Symantec™ Messaging Gateway 10.5

Powerful email gateway protection

Data Sheet: Messaging Security

Overview

Symantec Messaging Gateway enables organizations to secure their email and productivity infrastructure with effective and accurate real-time antispam and antimalware protection, targeted attack protection, advanced content filtering, data loss prevention, and optional email encryption. Messaging Gateway is simple to administer and catches more than 99 percent of spam with less than one in one million false positives. With Messaging Gateway defending the email perimeter, organizations can effectively respond to new messaging threats, minimizing network disruption, preserving employee productivity, and protecting company reputation.

Messaging Gateway leverages real-time automatic antispam and antimalware updates from the Symantec™ Global Intelligence Network, Symantec Disarm targeted attack protection technology, customer specific rules, and on-box connection throttling (using both global and self-learning local IP reputation). Comprehensive reporting allows administrators to focus on the overall security posture of the organization while effectively reporting status to key executives and management. Advanced content filtering, data loss prevention, and email encryption help organizations control sensitive data, reducing the risks and costs associated with data loss, and at the same time meeting regulatory compliance and corporate governance demands. Messaging Gateway is available as a physical appliance, a VMware®-certified virtual appliance, or a Microsoft® Hyper-V™ virtual appliance, enabling organizations to easily add capacity to keep messages flowing in the face of growing spam volume.

Reduce risk exposure

Best protection with superior effectiveness and personalized threat detection

Messaging Gateway is powered by the Symantec Brightmail™ antispam filtering engine—a set of technologies that identify email borne threats based on reputation on both the global and local level. This enables it to block more than 99 percent of spam with less than one in one million false positives in addition to blocking up to 90 percent of unwanted email before it reaches your network. Backed by one of the world's largest malware research organizations, the Symantec Global Intelligence Network, Symantec's messaging security solutions draw on real-time intelligence from 120 million devices and over 75 million users to identify new threats before they wreak havoc on unsuspecting victims and organizations.

A key part of the Global Intelligence Network is the patented Symantec Probe Network—a system of over five million decoy email accounts and domains focused on collecting fraud, phishing, and spam samples. The Probe Network has a global presence, including targeted deployments for foreign language content, and can gauge global spam and phishing activity. Symantec analyzes over three billion email messages each day and protects over 850 million mailboxes against spam and malware threats. URL reputation data is also compiled in order to block spam, malware, and phishing messages by identifying threat URLs contained in messages.

Symantec™ Disarm Technology protects users from targeted attacks by removing zero-day document threats from Microsoft Office® and PDF attachments. Potentially malicious active content is removed from the attachment, and the clean document is reconstructed, reattached to the email, and sent to its destination. Disarm stops never-before-seen threats, not just known malware.

Customer Specific Rules provide customers the option to obtain personalized spam rules, in addition to Symantec spam rules, based entirely on submissions from administrators and end users, with full control over the aggressiveness of filter creation

and the ability to instantly remove their tailored rules in case of false positives. Customers can submit messages to Symantec, and based on administrator preferences new rules and filters will be created. Customer specific rules provide automated protection against emerging spam attacks and other types of unwanted mail. More importantly, this can help prevent email attacks that directly target your company and end-users.

Greater control with data loss prevention and email encryption

The loss of your sensitive company information can lead to a damaged reputation, lost customers, and ultimately a decrease in revenue—a setback no company can afford. Messaging Gateway features advanced content filtering and data loss prevention technologies that make it easier to protect and control sensitive data. Administrators can easily build effective and flexible policies that enforce regulatory compliance and protect against data loss. Messaging Gateway appliances leverage integration with sophisticated structured data matching technology from Symantec™ Data Loss Prevention, which analyzes data held in your databases, such as customer and patient records, banking information, order processing, or customer relationship management (CRM), and creates unique fingerprints for the actual data.

In addition to on-box data loss prevention capabilities, Messaging Gateway has the ability to act as an enforcement point for the market-leading Symantec Data Loss Prevention product, giving you the ability to monitor and protect sensitive information being communicated via e-mail, ensuring information ends up where it belongs. The integrated quarantine management capability allows data loss prevention administrators to directly manage and take action on items quarantined by Messaging Gateway from within the Symantec™ Data Loss Prevention Enforce console. For additional security, Transport Layer Security (TLS) encryption is used when sending messages to Symantec Data Loss Prevention.

Messaging Gateway offers a premium add-on, Symantec Content Encryption, that can be deployed as a hosted service or on-premise. For customers who prefer hosted encryption, Symantec Content Encryption provided by Symantec.cloud, offers automatic encryption based on policies and provides flexible message delivery options, making it easy for recipients to receive and reply securely. For customers who prefer on-premise encryption, Messaging Gateway can be integrated with Symantec™ Gateway Email Encryption Powered by PGP™ Technology. Used as a policy enforcement point, Messaging Gateway evaluates messages against customer-specified criteria, and if it's determined encryption is necessary, sends them to Gateway Email Encryption to be encrypted per customer-specified policies.

With email being the most common form of business communication used today, more and more companies are quickly realizing the need for encrypted email as a result of regulations that require private information be encrypted. Combining the content filtering and data loss prevention capabilities of Messaging Gateway with Symantec Content Encryption, your company can avoid stiff fines and costly data breaches.

Messaging Gateway provides you with a robust messaging security solution and cohesive data loss prevention and encryption strategy from a single vendor, which reduces the cost of solutions sprawl and time spent on administration and reporting.

Reduce cost and complexity with easy management

Flexibility and choice

Your IT environment is unique and tailored to your business needs. Your preferences and requirements for deploying a messaging security technology can vary greatly from other organizations. Messaging Gateway adjusts to meet your specific needs by providing flexible deployment options. In addition to deploying Messaging Gateway on a physical hardware appliance,

you have the option to deploy it as a virtual appliance, the fastest growing segment for messaging security deployments. Messaging Gateway is certified with both VMWare and Microsoft Hyper-V virtual environments.

