puremessage

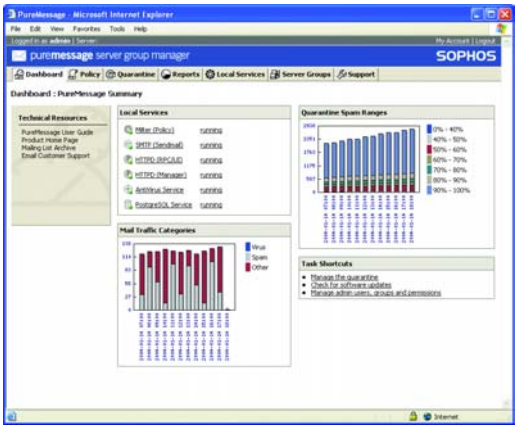
Schutz für E-Mail/Gateway

Sophos PureMessage schützt Unternehmen vor Spam, Viren und anderen E-Mail-basierten Sicherheitsbedrohungen. Dadurch werden Netzwerkausfallzeiten, Produktivitätsverluste und Störungen der E-Mail-Infrastruktur vermieden. Möglich macht das nicht nur der Einsatz führender Antispam- und Antiviren-Technologien zum Filtern der E-Mails, sondern auch das individuell konfigurierbare Policy-Management und der erstklassige 24/7-Support von Sophos.

So funktioniert's

PureMessage bildet eine Schnittstelle zum Mail-Gateway, um ein- und ausgehende E-Mails zu filtern und die E-Mail-Richtlinen des Unternehmens durchzusetzen.

- **Anti-Spam:** Schutz vor neusten Spam-Methoden wird durch führende Antispam-Technologie ermöglicht. Dazu gehören: PureView Content-Scanning, PureDetect E-Mail-Analyse und PureTrace Daten-Rückverfolgung.
- **Anti-Virus:** Preisgekrönte Antiviren-Technologie überprüft alle E-Mails am Gateway und schützt so das gesamte Unternehmen vor E-Mail-Viren, -Trojanern und -Würmern.
- **Policy-Management:** Aufgrund seines flexiblen Richtlinien-Rahmens setzt PureMessage Filter-Richtlinien für eingehende und ausgehende E-Mails durch und erfüllt so die Ansprüche eines Unternehmens hinsichtlich Sicherheit, Kommunikation und der Einhaltung von Richtlinien.
- **Zentrale Administration:** Eine webbasierte Administrationsoberfläche ermöglicht die optimale Steuerung des E-Mail-Filtering durch das flexible Management der Filter-Richtlinien, die Verwaltung von E-Mails in Quarantäne sowie Multiserver-Synchronisation und Reporting.
- **Steuerung durch den Enduser:** Zwei optionale Enduser-Oberflächen bieten zeitgesteuerte, E-Mail-basierte Einsicht in die Quarantäne oder webbasierten On-Demand-Zugriff auf die persönliche Quarantäne, Whitelists und Filter-Einstellungen.



PureMessage Dashboard: alle Infos auf einen Blick

Produktmerkmale und Vorteile

PureMessage ist die optimale Lösung für die speziellen Herausforderungen großer Unternehmen hinsichtlich E-Mail-Filtering und Spam-Management.

- Schützt alle E-Mail-Benutzer im Netzwerk vor aktuellen Spam- und Virenbedrohungen.
- Schützt globale Unternehmen vor Spam und Viren in mehrsprachigem E-Mail-Verkehr.
- Synchronisiert sich automatisch mit täglichen Updates aus den Antispam- und Antivirus-Laboren von Sophos.
- Erkennt bis zu 98% aller Spam-E-Mails und schützt vor Scams, einschließlich sog. "Phishing Attacks".
- Stoppt schädlichen Code am Gateway, bevor er sich im Unternehmensnetzwerk ausbreiten kann.
- Schützt vor Kosten durch Verstöße gegen Vertraulichkeitsvorschriften sowie durch Haftungsansprüche und Rufschädigung.
- Richtlinien entsprechend den Unternehmensvorgaben können erstellt, überwacht und durchgesetzt werden.
- Durchsicht der Quarantäne nach legitimen E-Mails durch den Enduser sowohl durch zeitgesteuerte E-Mail-Digests als auch optional via Web-Zugriff.
- Ermöglicht Unternehmens- und Enduser-Einstellungen mit sowohl globalen als auch Enduser-spezifischen Whitelists und Blacklists.
- Integrierbar in für Großunternehmen typische E-Mail-Systeme, die auf Sendmail und Postfix MTAs basieren.
- Filtert Millionen E-Mails pro Tag mit einer skalierbaren Architektur für E-Mail-Verarbeitung und -Quarantäne.
- 24-Stunden-Support an 365 Tagen im Jahr.

