

Functionality comparison

	PureMessage for UNIX	Email Appliances	PureMessage for Microsoft Exchange
Scans inbound, outbound and internal mail	Yes	Yes, but most organizations find it easier to handle internal mail using workgroup-level routing	Yes, email policy can be defined by email direction
Applies different rights for different types of administrators	Yes, basically any combination of rights can be granted	Yes, preconfigured helpdesk and system administrator options	No
Scans message stores at groupware level	No	No	Yes, on access, proactive and background scanning
Scans compressed and password protected files	Yes, they are analyzed for viruses and true file type	Yes, they are analyzed for viruses and true file type	Yes, they are analyzed for viruses and true file type
Scans for viruses in emails and attachments	Yes	Yes	Yes
Content scanner (e.g. keywords) can filter within:	Subject, sender, recipient, message headers or message body and attachment content (using the Attachment Scanning module)	Subject and message body and attachments (common Office files, e.g. PDF, DOC, XLS, PPT and XML)	Subject, message body and attachments (common Office files, e.g. PDF, DOC, XLS, PPT and XML)
Assigns rules for content filtering	An unlimited number of content rules can be created	Up to 80 independent rules can be created, 40 for inbound and 40 for outbound.	Six content filtering policy slots in total. Two file type and two phrase matching policies are available for each email direction, i.e. inbound, outbound and internal email. User/group exceptions can be set for each policy
Scans content of emails	Yes	Yes	Yes
Default policies available	Yes, although the flexibility of the policy to handle a wide variety of scenarios is one of the main advantages of PureMessage	Yes, there is a default Sophos recommended policy with the ability to specify virus, spam and content policies manually if required	Yes, default SophosLabs security policy and potentially malicious file types and offensive language policies
Group-based policy	Yes, including manually created groups as well as Active Directory, OpenLDAP and Sun Directory Service integration/synchronization	Yes, including manually created groups as well as Active Directory synchronization and support for other LDAP directory servers.	Yes, including manually created groups as well as Active Directory integration/synchronization
Granular policy controls - can be set for departments, regions or individuals	Yes, including group level options configurable by group administrators	Yes	Yes
Dashboard	Shows service status (e.g. militer, IP blocker, MTA, etc.), and provides links to most used administrative features including quarantine management and user configuration	At-a-glance, real-time view of daily traffic statistics, system performance, throughput, quarantine usage, latest threats blocked, hardware health and more	Health status for all servers (scanning/updates) Mail flow monitoring Quarantine database monitoring Top malware threats Activity monitor – real time view of email traffic
Allow and block lists	Yes, configurable globally, per group/domain and per user by the administrator. Configurable by group administrators via the Groups UI and by end-users through the end-user web interface	Yes, configurable globally by the administrator. End-user allow- and block- lists are configurable by end-users through the end-user web interface	Yes, configurable globally by the administrator

