Symantec

DATA SHEET

Messaging Gateway 10.6

Symantec is the overall revenue leader in messaging security in the “IDC MarketScape: Worldwide Email Security 2016 Vendor Assessment.”

Introduction

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, and built-in data protection capabilities to keep your email secure and confidential. 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 automatic antispam and antimalware updates.

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 uses advanced multilayered detection technologies and real-time threat intelligence from the Symantec Global Intelligence Network to stop advanced threats in their tracks.

Figure 1 – Symantec Messaging Gateway uses advanced multilayered detection technologies.

Combining multilayer detection with rich threat intelligence delivers powerful protection against spear phishing, business email compromise (BEC), ransomware, and other advanced threats.

- Blocks spam using a combination of Symantec global and local sender reputation databases and customer-specific spam rules that restrict up to 90 percent of unwanted email before it reaches your network.
- Stops spear phishing and BEC using advanced heuristics to scan email, and domain intelligence to stop URL hijacking and identity spoofing.
- Protects users from targeted attacks such as ransomware by removing zero-day document threats from Microsoft Office® and PDF attachments. Messaging Gateway removes potentially malicious active content from an attachment and reconstructs the clean document, reattaches it to the email, and sends to the end user.
- Defends against malicious links in email using URL reputation filtering based on Symantec's global database.

Protect sensitive data in email

Messaging Gateway prevents data leakage with built-in content filtering, data loss prevention and policy-based encryption controls that block, quarantine, or encrypt sensitive email.

- Advanced content filtering controls prevent unwanted email from reaching users, and data loss prevention technologies 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 by fingerprinting and identifying actual company data within messages or attachments.
- Policy-based email encryption evaluates messages against customer-specified criteria. If encryption is necessary, messages can be sent to Symantec Content Encryption, an add-on available as a hosted service or on-premises implementation.
- Tight integration with market-leading Symantec Data Loss Prevention provides a monitoring and enforcement point for sensitive information in email.

Manage messaging security infrastructure with less overhead

A single web-based console provides a consolidated view of threat trends, attack statistics, and noncompliance incidents, and enables simplified management of multiple Messaging Gateway appliances in a mixed IPv6/IPv4 environment.

- Dashboard, summary, and detailed reports, including 50 preset reports customizable by content or time and schedule generation, highlight threat trends and potential compliance issues.
- Generated Syslog data can be exported into third-party security information and event management tools for further correlation analysis.
- Simple message tracking using a graphical message-audit interface provides the ability to quickly determine message disposition and delivery status.
- Customizable policy definitions filter delivery of unwanted email, such as newsletters and other marketing content.

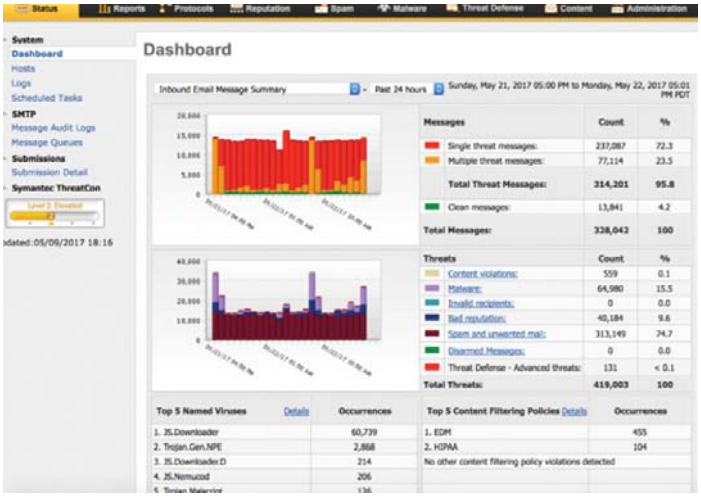

Figure 2 – Symantec Messaging Gateway console

Integrate with Symantec Content and Malware Analysis

For additional advanced threat protection capabilities, Messaging Gateway can offload messaging 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.

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

Symantec Messaging Gateway 8300 Series hardware appliances

	Symantec Messaging Gateway 8340	Symantec Messaging Gateway 8380
Organization size	Small/medium business	Enterprise/large enterprise
Typical implementation	Combined control center/scanner, dedicated scanner, or dedicated control center	Combined control center/scanner, dedicated scanner, or dedicated control center
Form factor	1RU rack mount	1RU rack mount
Power supply	Single	Redundant, hot-plug, auto-switching, universal power supply
CPU	Single quad-core processor	Dual six-core processors
Hard drive/RAID	2 x 1 TB SAS RAID 1	6 x 300 GB Serial-attach SCSI (hot-swappable) RAID 10
NIC	Gigabit Ethernet ports	Gigabit Ethernet ports

Learn more about:

Symantec Messaging Gateway

Symantec Content and Malware Analysis

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 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