

Comparison of features

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Notes/Domino
Network location	Gateway	Gateway	Gateway and groupware	Groupware
Organization size	Organizations with up to 80,000 messages per hour (ES4000) or 20,000 messages per hour (ES1000)	50–25,000+ end users	50–10,000+ end users	50–10,000+ end users
Customer requirements	Appliance-based protection against spam, malware, and data loss with minimal administrative overhead. End-user spam quarantine functionality. More reliable and accessible support services.	Complete protection from spam, malware and data loss, plus enforcement of custom messaging policies. Extensive user- or group-based policy flexibility. Delegated administration. End-user spam quarantine functionality.	Spam and malware protection in a single or clustered Microsoft Exchange server environment. Virus protection for Exchange message stores using standard Microsoft APIs. Ability to control email traffic by attachment content, file type, size, email content. End-user spam quarantine functionality.	Malware protection in a single or clustered Domino server environment. Ability to control email traffic by attachment file type, size or email content. Option to allow end users control of non-malware quarantined files.
Ideal customer profile	Organizations looking with limited in-house IT resources dedicated strictly to security. Organizations seeking to reduce the amount of time spent on email security.	Large or complex organizations with established UNIX skills, diverse email management requirements (group, department, customer, etc.) <ul style="list-style-type: none"> Higher education Government Managed email service providers 	Small, medium and large organizations looking for: <ul style="list-style-type: none"> Anti-virus protection for their Exchange message stores A standard Windows gateway solution for spam, virus and spyware protection, and email content control 	Small, medium and large organizations looking for: <ul style="list-style-type: none"> Anti-virus protection for their Lotus Notes email and databases. Basic email content filtering
Installation	Easy installation in any network – plug and protect.	Supports a range of single- and multi-server installation options.	Easy installation – InstallShield Wizard. Out-of-the-box settings provide immediate protection from malware and spam.	Easy installation – InstallShield Wizard. Out-of-the-box settings provide immediate protection from malware.
Supported platforms	Management console <ul style="list-style-type: none"> Web-based Onboard software <ul style="list-style-type: none"> Hardened FreeBSD operating system Postfix MTA 	Management console <ul style="list-style-type: none"> Web-based PureMessage software <ul style="list-style-type: none"> Linux Solaris FreeBSD Debian Virtualization on VMwareESX and Sun Solaris 10 containers. MTAs <ul style="list-style-type: none"> Sendmail 8.11.6 or higher Postfix 2.0.x and 2.1 Supports Sun Java™ System Messaging Server 6 and SunOne Messaging Server 5.2 on Solaris and SPARC 	Management console <ul style="list-style-type: none"> Windows 2000/2003/XP Pro/Vista Windows Server 2008 Active Directory (optional) MMC 3 PureMessage services <ul style="list-style-type: none"> Microsoft Exchange Server 2000/2003/2007 Microsoft SQL 2000/2005 IIS 	Management console <ul style="list-style-type: none"> Windows 2000, XP Pro or Windows 2003 Domino version: <ul style="list-style-type: none"> V6.x V7.x

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Notes/Domino
Management console	Web-based: "three-clicks-to-anywhere" navigation. Designed for management by exception - system notifies admin when attention is required.	Web-based GUI and UNIX command line.	Windows MMC snap-in. Exchange 2007-style layout	Notes-based interface.
Database	Not applicable.	PostgreSQL (bundled).	SQL Server Express 2005 (bundled) SQL Server.	Notes databases.
Multi-server capability	2-unit failover capability (active/passive).	Highly configurable – synchronized administration with option to distribute functions across multiple servers.	Manage and monitor all email servers from one console Supports Exchange clustering. Quarantine and reporting data from multiple servers can be stored in a single database.	Supports Domino clustering.
Quarantine management	Administrator: Powerful message tracking with single-point access to logs and onboard quarantine. End user: Personal quarantine accessed via email digest or web interface.	Administrator: Consolidated and group-based view of quarantined items across all servers. End user: Personal quarantine accessed via email digest or web interface.	Administrator: Consolidated view of quarantined items across all Exchange servers. End user: Personal quarantine accessed via email digest or web interface. Active Directory single sign-on	Administrator: Consolidated view of quarantined items across all Domino servers. End user: Optional devolution of review and release of non-malware quarantined files to end users.
Allow lists and block lists	Offers both administrator and end-user-defined allow and block lists.	Offers both administrator and end-user-defined allow and block lists.	Administrator-defined allow and block lists.	Not applicable.
Policy enforcement	Enables customized policy for unwanted and malicious content and attachments. Routing to third-party encryption or archiving systems. Set policies for inbound and outbound email flows. Adds disclaimers (global, user or group).	Offers a fully configurable, highly flexible policy engine for inbound and outbound email.	Enables customized policy for unwanted and malicious content and attachments. Set policies for inbound, outbound and internal email flows. Uses Active Directory users and groups within email policy. Search for content within common office applications. Adds disclaimers.	Enables customized policy for unwanted and malicious content and attachments. Adds disclaimers.
Spam thresholds	Configurable policies for medium- and high-risk spam.	Multiple configurable policies and thresholds.	Configurable policies for medium- and high-risk spam.	Not applicable.
Reputation filtering	Blocks email from known bad senders at MTA or policy level.	Blocks email from known bad senders at MTA or policy level.	Blocks email from known bad senders as part of spam analysis.	Not applicable.
Virus policy	Policy customization for viruses and encrypted, suspicious and restricted attachments.	Policy customization for viruses and suspicious attachments.	Policy customization for viruses and suspicious attachments.	Policy customization for viruses and suspicious attachments.

	Sophos Email Appliances	PureMessage for UNIX	PureMessage for Microsoft Exchange	PureMessage for Notes/Domino
Languages supported	Mail processing: anti-virus and anti-spam, fully internationalized. End-user interface: English, French, German, Italian, Spanish, Japanese, Traditional Chinese, Simplified Chinese and Swedish Management console: English	Mail processing: anti-virus and anti-spam, fully internationalized. End-user interface: English, French, German, Italian, Spanish, Japanese, Traditional Chinese. Management console: English.	Mail processing: anti-virus and anti-spam, fully internationalized. Admin and end-user interfaces: English and Japanese	Mail processing: fully internationalized. Admin and end-user interfaces: English.
Customization via Sophos ProServices	No.	Yes. Sophos Professional Services provides a range of customizations.	No.	No.
User directory management	Fully synchronized and automated Active Directory integration, tools for manual integration with other directory services.	Built-in list management, plus LDAP or Active Directory.	Fully synchronized and automated Active Directory integration.	Domino directory integration.

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