Functionality comparison

	PureMessage for UNIX	Email Appliances	PureMessage for Microsoft Exchange
Filters attachments/ removes suspicious attachments	Yes, can remove suspicious files based on true file type (can identify true file regardless of extension or header)	Yes, can remove suspicious files based on true file type (can identify true file regardless of extension or header)	Yes, can remove suspicious files based on true file type (can identify true file regardless of extension or header)
Message headers can be added or replaced	Yes	Yes	All messages are given x-headers that cannot be modified or replaced
Ability to handle inappropriate/offensive messages separately from other quarantined messages	Any class of messages can be handled separately from any other, and any class of message can be included or excluded from end user quarantines	Yes, only spam or suspected spam is viewable in the end-user quarantine. If the offensive content rule is enabled, offensive messages will only be visible to the administrator	Yes, only spam or suspected spam can be viewed in the end-user quarantine. Messages that infringe content policy are only visible to the administrator
Reputation filtering (IP blocking)	Can be deployed as a part of the weighted spam check, at the MTA level or at the policy level (before the weighted spam check)	Can be deployed at the MTA level or at the policy level (before the weighted spam check)	Deployed as part of the weighted spam check
Ability to add banners to messages	Yes, can be added at the top or bottom of messages in HTML or plain text	Yes, can be added at the top or bottom of messages in HTML or plain text.	Yes, can be added at the top or bottom of messages in HTML or plain text
Actions that can be taken on messages	Reject, Discard, Tag, Add header, Quarantine, Deliver, Quarantine and deliver, Forward, CC, BCC, Drop attachments and deliver	Reject, Discard, Tag, Add header, Quarantine, Deliver, Quarantine and deliver, Forward, Redirect, Drop attachments and deliver , Re-route to, Copy to	Discard, Quarantine, Deliver, Redirect, BCC, Drop attachments and deliver, Quarantine and deliver
Record communications	Yes, archives messages and message logs. All delegated (group) activity is logged.	Yes, archives quarantined messages and message logs.	Yes, for message logs only
Ability to block messages sent to too many recipients	Yes, there is a policy test for number of recipients > N. The Postfix MTA can throttle connections using Anvil or reject based on number of recipients	The system has thresholds that invoke connection throttling and connection dropping at Sophos-managed thresholds. This helps automatically protect against DHA attacks	Yes, administrator configurable
Different actions for different recipients (i.e. quarantine for some, tag and pass for others - dependant on user group)	Yes	Yes	Yes
Global quarantine management	Yes	Yes	Yes
End-user quarantine access	Yes, in two ways: end-user web interface (with Active directory and LDAP integration), and email based quarantine digest. Methods used are configurable by the administrator	Yes, in two ways: end-user web interface (with Active directory and LDAP integration), and email based quarantine digest. Methods used are configurable by the administrator	Yes, end-user web interface with Active Directory integration providing single sign on
Message routing to third parties	Yes, with Policy Router module	Yes	No
Evidence of internal controls	Logs and quarantine can be archived at administrator's discretion. All delegated (group) activity is logged. Records anti-virus upgrades.	Archives logs, records anti-virus upgrades, archives quarantine	Log and quarantine can be archived at administrator's discretion
Changes made by Sophos support are logged	No	Yes, when remote assistance is enabled	No
Policy-based reporting	Yes, by tagging messages based on policy considerations custom reports for these concerns can be generated	Yes, reports based on policy hits/trends are supported	Yes, reports based on policy hits/trends are supported

Functionality comparison

	PureMessage for UNIX	Email Appliances	PureMessage for Microsoft Exchange
Custom logging	Yes, can log messages based on policy rules hit (i.e. for keyword infractions)	No	No
Custom reports	Yes, all data is stored in the Postgres/SQL database and reports can be generated from this. This feature is not supported though	No	No
Prevention against Denial of Service (DoS) attacks	Yes, provides multiple forms of protection, including perimeter protection based on configurable parameters (number of recipients, number of messages/sender, number of messages/relay, etc) as well as connection throttling in real time via Anvil on Postfix	Yes, measures message velocity from a given host, will block receipt of messages from the offending sender. Also has thresholds resulting in connection throttling/dropping based on number of concurrent connections, number of recipients/connection and number of invalid recipients/connection	No, but this functionality is built into IIS SMTP service (which PureMessage for Microsoft Exchange utilizes)
Prevents against Directory Harvest Attacks	Yes, many methods for handling this are available, including connection throttling, recipient validation	Yes, through connection throttling. If a single IP sends a message to multiple addresses and the first five aren't valid addresses it starts to throttle the connections (process them more slowly), after 20 invalid addresses it terminates the connection	Yes, through recipient validation and the ability to configure the response provided for invalid recipients
Archiving	Messages can be archived to the quarantine or the file system in a standard format. Customer can search for messages quarantined for any policy consideration (i.e. offensive content, compliance infractions etc.)	Archives quarantined messages and message logs. Messages archived contain meta-data, including reason for quarantine, which enables sorting and filtering. Messages can also be routed to third-party archiving systems.	No, although everything that's quarantined is archived to disk
Encryption	Integrates seamlessly with third-party servers using the Policy Router Module	Includes on-board TLS encryption. Can also integrate with third-party systems for stronger global or policy-based encryption.	Can integrate with third-party server
Clustering support	Yes	2-unit Active/passive failover	Yes

PureMessage is also provides complete malware protection for Lotus Notes/Domino. For more information about Email Security and Control, visit www.sophos.com/email

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

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

SOPHOS
secured.