# Symantec™ Messaging Gateway powered by Brightmail™

## Powerful email gateway protection powered by Brightmail

**Data Sheet: Messaging Security**

## Overview

Symantec™ Messaging Gateway powered by Brightmail™, delivers inbound and outbound messaging security, with effective and accurate real-time antispam and antimalware 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 a 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, 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 both a physical appliance and a VMware®-certified 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 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 1 in 1 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 3.5 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. This network gathers more than 30 million probe messages per day. On a broader scale, Symantec also collects anonymous customer statistics on over 8 billion email messages daily and protects over 850 million mailboxes against spam and malware threats. As a customer, you can submit messages to Symantec, which automatically conducts an assessment on your submitted messages to determine if they are legitimate. If a message is deemed illegitimate, rules and filters are created, which are in turn pushed out to your organization to protect against global attacks.

Customer specific rules provide customers the option to obtain personalized spam rules based entirely on submissions from administrators and end users, with capability to control the aggressiveness of filter creation and to remove rules in case of false positives. 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.

Java POWERED

Confidence in a connected world.

✓Symantec™

*Greater control with Data Loss Prevention and E-mail 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 (for example, customer and patient records, banking information, order processing, customer relationship management (CRM), etc.) 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 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.

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 PGP® Universal Gateway Email from Symantec™.  Universal Gateway is configured in gateway mode and acts as an "arm" of Messaging Gateway.  Messaging Gateway will send messages marked for encryption to Universal Gateway on an as-needed basis. Once emails are received on Universal Gateway from Messaging Gateway, they are automatically encrypted and delivered in the method determined by encryption policy so that they can be easily used by the recipient.

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, costly data breaches, and allow the uninterrupted growth of your company, knowing that the evolving threat landscape will not slow you down.

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. Symantec's strategic partnership with VMware and expertise in virtual deployments puts it in position to better secure your virtual messaging security infrastructure.

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.

Confidence in a connected world.    Symantec.

Furthermore, Symantec is one of the leaders in the messaging security segment, ensuring you will be partnered with a known brand that protects more customers than anybody else. As your IT needs and environment change, and threats become more complex, you can be certain that Symantec can offer a secure and robust solution that is perfectly tailored to you and your industry.

### 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. By removing the complexity of multiple consoles, disparate policies, and incompatible logging and reporting procedures, Messaging Gateway significantly reduces the total cost of ownership (TCO) 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 v. 2.0, 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

- Messaging Gateway offers organizations substantial and measurable advantages.
- Blocks more than 99 percent of spam with less than one in one million false positives and real-time automatic updates.
- Antimalware protection powered by Symantec's award-winning antimalware engine, including zero-day 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.

Confidence in a connected world.   ◆Symantec.

- 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, 120 million antimalware sensors, and over 3.5 million accounts in patented 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 hypervisor in the hardware environment of a customer's choice.

## 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 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 146GB Serial-Attach SCSI (hot-swappable) RAID 1 | 6 x 300GB Serial-Attach SCSI (hot-swappable) RAID 10 |
| NIC | Two Gigabit Ethernet Ports | Two 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

Confidence in a connected world. ✓Symantec.

**Virtual Hypervisors (Virtual Edition)**

- VMware ESXi/ESX/vSphere 4.0, 4.1, 5.0

**Browser Requirements (Administrative Console)**

- Windows IE 8, 9
- Mozilla Firefox 13 or later
- Chrome 19 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 the 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 industry-leading 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

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.     20012004-3  08/12

Confidence in a connected world.   Symantec.