

Business challenge

The role of the gateway in enterprise security architecture is becoming increasingly critical with the growth and rapid evolution of email-borne threats. It is the ideal location for the control and enforcement of policy for email traffic, and efficient management can ease the downstream load on the network. The need to demonstrate regulatory compliance also requires the detailed implementation of enterprise email policy management to be well understood and to provide evidence of control.

The Sophos solution

Sophos PureMessage® for UNIX offers an extended policy module that integrates a broad range of threat detection capabilities into a single policy framework, allowing threats to be stopped at the gateway, and minimising their impact on the enterprise network. It enables comprehensive message management, ensuring that both inbound and outbound messages comply with corporate policies and meet the needs of regulatory compliance.

PureMessage allows administrators to manage the transmission of private or confidential information, maintain records of communication, and monitor all email traffic. All policies for spam, virus, and content security are designed in a single visual environment and policies for inbound and outbound mail can be deployed on a single machine. PureMessage also provides the granular control needed to handle complex messaging scenarios, such as messages with multiple recipients.

The PureMessage policy manager allows all policy tests and actions to be defined in one place, easing the management of complex configurations. Its interactive policy tree aids understanding of the combined effects of security, content filtering, and message routing policies, and provides evidence of controls in both visual and script-based views.

PureMessage includes over 30 tests and actions that can be used to construct custom message handling policies, allowing organisations to look for specific keywords and patterns, scan for common attachment names, and route messages through secure transmission systems.

Extensible lists can be used to monitor specific sender-recipient paths, store messages for later archiving, and log specific communication streams. By integrating with existing processes for logging, storing, and reviewing specific communication between internal and external parties, PureMessage can play a critical role in enforcing an organisation's security and compliance policies.



Key benefits

- » Integrates a range of threat detection capabilities into a single policy framework.
- » Incorporates a rich policy environment to support complex security or regulatory compliance requirements.
- » Logs messages based on specific policy rule "hits", enabling the generation of monitoring and compliance reports.
- » Manages privacy and confidential information by looking for keywords, scanning attachments, and modifying headers to route messages through secure systems.
- » Provides extensible lists that allow complex monitoring scenarios to be broken down into easily maintainable elements.
- » Includes a graphical user interface to simplify the task of defining message-handling policies.
- » Allows inappropriate or offensive messages to be managed separately from spam in a grey area.
- » Includes unlimited 24-hour telephone, email, and online support, 365 days a year.

PureMessage policy management

Policy tests and actions

Group-based policy

PureMessage allows you to configure different policies for specific sub-groups within your organisation. This gives you the power to automate policy enforcement across your organisation and take into account the unique needs of different users and groups, e.g:

- Opting specific users out of spam quarantining
- Filtering mail differently by type of recipient (e.g. teachers and students)
- Relaxing global restrictions on attachment types/sizes for heavy users of graphics files.

Content scanning

PureMessage provides a range of controls for scanning message subjects, bodies and attachment content* for specific keywords, phrases or patterns. This helps you build powerful content security rules that map to corporate communication policies, regulatory requirements, or intellectual property practices, e.g:

- Monitoring outbound mail for specific attachment types, such as sensitive documents
- Identifying all the mail traffic associated with a specific project or business deal
- Scanning messages/attachments for offensive content or intellectual property violations
- Detecting disallowed file types, regardless of extension or content type headers.

Message routing

PureMessage gives you complete control over the routing of inbound or outbound mail, allowing you to re-route messages to individuals or third-party systems. This feature complements your content security rules with specific automated actions that map to your internal policies, e.g:

- Logging specific messages and forwarding them to a reviewer (e.g. compliance officer)
- Archiving messages to a specific disk location for pickup by your archiving system
- Forwarding messages through secure delivery (e.g. encryption) systems.

Policy reporting

PureMessage allows you to tag messages when triggered by custom policies, providing flexible reporting. Out-of-the-box reports allow you to monitor custom rule hits, e.g:

- Summarising all email traffic related to a specific business deal or partnership
- Ongoing monitoring of corporate policy violations.

* Attachment content scanning is available as a plug-in to PureMessage. Please contact your account manager for details.

Key features

- » Includes default policies that can be tailored to match specific business processes.
- » Scans message logs for unusual traffic patterns, notifying and automatically responding to potential denial of service or directory harvest attacks.
- » Provides a broad range of controls for testing and handling suspicious attachments even before they enter users' mailboxes.
- » Enables tests for attachment name, size and type to be combined to scan for specific confidential documents.
- » Includes both basic keyword tests and more advanced pattern/phrase testing capabilities.
- » Allows messages to be routed through third-party encryption or other systems, based on policy decisions.
- » Archives messages automatically to the quarantine or the file system in a standard format.

To evaluate PureMessage, visit www.sophos.com/products

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centres, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2005. Sophos Plc. All rights reserved. All trademarks are the property of their respective owners.

ds/051122

SOPHOS
WWW.SOPHOS.COM