DATA SHEET

# Messaging Gateway On-Premises Appliance

## Introduction

Smart, comprehensive email security—whether your email system is on-premises, cloud-based, or both—begins with a clear, realistic understanding of what you're up against. Email is still the most popular and pervasive tool cybercriminals use to launch and distribute threats including spear phishing, ransomware and business email compromise (BEC) attacks. According to the 2018 Symantec™ Internet Security Threat Report (ISTR), in 2017 one out of every 412 emails contained a malware attack, 7,710 organizations are hit by a Business Email Compromise Attack every month, and spear-phishing is the most widely used infection vector, being used by 71 percent of targeted attack groups.

## Messaging Gateway

Symantec™ Messaging Gateway is an on premises email security solution that provides inbound and outbound messaging security including, powerful protection against the latest messaging threats, including ransomware, spear phishing, and business email compromise. It catches more than 99 percent of spam with a less than 1 in 1 million false positives, and effectively responds to new messaging threats with real-time antispam and antimalware intelligence; built-in data protection capabilities keep your email secure and confidential.

Messaging Gateway can be implemented as a virtual or physical appliance, and you can easily add capacity to keep messages flowing as the volume of spam increases.

### Stop Advanced Threats in Their Tracks

Messaging Gateway combines multilayer detection technologies, powered by insights from the world's largest civilian threat intelligence, to effectively block and quarantine suspicious email.

**Multilayer Spam and Malware Filtering**

Block unwanted email and prevent delivery of malicious links and attachments.

**Targeted Attack Protection**

Get strong protection against spear phishing, ransomware, and BEC attacks.

**Content Filtering and Data Loss Prevention**

Filter content for extensive inbound defense. Prevent leakage of sensitive company information.

- Stops BEC attacks using advanced heuristics, a BEC scam analysis engine, sender authentication, and domain intelligence to stop URL hijacking and identity spoofing.
- Symantec Email Fraud Protection automates the creation of sender authentication protocols (DMARC, DKIM, and SPF), protecting all recipients from impersonation attacks.
- Defends against malicious links used in spear phishing campaigns with URL reputation filtering based on Symantec's global database which includes advanced phishing variant detection, which sniffs out spear phishing links that are similar to known phishing attacks.
- Protects users from targeted attacks such as ransomware by removing zero-day document threats from Microsoft Office and PDF attachments. Potentially malicious active content from an attachment is removed and a clean document is re-constructed, reattached to the email, and sent to the end user.

- Blocks spam and directory harvesting attacks using a combination of Symantec global and local sender reputation databases, heuristics and customer-specific spam rules that restrict up to 99 percent of unwanted email before it reaches your network. Outbound sender throttling prevents outbound spam attacks from compromised internal users, and negatively impacting sender reputation.

- Defends against malicious links used in spear phishing campaigns with URL reputation filtering based on Symantec's global database which includes advanced phishing variant detection, which sniffs out spear phishing links that are similar to known phishing attacks.

### Protect Sensitive Data; Prevent Unwanted Email

Messaging Gateway provides built-in content filtering and data loss prevention controls that block or quarantine sensitive and unwanted email.

- Advanced content filtering controls prevent unwanted email such as newsletters and other marketing content from reaching users.

- Built-in data loss prevention policies make it easier to safeguard company data within messages or attachments. Administrators can build effective and flexible policies using 100 pre-built dictionaries, patterns, and policy templates that help you implement automated data protection and enforcement policies.

- Automatic SMTP over TLS encryption ensures all email communications in transit are secure.

### Manage Messaging Security with Deep Visibility

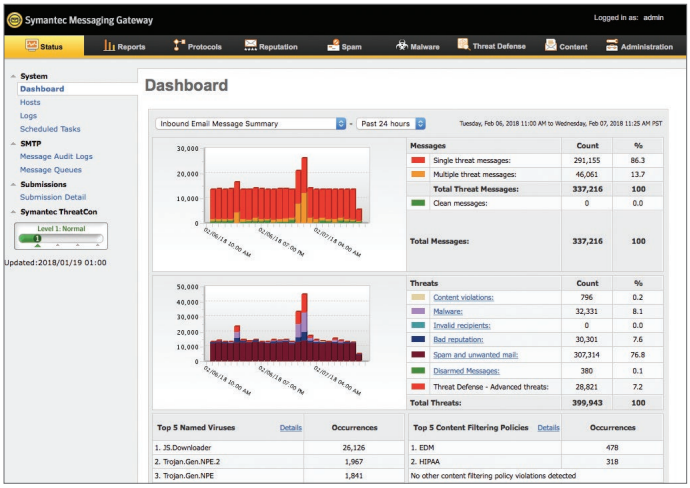
A single web-based console provides granular policy configuration and control, detailed reporting, and a consolidated view of threat trends, attack statistics, and non-compliance incidents. Multiple Messaging Gateway appliances can be managed in a mixed IPv4/IPv6 environment.

- Dashboard, summary, and detailed reports, including 50 preset reports that are customizable by content and schedule frequency, highlight threat trends and potential compliance issues.

- Generated Syslog data can be exported into third-party security and information tools (SIEM) for further correlation analysis.

- Simple message tracking using a graphical message-audit interface provides the ability to quickly determine message disposition and delivery status.

- Automatically receive threat alerts and notifications on virus outbreaks, policy violations, and quarantine information.




# Integrate with Symantec Content Analysis, Threat Isolation, and DLP

- For additional advanced threat protection capabilities, Messaging Gateway can offload messaging file-based content to Symantec Content Analysis for further inspection. This includes actionable intelligence that combines static analysis, machine learning and behavior analysis techniques. An adaptive and customizable sandbox delivers comprehensive malware detonation to quickly analyze suspicious files, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

- For advanced protection from potentially malicious web links contained in email, URLs can be rewritten to Symantec Email Threat Isolation, a technology that executes web sessions away from endpoints. Sending only safe rendering information to users' prevents any website delivered zero-day malware from reaching end user devices. Rendering potential spear phishing sites in read-only mode also stops credential theft, since users are prevented from submitting corporate credentials or other sensitive information.

- For organizations using or considering Symantec's market-leading DLP solution, Messaging Gateway tightly integrates with Symantec DLP to extend policy encforcement to the email channel. Policy-based encryption is available as a Symantec Content Encryption add-on.

### Messaging Gateway Certifications

- Common Criteria EAL2
- FIPS 140-2

# Symantec Messaging Gateway S450 Series Hardware Appliances

| | Symantec Messaging Gateway S450 |
|---|---|
| Organization size | Enterprise/large enterprise |
| Typical implementation | Combined control center/scanner, dedicated scanner, or dedicated control center |
| Form factor | 1U rack mount |
| Power supply | 2 1600-watt PSU, redundant |
| CPU | Dual twelve-core processors |
| Hard drive/RAID | 4 x 4TB<br>SAS HDD<br>RAID 10 |
| NIC | 10-Gigabit Ethernet ports |

# System Requirements

Virtual appliance option (same features and functionality)

- VMware ESXI™/VMware ESX®, VMware vSphere® 5.x, 6.x
- Microsoft Hyper-V® 2008 or 2012

Browsers (for administrative console)

- Microsoft Internet Explorer® 11.0 or later
- Mozilla® Firefox® 45 or later
- Google Chrome™ 55 or later

## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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



19D214107_DS_SMG_ON-PREMISE_APPLIANCE_EN