

PureMessage für UNIX

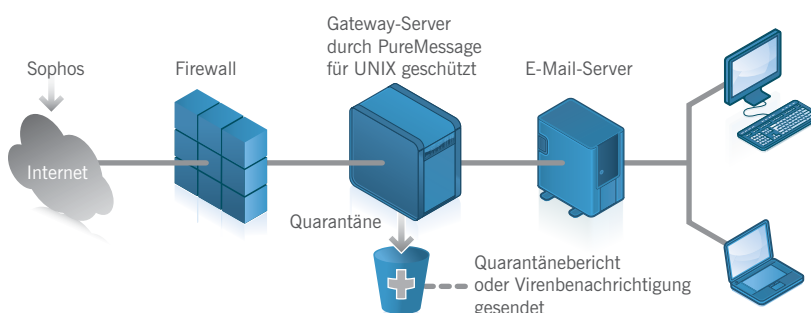
PureMessage für UNIX ist eine Komponente der Lösung „E-Mail Security and Data Protection“ und vereint hochgradig skalierbaren und konfigurierbaren Schutz vor Malware und Spam sowie Enforcement von Richtlinien am Gateway. Der Verwaltungsaufwand ist dabei minimal. Die flexiblen Installations- und Richtlinienoptionen passen sich an die unterschiedlichsten E-Mail-Verwaltungsszenarien, wie sie vor allem in Großunternehmen, Behörden, höheren Bildungseinrichtungen und Managed-Service-Providern zu finden sind, an.

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

- Sender Genotype® schützt mit Reputation Filtering und proaktiver Botnet-Erkennung vor bekannten und unbekanntem Spam-Quellen und beseitigt so bis zu 90% des Gesamt-Spamvolumens bereits vor einer Überprüfung.
- Genotype® Detection blockt Malware-Familien und Spamkampagnen vorzeitig ab.
- Abwehr vor unerwünschten und unbefugten Zugriffen auf Ihr Gateway ist durch Behavioral Genotype® Protection 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 von Sophos SXL vor neuesten Spamkampagnen.
- True File Type-Erkennung sorgt für verlässliche Kontrolle über Dateitypen in E-Mail-Anhängen.

Flexible Richtlinien-Funktionen für maximale Compliance und Data Leakage Prevention

- PureMessage für UNIX durchsucht E-Mails und Anhänge nach bestimmten Stichwörtern, Kreditkartennummern, Ausdrücken oder Mustern und kennzeichnet ein-/ausgehende E-Mails je nach ihrem Inhalt bzw. leitet sie entsprechend um. Es können auch E-Mails blockiert und Dateianhänge gelöscht oder umbenannt werden. Außerdem lassen sich auf Basis zahlreicher E-Mail-Eigenschaften Benachrichtigungen, Warnmeldungen und Routing zu Verschlüsselungslösungen anderer Hersteller einrichten.
- PureMessage für Unix lässt sich durch die gesonderte Zuweisung von Richtlinien an diverse Gruppen und Benutzer an die Anforderungen des Unternehmens anpassen und stellt so die Einhaltung der allgemeinen Nutzungsbedingungen sicher.
- Mit TLS-Verschlüsselung oder Einbindung in Drittanbieter-Verschlüsselungs-Services sorgt PureMessage für UNIX für den Schutz vertraulicher Daten.



Haupteigenschaften

- » Erkennung von über 99% aller Spam-Mails und Schutz vor E-Mail-Betrügereien wie Phishing-Attacken
- » Erkennung von Viren, Spyware, Trojanern und Würmern in ein- und ausgehenden E-Mails mit anschließender Desinfektion, Beseitigung oder Verwahrung (in Quarantäne)
- » Enttarnung neuer Spam-Kampagnen und Erkennung neuer Virenvarianten dank Genotype-Verfahren
- » Blockieren unbekannter Bedrohungen mit Behavioral Genotype® Protection zur präventiven Vermeidung von Schäden
- » Echtzeit-Spamschutz durch Einsatz von Sophos SXL
- » Das Sender Genotype-Verfahren spürt Botnets proaktiv auf und blockiert mit innovativer Reputation Filtering-Technologie bis zu 90% des Spamaufkommens bereits bei der Verbindungsherstellung.
- » Leistungsstarke Steuerung der Inhaltsüberprüfung zum Schutz vor Datenverlust
- » Einhaltung von Sicherheitsbestimmungen und gesetzlichen Vorschriften durch flexibles Richtlinienmanagement
- » Automatische Updates für neuesten Schutz aus den SophosLabs, dem weltweiten Netzwerk aus Spam- und Virenanalysecentern von Sophos
- » Enduser-Quarantäne-Überblick, Zulassen und Blockieren von Listen
- » Angepasstes E-Mail-Management und Senkung der Arbeitslast durch delegierte Administration
- » 24/7-Support an 365 Tagen im Jahr für Lizenzdauer und Support je nach Bedarf

