

Sophos PureMessage is a trusted and proven solution that protects organisations against viruses, spam and other email-borne security threats. It combines industry-leading anti-virus and anti-spam technologies with flexible policy management and Sophos's first-class technical support. PureMessage provides comprehensive mail filtering that enables organisations to protect against network downtime, productivity loss and threats to their email infrastructure.

## How it works

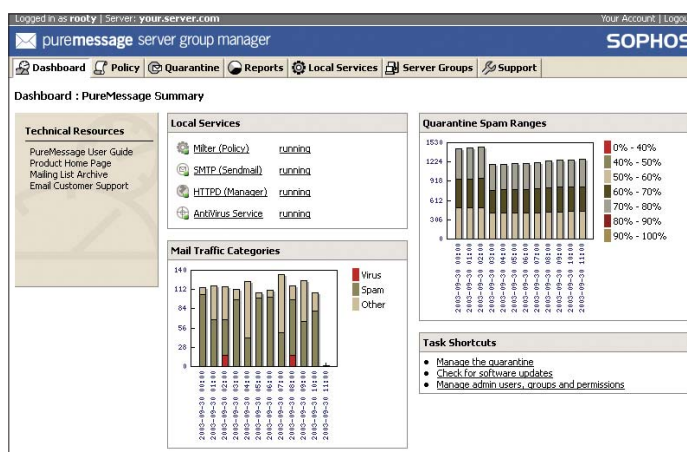
PureMessage filters messages at the gateway before they enter the organisation. It provides consolidated single-pass protection from viruses and spam, enabling enforcement of the organisation's message handling policy.

- **Anti-virus:** PureMessage checks all email messages at the server in real time, protecting against mass-mailing Trojan horses, worms and viruses. Malicious code is stopped at the gateway before it can proliferate within a corporate network.
- **Anti-spam:** PureMessage applies a combination of spam and legitimate message identification tests that are updated daily, ensuring protection from the latest spamming techniques.
- **Administrative tools:** PureMessage features an easy-to-use web-based interface to manage configuration and administration tasks. These include creating and managing policies, monitoring services, performing automatic updates, managing quarantined messages, and monitoring and reporting across multiple servers.
- **Policy management:** PureMessage's powerful RFC 3028-compliant policy framework enables organisation-specific message handling policies to be defined, controlled and enforced.

## Features and benefits

- Protects all email users on the network by detecting viruses at the gateway.
- Simplifies deployment by scanning for viruses from one central location.
- Scans all outbound email for viruses automatically, keeping the organisation up to date and protected, even when individual workstations are not.
- Protects against new, unknown email-aware worms entering the network, using sophisticated threat reduction technology.
- Defends against the latest spam and viruses with automatic, daily updates.
- Removes up to 98% of spam at the gateway using a balanced combination of spam and legitimate message identification tests.
- Identifies new spamming techniques, preventing spammers from innovating against detection techniques.
- Includes customisable user preferences and privileges such as opt-in/opt-out, thresholds, digests and spam handling methods.
- Uses quarantine digests to enable quick retrieval of legitimate messages, eliminating the impact of false positives without the need for administrative intervention or additional tools.
- Allows message handling policies to be easily defined, configured, monitored and enforced.
- Protects against the costs of confidentiality breaches, legal liability and damage to the organisation's reputation.
- Enables organisations to establish, monitor and enforce appropriate use, receipt and regulatory compliance policies and procedures, at both the end-user and infrastructure levels.

|   |  |
|---|--|
| <b>Function</b>                         | <p>Message filtering at the email gateway on Unix/Linux platforms:</p> <ul style="list-style-type: none"> <li>• Single-pass virus scanning of inbound and outbound messages</li> <li>• Spam identification and quarantine management</li> <li>• Email policy control, inbound and outbound.</li> </ul>   |
| <b>Mode of operation</b>                | <p>PureMessage Anti-Spam tests for spam probability and uses policy rules to route messages (e.g. deliver, quarantine, archive).</p> <p>PureMessage Anti-Virus intercepts and scans email attachments as they are sent or received. Virus-free messages are passed to the mail server. Infected attachments are disinfected, deleted or quarantined.</p> |
| <b>Policy enforcement</b>               | <p>Threat reduction technology to block existing and new, unknown email-aware worms:</p> <ul style="list-style-type: none"> <li>• Automatic checking of executable content and files in email for malicious code</li> <li>• Applies appropriate message handling policy to ensure fast and reliable protection.</li> </ul>                               |
| <b>Use of the Sophos virus engine</b>   | Via SAV Interface.   |
| <b>SMTP gateway platforms supported</b> | <p>Linux on x86 (RedHat 6.2 to 8.x, or Debian 2.1 or higher)</p> <p>Sun Solaris on Sparc (2.6 or higher)</p> <p>HP-UX on PA_RISC1.1 (11.0 or higher)</p> <p>FreeBSD on x86 (4.5 to 4.8)</p> <p>AIX on RISC (4.3.3 or higher).</p>  |
| <b>System requirements</b>              | <p>Memory: 1GB minimum.</p> <p>Disk space: 150MB plus quarantine space.</p>  |
| <b>Network requirements</b>             | 100Mbit network or better (if using PureMessage via network).  |
| <b>Updating</b>                         | <p>PureMessage polls a dedicated server:</p> <ul style="list-style-type: none"> <li>• Configurable frequency</li> <li>• Default three times a day.</li> </ul>  |



*PureMessage's Dashboard showing summary information*

An application form for evaluation software can be obtained from <http://www.sophos.com/products>

fs/031003