos sind für Unternehmen konzipiert, die den Zeit- und Arbeitsaufwand bei der Verwaltung des E-Mail-Gateways minimieren möchten, aber dennoch auf umfassenden Schutz nicht verzichten können. Diese branchenweit ersten Managed Appliances beseitigen bzw. reduzieren zuverlässig einen Großteil des Verwaltungsaufwands und verschaffen Ihnen somit einen signifikanten Zeitvorteil. Um sicherzustellen, dass die Appliances stets über aktuellsten Schutz verfügen und jederzeit verfügbar sind, werden sie extern auf ihre Verbindung mit Sophos überwacht.

Drei Modelle sind erhältlich: Die ES1100 (200.000 E-Mails pro Stunde), die ES5000 (380.000 E-Mails pro Stunde) und die ES8000 (550.000 E-Mails pro Stunde).

Sophos SafeGuard MailGateway

Die Sophos SafeGuard MailGateway Software-Appliance ist eine leistungsstarke, flexible Standalone-Lösung zur E-Mail-Verschlüsselung. Sie kann problemlos gemeinsam mit anderen Sophos E-Mail-Produkten oder in SMTP-E-Mail-Infrastrukturen anderer Anbieter eingesetzt werden. Durch ihre Vielseitigkeit, High-Performance und Skalierbarkeit erweist sich diese Software-Appliance selbst für den Einsatz in Umgebungen mit hochkomplexen Anforderungen als ideal.

Software-Lösungen: Gateway und Groupware

PureMessage für UNIX

PureMessage für UNIX ist eine hochgradig skalierbare und konfigurierbare softwarebasierte Gateway-Lösung, die sich ideal für große Organisationen, Behörden und höhere Bildungseinrichtungen sowie für Managed-Service-Provider eignet. Die flexible Installation und Richtlinienerstellung lassen sich an die unterschiedlichsten Anforderungen bei der Bewältigung des täglichen E-Mail-Aufkommens anpassen. PureMessage für UNIX bietet Schutz und Richtlinien-Enforcement ohne großen Verwaltungsaufwand.

PureMessage für Microsoft Exchange

PureMessage für Microsoft Exchange ist eine umfassende Softwarelösung für Windows SMTP-Gateways und Microsoft Exchange-Groupware. Durch die Einbindung von Active Directory und die umfangreichen Funktionen zur Erstellung und Durchsetzung von Richtlinien können Sie für ein- und ausgehende sowie für interne E-Mails im Handumdrehen Regeln zur Inhaltsfilterung einrichten. PureMessage für Microsoft Exchange ist hochgradig skalierbar und unterstützt alle bekannten Exchange-Cluster-Modelle. Über eine einzige Management-Konsole können Sie mehrere Serverinstallationen verwalten und überwachen.

PureMessage für Lotus Domino

PureMessage für Lotus Domino schützt eingehende, ausgehende und interne E-Mails in Domino-Datenbanken und -Posteingängen zuverlässig vor Spam und Malware. Leistungsstarke Funktionen zum Enforcement von Inhaltsrichtlinien suchen nach Stichwörtern, sensiblen Daten und True File Types. Ausgehende E-Mails können mit individuell anpassbaren Disclaimern versehen werden, und eine Konsole im Stil von Notes vereinfacht die zentrale Verwaltung und Konfiguration.

Begriffserläuterungen

Genotype-Verfahren

Schützt proaktiv vor neuen Varianten von Viren- und Spambfamilien, noch bevor ein spezifischer Schutz in Form von Virenkennungen zur Verfügung steht.

Behavioral Genotype Protection

Liefert die Vorteile eines Host Intrusion Prevention Systems (HIPS), das vor unbekanntem Bedrohungen schützt, indem Programmcode bereits vor seiner Ausführung analysiert wird.

Sophos SXL

Unsere Online-Datenbank mit Spamschutz-Informationen bietet Echtzeit-Schutz vor neuesten Spamkampagnen.

Varianten- und Spam-Profilierung

Dieses Verfahren ermöglicht über mehrere Erkennungsmechanismen in der Sophos Anti-Spam-Engine eine wirksame Reaktion auf immer wieder neue Spamkampagnen.

Sender Genotype-Verfahren

Spürt Botnets proaktiv auf und blockiert mit innovativer Reputation Filtering-Technologie bis zu 90% des Spamaufkommens bereits bei der Verbindungsherstellung.

Integration von Verzeichnisdiensten

Einfache Einbindung von Microsoft Active Directory und anderen Verzeichnisdiensten, wodurch ein gruppen- und userbasiertes Richtlinien-Enforcement möglich wird.

Untersuchung von Stichwörtern und Zeichenketten

Durch die Überprüfung von E-Mails auf Stichwörter und Zeichenketten wie Sozialversicherungs- und Kreditkartennummern und die Auslösung individuell anpassbarer E-Mail-Aktionen werden unerwünschte Inhalte fern- und vertrauliche Inhalte intern gehalten.