Einfachere und individuell anpassbare Verwaltung und Kontrolle

- Die Management-Konsole von PureMessage für UNIX ermöglicht die zentrale Verwaltung über mehrere Server und bietet automatisiertes Quarantäne-Management, E-Mail-Nachverfolgung und Berichterstellung zum gesamten E-Mail-Verkehr sowie zur Bewegung bedrohlicher Daten.
- Rollenbasierte Administration ermöglicht dem Hauptadministrator das Zuweisen von Rechten und Privilegien auf Basis individueller Unternehmensanforderungen. Diese Rechte können sich auf Richtlinien, Quarantäne, Gruppen, andere Unternehmen und Administratoren von Abteilungen beziehen. Darüber hinaus dürfen einzelne Benutzer über ihre eigene Quarantäne verfügen.
- PureMessage für UNIX kann flexibel in zahlreichen Netzwerkstrukturen eingesetzt und einfach mit anderen Elementen der Netzwerk-Infrastruktur (z.B. Verzeichnisdienste und Verzeichnisüberwachung) kombiniert werden.

Professionelle Beratung 24x7x365

- Unser 24x7x365 Support, mit einer der besten Reputationen der Branche, und die SophosLabs™, unser weltweites Netzwerk aus Bedrohungsanalysecentern, reagieren rasch auf neue und unbekannte Bedrohungen.

Sprachen

- Deutsch, Englisch, Französisch, Italienisch, Japanisch, Spanisch, Schwedisch und Traditionelles Chinesisch
- Management-Konsole: Englisch

Sophos E-Mail Security and Data Protection enthält verwaltete E-Mail Security Appliances und Software-Schutz für UNIX-, Exchange- und Notes-Server. Die Lösung vereint Schutz vor Viren, Spam und Phishing-Angriffen mit intensivem Richtlinienmanagement und sorgt so für Sicherheit und Kontrolle Ihrer E-Mail-Inhalte.

Mehr zu PureMessage für UNIX oder anderen „E-Mail Security and Data Protection“-Lösungen erfahren Sie unter www.sophos.de/products.

Systemvoraussetzungen

Unterstützte Plattformen*

- » 32-Bit Red Hat Enterprise Linux auf x86/x86-64 (3 bis 5)
- » 64-Bit Red Hat Enterprise auf x86-64 (4 und 5)
- » 32-Bit SUSE Linux auf x86/x86-64 (Enterprise Server 8 bis 10, Professional 8 bis 9.2)
- » 32-Bit Debian auf x86/x86-64 (3.0, 3.1 und 4)
- » 32-Bit FreeBSD auf x86/x86-64 (5.4, 6.1, 6.2, 6.3)
- » Sun Solaris auf SPARC (8 bis 10)
- » Sun Solaris 10 auf x86/86-64

Gateway-/E-Mail-Plattformen

- » Sendmail (einschl. 8.13.6): 8.11.6 und höher
- » Postfix (einschl. 2.5.4): 2.0.x, 2.1 und höher
- » Sun Java™ System Messaging Server 5.2 und 6 auf Solaris SPARC
- » Andere Mail Transfer Agents über Relay-Konfiguration

Arbeitsspeicher

- » Mind. 1 GB
- » Besser 2 GB

Festplattenspeicher

- » 500 MB plus Quarantäne-Speicher

* Als natives Betriebssystem oder als ein virtuelles Betriebssystem mit VMware ESX (für Linux) oder Sun Solaris 10-Containern (für Solaris) ausgeführt.

