PRODUCT BRIEF

Symantec® Messaging Gateway

Inbound and Outbound Messaging Security

AT A GLANCE

Symantec® Messaging Gateway (SMG) defends your email communications against spam, malware, and targeted attacks.

KEY BENEFITS

- Stop advanced threats
- Prevent unwanted emails
- Protect sensitive data
- Enable deep visibility to messaging threats

KEY FEATURES

- Multilayer detection technologies
- Advanced content filtering
- Data loss protection
- Detailed auditing
- Powerful security integrations

Overview

Email is one of the primary communication channels for any business. It is also one of the most popular and pervasive vectors for cyber criminals to launch and distribute threats, including spear phishing, ransomware, and business email compromise attacks. People are often considered the weakest link in any security program. Accidentally clicking on the wrong link or sending a file with sensitive data can have disastrous effects. Smart, comprehensive email security, whether your email system is on-premises, cloud-based, or both, begins with preventing these types of events from occurring. Block and quarantine suspicious emails before they ever reach your users, and monitor outbound emails to ensure that your corporate data is protected.

Symantec® Messaging Gateway (SMG) is an on-premises email security solution that provides inbound and outbound messaging security by delivering the following capabilities:

- Multilayer detection technologies
- Advanced content filtering
- Data loss protection
- Detailed auditing
- Powerful security integrations

With these core features, SMG secures email communications from spam, malware, and targeted attacks. It also prevents accidental or malicious data leakages. Additionally, SMG 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.

Multilayer Detection Technologies Stop Advanced Threats

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

- **Business email compromise (BEC) attacks:** The solution uses advanced heuristics, a BEC scam analysis engine, sender authentication, and domain intelligence to stop URL hijacking and identity spoofing.
- **Spear phishing attacks:** The solution defends against malicious links used in spear phishing campaigns with URL reputation filtering based on the Symantec global database, which identifies links that are similar to known phishing attacks.
- **Ransomware attacks:** The solution protects users from targeted ransomware attacks by removing zero-day document threats from Microsoft Office and PDF attachments. Any potentially malicious active content is removed from an attachment and a clean document is reconstructed, re-attached to the email, and sent to the end user.
- **Directory harvesting attacks:** The solution leverages a combination of Symantec global and local sender reputation databases, heuristics, and customer-specific spam rules that restrict up to 99% of unwanted email before it reaches your network. Additionally, outbound sender throttling prevents outbound spam attacks from compromised internal users, and negatively impacting sender reputation.
- **Impersonation attacks:** The solution integrates with Symantec Email Fraud Protection to automate the creation of sender authentication protocols (DMARC, DKIM, and SPF), protecting all recipients from impersonation attacks.

Content Filtering Prevents Unwanted Email

SMG advanced content filtering controls prevent unwanted email such as newsletters and other marketing content from reaching users. The solution also leverages a combination of Symantec global and local sender reputation databases, heuristics, and customer-specific spam rules that restrict up to 99% of spam before it reaches your network.

Data Loss Prevention Protects Sensitive Data

SMG provides built-in data loss prevention policies to 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 to help you implement automated data protection and enforcement policies. In addition, the solution also provides automatic SMTP over TLS encryption, ensuring that all email communications in transit are secure.

Detailed Auditing Enables Messaging Security Management with Deep Visibility

SMG includes a single web-based console that provides granular policy configuration and control, detailed reporting, and a consolidated view of threat trends, attack statistics, and non-compliance incidents.

- **Auditing tools:** Dashboard, summary, and detailed reports, including 50 preset reports that are customizable by content and schedule frequency, highlight threat trends and potential compliance issues.
- **SIEM integration:** Generated Syslog data can be exported into third-party security and information tools (SIEM) for further correlation analysis.
- **User-friendly:** Simple message tracking using a graphical message-audit interface provides the ability to quickly determine message disposition and delivery status.

In addition, the solution architecture ensures that multiple SMG appliances can be managed in a mixed IPv4 and IPv6 environment.

Powerful Security Integrations

For additional advanced threat protections, SMG can offload messaging file-based content to Symantec Content Analysis for further inspection. This inspection 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. SMG tightly integrates with Symantec DLP to extend policy enforcement to the email channel. Finally, policy-based encryption is available as a Symantec Content Encryption add-on.

Deployment Flexibility

SMG software is available on various platforms and can be deployed in flexible roles, offering modular and scalable architecture as per enterprise needs.

Feature	Description
Platform Support	*VMware, HyperV, KVM, Microsoft Azure, Symantec Messaging Gateway Appliance 8390 Hardware*
Deployment Roles	*All-in-one, control center, and quarantine-only scanner only; quarantine only*
Appliance Form Factor	*1U rack mount*
CPU	*Dual 20 Core processor*
Memory: Hard Drive/RAID	*192-GB RAM, 6 x 2.4-TB hard drive (RAID 10)*
NIC	*Dual port 1-Gb onboard, dual port 10GbE Base-T adapter*

Summary

SMG delivers a comprehensive set of threat detection capabilities that secure inbound and outbound email messages. These capabilities prevent insidious email threats such as business email compromise, ransomware, and spam, and ensure your users do not accidentally send out sensitive data. The solution also integrates with other leading Symantec security solutions to provide additional security against messaging threats.

For more information, please visit broadcom.com/symantec-smg

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

19D214107-PB101 August 11, 2023