

Functionality comparison

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Lotus Domino
Scans inbound, outbound and internal mail	Yes, but most organizations find it easier to handle internal mail using workgroup-level routing	Yes, but most organizations find it easier to handle internal mail using workgroup-level routing	Yes, email policy can be defined by email direction	Yes, email policy can be defined by email direction
Applies different rights for different types of administrators	Yes, preconfigured helpdesk and system administrator options	Yes, basically any combination of rights can be granted	No	Yes, can control administrator access to various databases
Scans message stores at groupware level	No	No	Yes, on access, proactive and background scanning	Yes, on access, proactive and background scanning
Scans compressed files and archives	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	Yes, they are analyzed for viruses and true file type
Scans for viruses in emails and attachments	Yes	Yes	Yes	Yes
Content scanner (e.g. keywords) and can filter within:	Subject and message body and attachments (common Office files, e.g. PDF, DOC, XLS, PPT and XML)	Subject and message body and attachments (common Office files, e.g. PDF, DOC, XLS, PPT and XML and specific tests for credit card numbers)	Subject, 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	Up to 80 independent rules can be created, 40 for inbound and 40 for outbound	An unlimited number of content rules can be created	Four 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	An unlimited number of content rules can be created
Scans content of emails	Yes	Yes	Yes	Yes
Default policies available	Yes, there is a default Sophos recommended policy with the ability to specify virus, spam and content policies manually if required	Yes, although the flexibility of the policy to handle a wide variety of scenarios is one of the main advantages of PureMessage	Yes, default SophosLabs security policy and potentially malicious file types and offensive language policies	Yes. A number of default policies are provided that are easily enabled
Group-based policy	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, OpenLDAP and Sun Directory Service integration/synchronization	Yes, including manually created groups as well as Active Directory integration/synchronization	Yes, including manually created groups as well as groups from the Lotus Name and Address Book

Functionality comparison

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Lotus Domino
Granular policy controls – can be set for departments, regions or individuals	Yes	Yes, including group level options configurable by group administrators	Yes	Yes
Dashboard	At-a-glance, real-time view of daily traffic statistics, system performance, throughput, quarantine usage, latest threats blocked, hardware health and more	Shows service status (e.g. milter, IP blocker, MTA, etc.), and provides links to most used administrative features including quarantine management and user configuration	Health status for all servers (scanning/updates) Mail flow monitoring Quarantine database monitoring Top malware threats Activity monitor – real time view of email traffic	Dashboard-type statistics are available in the Log & Statistics section of the interface
Allow and block lists	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, 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	Yes, configurable globally by the administrator. End-user allow and block lists are configurable by end-users through the Portal
Granular true file type detection	Yes, can filter and remove suspicious files based on true file type and identify true file types regardless of extension or header	Yes, can filter and remove suspicious files based on true file type and identify true file types regardless of extension or header	Yes, can filter and remove suspicious files based on true file type and identify true file types regardless of extension or header	Yes, can filter and remove suspicious files based on true file type and identify true file types 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	Headers can be added by administrators
Ability to handle inappropriate/offensive messages separately from other quarantined messages	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	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 can be viewed in the end-user quarantine. Messages that infringe content policy are only visible to the administrator	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
Reputation filtering (IP blocking)	Can be deployed at the MTA level or at the policy level (before the weighted spam check)	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)	Deployed as part of 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	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, Redirect, Drop attachments and deliver , Re-route to, Copy to	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	Discard, Quarantine, Deliver, Quarantine and deliver, Drop attachments and deliver
Record communications	Yes, archives quarantined messages and message logs	Yes, archives messages and message logs. All delegated (group) activity is logged	Yes, for message logs only	Yes, archives quarantined messages and message logs

Functionality comparison

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Lotus Domino
Ability to block messages sent to too many recipients	The system has thresholds that invoke connection throttling and connection dropping at Sophos-managed thresholds. This helps automatically protect against DHA attacks	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	Yes, administrator configurable	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	Yes
Global quarantine management	Yes	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	Yes, in two ways: end-user Portal (with Notes integration) and email-based quarantine digest. Methods used are configurable by the administrator
Message routing to third parties	Yes	Yes	No	No
Evidence of internal controls	Archives logs, records anti-virus upgrades, archives quarantine	Logs and quarantine can be archived at administrator's discretion. All delegated (group) activity is logged. Records anti-virus upgrades	Log and quarantine can be archived at administrator's discretion	Log and quarantine can be archived at administrator's discretion
Changes made by Sophos support are logged	Yes, when remote assistance is enabled	No	No	No
Policy-based reporting	Yes, reports based on policy hits/trends are supported	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
Custom logging	No	Yes, can log messages based on policy rules hit (i.e. for keyword infractions)	No	Logging levels and contents can be customized
Custom reports	No	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

Functionality comparison

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Lotus Domino
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, 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	No, but this functionality is built into IIS SMTP service (which PureMessage for Microsoft Exchange utilizes)	Yes, can monitor and take action on the number of messages from a sender in a given time period
Prevents against Directory Harvest Attacks	Yes, many methods for handling this are available, including connection throttling and recipient validation	Yes, many methods for handling this are available, including connection throttling, recipient validation	Yes, through recipient validation and the ability to configure the response provided for invalid recipients	No
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.)	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.). Messages can also be routed to third-party archiving solutions	No, although everything that's quarantined is archived to disk	No
Encryption	Integrates seamlessly with third-party servers using Policy Router Module	TLS encryption included at the MTA level and can also integrate with third-party end-to-end encryption solutions for policy-based encryption	Can integrate with third-party server	No
Clustering support	Yes	Yes	Yes	Yes, can be deployed in a replicated environment

For more information about Email Security and Control, visit www.sophos.com/products/enterprise/email