True File Type-Erkennung

Jegliche Versuche, E-Mail-Attachments durch Fälschung von Dateitypen zu verbergen, werden aufgedeckt.

Management mehrerer Server

Zentrale Verwaltung von Software, die auf mehreren Servern installiert ist: Überschaubare Ansicht aller E-Mails und einfache Übertragung von Konfigurations- und Richtlinienänderungen.

Remote-Überwachung

Konstante Überprüfung von mehr als 40 verschiedenen Einstellungen und Zuständen, wodurch Systemadministratoren und Sophos über evtl. erforderliche Korrekturmaßnahmen zur Erhaltung der E-Mail-Sicherheit informiert werden.

SophosLabs – niemand kennt sich besser mit Bedrohungen aus

Die hoch qualifizierten Analysten in den SophosLabs™, unserem globalen Netzwerk aus Bedrohungsanalysecentern, bauen auf 20 Jahre Erfahrung, um allen Kunden von Sophos proaktiven, schnellen Schutz vor bekannten und unbekanntem Bedrohungen zu bieten. Die in den SophosLabs™ verwendeten Verfahren, eine globale Übersicht über neue Bedrohungen und das Fachwissen über Schädlinge ermöglichen eine schnelle Analyse und Reaktion auf zunehmend komplexe Bedrohungen rund um die Uhr und gewährleisten den lückenlosen Schutz Ihres Unternehmens.

Branchenführender, rund um die Uhr verfügbarer Support

Dank des in der Lizenz inbegriffenen technischen Supports können Sie sich bei Problemen rund um die Uhr an unser erfahrenes Support-Team wenden. Kontaktieren Sie für individuellen Support unsere technischen Mitarbeiter per Telefon oder E-Mail oder nutzen Sie einfach unsere webbasierte Support-Knowledgebase. Die Experten in unseren weltweit präsenten Supportcentern bauen beim Rekonstruieren, Analysieren und Beheben von Problemen auf einschlägige Erfahrung und bewährte Verfahren.

Einfache Preis- und Lizenzstruktur

Auf der Basis einer Lizenz* pro User erhalten Sie nicht nur die aktuelle Software sondern alle zukünftigen Updates, Management- und Produkt-Upgrades sowie technischen Support. Sie können Ihre Lizenz außerdem durch unsere Web Security and Control-, Endpoint Security and Control- und NAC-Services erweitern.

Sprachen

E-Mail Appliances

Benutzeroberfläche und E-Mail-Digest-Listen: Deutsch, Englisch, Französisch, Italienisch, Japanisch, Spanisch, Chinesisch (sowohl vereinfacht als auch traditionell) und Schwedisch

Management-Konsole: Englisch

SafeGuard MailGateway Encryption Appliance: Englisch, Deutsch

PureMessage für UNIX

Benutzeroberfläche und E-Mail-Digest-Listen: Deutsch, Englisch, Französisch, Italienisch, Japanisch, Spanisch, Schwedisch und Traditionelles Chinesisch

Management-Konsole: Englisch

PureMessage für Microsoft Exchange: Englisch, Japanisch

PureMessage für Lotus Domino*: Englisch

Jetzt kostenlos testen

Testen Sie Sophos E-Mail Security and Data Protection jetzt 30 Tage lang kostenlos, indem Sie sich unter www.sophos.de/free-trials registrieren.

Sophos Produkte kaufen

Unter www.sophos.de/companyinfo/contacting finden Sie eine Sophos Niederlassung oder einen Sophos Partner in Ihrer Nähe. Sophos bietet außerdem Sonderpreise für Wohltätigkeitsorganisationen, Behörden und Bildungsinstitutionen an.

*Sophos PureMessage für Lotus Domino und SafeGuard MailGateway sind als separate Lizenzen erhältlich.

Unterstützte Plattformen

E-Mail Appliances

Alle Betriebssysteme: Das integrierte, optimierte Betriebssystem ermöglicht eine Installation an sämtlichen Netzwerk-Perimetern.

PureMessage für UNIX

- » Linux
- » FreeBSD
- » Solaris

PureMessage für Exchange

Konsole und Dienste

- » Windows® 2003 (32/64 Bit)
- » Windows Small Business Server 2003
- » Windows Server 2008 (32/64 Bit)/R2 (32/64 Bit)

Nur Konsole

- » Windows® XP/2003 und höher

Microsoft Exchange-Versionen

- » Exchange 2003/2007/2010

Microsoft SQL-Versionen

- » SQL 2005/2008
- » SQL Mirroring

Clustering

- » Exchange 2010: DAGs
- » Exchange 2007: SCC, CCR
- » Exchange 2003 R2: SCC, CCR
- » Exchange 2003 & ältere Versionen: SCC

PureMessage für Lotus Domino

- » Windows Server 2003 (32/64 Bit)
- » Windows Server 2008 (32/64 Bit)

E-Mail-Server**

- » Lotus Domino Server R7, R8.0x
- » und R8.5 (32/64 Bit)

**Lotus Domino Server R6 wird von PureMessage für Notes/Domino v3 unterstützt

