

Sophos PureMessage is a comprehensive, flexible email management solution which allows organisations to take greater control of their email traffic. It provides seamless and immediate protection from spam and viruses and allows policies to be easily built and managed using a variety of administrative tools. PureMessage enables organisations to protect against network downtime, productivity loss and other threats to their email infrastructure and usage.

How it works

Email entering a company's system via the internet is received by PureMessage via its integrated Sendmail mail transfer agent. The email is then automatically filtered, providing the following functionality:

- **Anti-spam:** PureMessage performs a series of tests to determine the probability that an individual message is spam. Based on this probability, an associated policy determines how to route the message (e.g. deliver, quarantine, archive).
- **Anti-virus:** PureMessage uses the Sophos virus engine to detect email-borne viruses, Trojan horses and worms, providing total protection for an organisation's network.
- **Administrative tools:** PureMessage features a number of easy-to-use web-based interfaces to manage administrative tasks such as creating and managing policies, monitoring services, performing automatic updates and managing quarantined messages. They also allow configuration, monitoring and reporting across multiple servers.
- **Policy enforcement:** PureMessage ensures compliance with internal policies by performing various actions such as searching for specific keywords, adding message footers, converting mail formats and auditing mail for integrity.

Technical details

OS supported: Linux on x86 (RedHat 6.0 or higher, or compatible distribution); Sun Solaris on SPARC (2.6 or higher); FreeBSD on x86 (4.1 or higher); HP-UX on PA_RISC1.1 (11.0 or higher); AIX on RISC (4.3.3 or higher).

Memory requirements: 512MB minimum, 1GB recommended.

Network requirements: 100Mbit network or better (if using PureMessage via network.)

Features and benefits

- Identifies 98% of spam using over 750 tests to calculate the probability that a message is spam, resulting in inboxes free from unsolicited bulk emails.
- Allows organisations to define their spam identification and handling policies uniquely (e.g. deliver, quarantine, archive).
- Guards networks against malicious code entering and spreading via email, by providing scanning, cleaning and quarantine management for viruses, worms and malicious code.
- Ensures up-to-the-minute virus protection via automatic updates.
- Provides easy management, implementation and enforcement of inbound and outbound mail policies – including anti-spam, anti-virus, acceptable use and acceptable receipt – to maintain quality of email communication.
- Analyses message traffic over time to provide perimeter security against Denial of Service (DoS) attacks and Directory Harvest Attacks (DHA).
- Increases productivity by ensuring organisations are using email efficiently.
- Provides a flexible application programming interface (API) for the development of proprietary, custom-filtering solutions.
- Extends to meet the requirements of growing organisations.
- Protects corporate assets from virus attacks and prevents intellectual property from leaking out via email.
- Minimises administrative load and effectively eliminates false positives by allowing users access to quarantined messages through their inboxes.