IPv6 supportability means you can choose to deploy your Messaging Gateway in a mixed IPv6/IPv4 network. This allows customers to process, scan, and report on IPv6 based email traffic.

Unified management and administration

Messaging Gateway includes a powerful control center for unified management and administration of your company's messaging infrastructure. From a single Web-based console, administrators can easily manage multiple Messaging Gateway appliances to view trends, attack statistics, and noncompliance incidents. Lightweight Directory Access Protocol (LDAP) credentials can be used to authenticate administrative access and configure groups and policies. By removing the complexity of multiple consoles, disparate policies, and incompatible logging and reporting procedures, Messaging Gateway significantly reduces the total cost of ownership of messaging security infrastructure.

Messaging Gateway supports a full set of reporting options, including a dashboard and executive summaries that highlight system efficacy and impact. Reporting helps administrators proactively identify data loss trends and demonstrate compliance. The management console includes more than 50 preset reports that can be customized by content or time, scheduled for automatic report generation, and exported. Simplified message tracking through a graphical message-auditing interface gives administrators the ability to quickly determine message disposition and delivery status. Feedback on submissions for customer specific rules is available, allowing administrators visibility into what users are submitting and whether there is a rule in place for a submitted message. As the market trends shift and spam becomes more targeted, Messaging Gateway provides administrators with the ability to customize their definition of unwanted email by creating policies for newsletters and marketing email. Additionally, Messaging Gateway can be managed from Symantec™ Protection Center, a single sign-on management console that allows your company to manage and report on all of your security solutions simultaneously.

Messaging Gateway requires very little configuration out of the box, facilitating easy and fast initial deployment. Spam signatures and malware definitions are automatically updated in real-time, leveraging the powerful Global Intelligence Network to simplify management and help ensure the benefits of the latest threat detection across your company.

Key benefits

- Blocks more than 99 percent of spam with less than one in one million false positives and real-time automatic updates.
- Targeted attack, malware, and zero-day threat protection.
- Customer specific rules allow customers to create spam rule sets tailored to their particular environment with easy reporting to determine effectiveness of the custom rules.
- Protects sensitive client data and valuable confidential information, with the ability to fingerprint and identify actual company data within messages or attachments.
- Protects company reputation and manages risks associated with data loss, internal governance, and regulatory compliance.
- Process, scan and report on IPv6 email traffic.
- Optional Symantec Content Encryption subscription integrates email encryption into Messaging Gateway console, leveraging powerful built-in content filtering and data loss prevention policies.
- Includes a dashboard, summary reports, and detailed reports demonstrating the efficacy and impact of Messaging Gateway while proactively highlighting threat trends and potential compliance issues.

- Reduces administrative costs by removing the complexity of multiple consoles, disparate policies, and incompatible logging and reporting, while demonstrating efficacy and impact of messaging security.
- The Global Intelligence Network provides real-time updates to spam and malware protection derived from over 850 million protected mailboxes and over five million accounts in the patented Symantec Probe Network.
- Provides effective, real-time protection against new and emerging threats before they cause disruptions.
- Powerful, cost-effective, easy-to-use Symantec Messaging Gateway 8300 series hardware appliances simplify deployments for small businesses and scaling to the most demanding enterprise environments.
- Flexible, configurable, easy-to-use Messaging Gateway virtual edition runs on VMware or Microsoft hypervisors in the hardware environment of the customer's choosing.

System requirements

Supported platforms

Messaging Gateway can be deployed on a family of Symantec 8300 Series hardware appliances that can scale across organizations from small businesses to large enterprises. There is also a virtual appliance option, the Messaging Gateway virtual edition, which offers the same software, features, and functionality, deployed on VMware or Microsoft Hyper-V environments. Appliances can be deployed as dedicated control centers, scanners, or combined control center/scanners.

Appliance Model	8340	8360	8380
Organization	SMB (Up to 1,000 users)	Enterprise/Large Enterprise	Enterprise/Large Enterprise
Typical Deployment*	Control Center/ Scanner	Dedicated Scanner or Control Center	Dedicated Scanner or Control Center
Form Factor	1RU Rack Mount	1RU Rack Mount	2RU Rack Mount
Power Supply	Single	Redundant, hot-plug, auto-switching, universal power supply	Redundant, hot-plug, auto-switching, universal power supply
CPU	Single Dual-Core Processor	Dual Quad-Core Processors	Dual Quad-Core Processors
Hard Drive / RAID	2 x 500GB SATA RAID 1	2 x 300GB Serial-Attach SCSI (hot-swappable) RAID 1	6 x 300GB Serial-Attach SCSI (hot-swappable) RAID 10
NIC	Two Gigabit Ethernet Ports	Four Gigabit Ethernet Ports	Four Gigabit Ethernet Ports
** Customers may deploy any appliance model as a combined control center/scanner, dedicated scanner, or dedicated control center*			

Appliance Platforms

- Symantec Messaging Gateway 8300 Series appliances
- Symantec 8300 Series appliances
- Symantec Brightmail Appliance 8300 Series
- Symantec Mail Security 8300 Series

Virtual Hypervisors (Virtual Edition)

- VMware ESXi/ESX/vSphere 4.x, 5.x
- Microsoft Hyper-V 2008 or 2012

Browser Requirements (Administrative Console)

- Microsoft Internet Explorer® 8.0, 9.0, or 10.0
- Mozilla Firefox® 20 or later
- Google Chrome® 28 or later

More Information

Visit our website

http://www.symantec.com/messaging-gateway

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21320399 09/13

Confidence in a connected world.