

PureMessage for UNIX

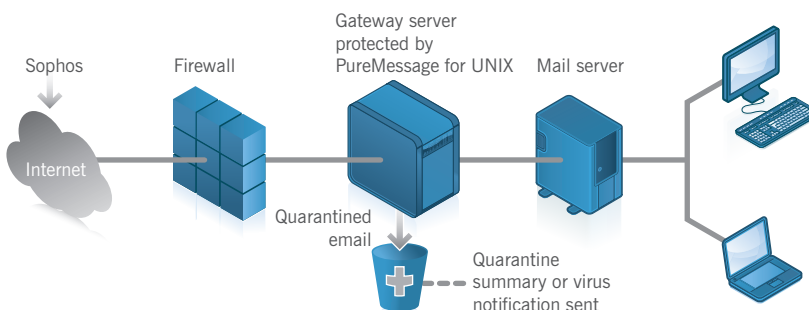
PureMessage for UNIX, part of Email Security and Control, integrates highly scalable, highly configurable anti-malware, anti-spam and policy enforcement at the gateway with minimal administrative burden. Its flexible deployment and policy capabilities adapt to a wide range of email management needs, particularly those of large organizations, government and higher education establishments, and managed service providers.

Proactive protection against spam, malware, phishing and other email-borne threats

- Sender Genotype protects against known and unknown spam sources, effectively eliminating up to 90 percent of spam before scanning.
- Genotype detection technology proactively blocks families of malware and spam campaigns.
- Behavioral Genotype® Protection provides unique built-in intrusion prevention technology for the gateway. It detects new threats before code even begins to execute, proactively protecting against zero-day malware.
- A range of anti-spam techniques including obfuscation detection, URL tracking, heuristics, and content fingerprinting eliminates more than 99 percent of spam.
- A comprehensive real-time system protects against the latest spam campaigns with Sophos SXL technology.

Simplified, customizable administration and control

- PureMessage for UNIX scans email for specific keywords, phrases, or patterns, and re-routes or tags inbound/outbound messages based on content. It can also block messages, remove or rename attachments, and notify or warn a user, based on a wide range of message attributes.
- Administrators can assign different policy rules to different groups and users, ensuring that PureMessage fits the organization’s needs and enforces its acceptable use policy.
- PureMessage for UNIX’s management console enables centralized administration across multiple servers, providing automated quarantine management, message tracing and reporting on email traffic and threat activity.
- The management console allows the master administrator to assign rights and privileges relating to policy, quarantine, and reporting to sub-administrators of departments, groups, or even separate companies, based on organizational need. In addition, individual users are able to manage their own personal quarantines.



Key benefits

- » Detects over 99 percent of spam and protects against email scams, including phishing attacks
- » Detects, disinfects, deletes or quarantines viruses, spyware, Trojans, and worms in incoming and outgoing email
- » Employs Genotype technology to catch evolving spam campaigns and new virus variants
- » Blocks unknown threats before they cause damage, with Behavioral Genotype technology
- » Provides real-time anti-spam protection with Sophos SXL technology
- » Sender Genotype advanced connection control provides proactive botnet detection and reputation filtering, blocking up to 90 percent of spam at the connection level.
- » Provides powerful content scanning controls to protect against confidential information leakage
- » Incorporates a flexible policy environment to support complex security or compliance requirements
- » Updates automatically with the latest protection from SophosLabs, a global network of threat analysis centers
- » Provides end-user quarantine review, allow lists, and block lists
- » Enables customized email management and reduces workload, through delegated administration
- » Includes 24x7x365 support for the duration of the license and Sophos can be contacted for one-to-one

Faster, better, proactive protection using innovative technologies

- Genotype® malware and spam detection technology proactively blocks families of malware and spam campaigns even before specific email samples have been analyzed, providing zero-day protection against emerging threats.
- A range of technologies, including Dynamic Code Analysis™, pattern matching, emulation and heuristics, automatically check for malicious code within emails.
- Reputation filtering blocks email from known bad senders at the connection level, effectively eliminating up to 80 percent of spam before scanning is required.
- Sophos's unique, pre-runtime HIPS technology uses Behavioral Genotype Protection to block suspicious code before it executes, while constantly validating code against an extensive library of legitimate applications, minimizing the risk of false positives.
- Multilingual scanning technology cleans up and deconstructs complex, disguised message content and analyzes URLs contained within emails.
- PureMessage for UNIX automatically receives the latest anti-virus updates and new spam rules created by expert analysts in SophosLabs every five minutes.

Industry-leading expertise 24/7

- Our 24/7 customer support operation is highly acclaimed, while SophosLabs™, our global network of threat analysis centers, provides a rapid response to emerging and evolving threats.

Languages available

- English, French, German, Italian, Japanese, Spanish, Swedish and Traditional Chinese
- Management console: English

Sophos Email Security and Control includes managed email security appliances and software protection for Exchange, UNIX and Notes servers, providing unique integration of anti-virus, anti-spam, anti-phishing and policy enforcement capabilities to secure and control email content.

To find out more about PureMessage for UNIX or any of our Email Security and Control products, visit www.sophos.com/products

ds/080319

Platforms supported

- » 32-bit Red Hat Enterprise Linux on x86/x86-64 (3 to 5)
- » 64-bit Red Hat Enterprise Linux on x86-64 (4 and 5)
- » 32-bit SUSE Linux on x86/x86-64 (Enterprise Server 8 to 10, Professional 8 to 9.2)
- » 32-bit Debian on x86/x86-64 (3.0, 3.1, 4)
- » 32-bit FreeBSD on x86/x86-64 (5.3, 5.4, 6.1, 6.2)
- » Sun Solaris on SPARC (8 to 10)
- » Sun Solaris 10 on x86/x86-64

Gateway/email platforms

- » Sendmail (8.13.6 included): 8.11.6 or higher
- » Postfix (2.3.4 included): 2.0.x and 2.1 or higher
- » Supports Sun Java™ System Messaging Server 5.2 and 6 on Solaris SPARC
- » Other Mail Transfer Agents: supported via relay configuration

Memory

- » Minimum: 1 GB
- » Recommended: 2 GB

Disk space

- » 200 MB plus quarantine space