SOPHOS

Technische Daten

puremessage

PureMessage Engine

Alle E-Mails werden am E-Mail-Gateway abgefangen, um konforme Richtlinien für das E-Mail-Filtering von ein- und ausgehenden E-Mails anzuwenden, die auf einem RFC 3028-, Sieve-basierten Richtlinien-Rahmen und einem oder mehreren installierten PureMessage-Modulen basieren.

PureMessage Manager

Die Administrationsoberfläche zum Verwalten der PureMessage-Server für:

- Konfiguration der E-Mail-Filterrichtlinien und Verwaltung der Softwarekomponenten
- Automatisches Quarantäne-Management
- Automatische Updates
- Delegierte Administration
- Multiserver-Synchronisation und -Reporting.

Verschiedene Enduser-Oberflächen

Optional stehen E-Mail-basierte Quarantäne-Digests und webbasierte Enduser-Oberflächen zur Verfügung, über die Anwender ihre persönliche Quarantäne, Whitelists, Blacklists und Filtereinstellungen verwalten können.

PureMessage AS Antispam-Modul (optional)

Eigens entwickelter Spamschutz für höchste Präzision bei der Identifikation von Spam-Mails basierend auf branchenführender Forschung und Technologie:

- PureView™ – konvertiert E-Mails zur Analyse durch spezielle Spam-Sensoren in verschiedene Formate und schützt so vor Versteck-Taktiken bzw. verschleiertem Spam.
- PureDetect™ – Überprüfung von Inhalt und Struktur des E-Mail-Verkehrs auf Tausende Spam-Indikatoren. Zu den angewendeten Methoden zählen genotypische Kampagnen-Analyse, Erkennung von Verschleierungstaktiken, Inhalts- und Struktur-Heuristiken, Erkennung von beleidigenden Inhalten, anpassungsfähige Filter und selbstlernende Komponenten.
- PureTrace™ – Prüfung der Ursprungs- und Zielorte von Spammer-Aktivitäten. Die angewendeten Methoden sind u.a. Rückverfolgung von Spammer-Daten, Filtern von Ziel-URLs sowie Tests, wie Sender Permitted From (SPF), DNSBL.

PureMessage AV Antiviren-Modul (optional)

Virenschutz am Gateway für eine einfache Verteilung schützt Unternehmen auch, wenn einzelne Arbeitsplatzrechner nicht up-to-date sind.

- Mittels Dateifilterungstechnologie werden bekannte und neue E-Mail-Würmer abgeblockt.
- Ausführbarer Inhalt und Dateien in E-Mails werden automatisch auf schädlichen Code überprüft.

PureMessage EP Extended Policy (optional)

Extended Policies -Tests erweitern die Funktionen von PureMessage, um Stichwort-, Inhalt-, Attachment- und Header-basierte Tests und Maßnahmen durchzusetzen.

Unterstützte Plattformen

Linux auf x86 (Red Hat 6.2 bis 9 und Enterprise 2.1 bis 3 oder kompatible Distributionen).
Sun Solaris auf Sparc (2.6 oder höher).
HP-UX auf PA_RISC1.1 (11.0 oder höher).
FreeBSD auf x86 (4.5 bis 4.8).
AIX auf RISC (4.3.3 oder höher).

Gateway-/E-Mail-Plattformen

Enthält Sendmail: Unterstützung von Version 8.11.6 oder höher.
Enthält Postfix: Unterstützung von Version 2.0.x.
Andere E-Mail-Plattformen: Unterstützung über Relay-Konfiguration.

Systemvoraussetzungen

Speicher: 1 GB Minimum.
Festplattenspeicher: 150 MB plus Speicher für die Quarantäne.

Ein Anforderungsformular für Testsoftware finden Sie unter http://www.sophos.de/products

fs/040209

Boston, USA • Mainz, Deutschland • Mailand, Italien • Oxford, UK • Paris, Frankreich
Singapur • Sydney, Australien • Vancouver, Kanada • Yokohama, Japan

SOPHOS
www.sophos.de

© Sophos. All registered trademarks and copyrights are understood and recognised by Sophos.