On-Premises Email Security with Advanced Threat Protection

The frequent use of email makes it the No. 1 target for attacks by hackers who want to compromise your security. The widespread adoption of traditional email security solutions has forced attackers to seek more sophisticated ways to infiltrate organizations. Traditional blocking tools will not protect you from targeted spear phishing, business email compromise (BEC), and other sophisticated email attacks. Your organization must augment traditional email security methods with the most current detection technologies, such as machine learning, predictive and behavior analysis, and sandboxing.

Messaging Security

Symantec™ Messaging Gateway delivers on-premises inbound and outbound messaging security on a single platform. It effectively responds to new messaging threats with real-time antispam and antimalware protection, advanced threat protection, and data loss prevention technologies.

Messaging Gateway integrates with Symantec™ Content and Malware Analysis to provide additional advanced threat protection capabilities. Together, they effectively block known and unknown threats, empower organizations to quickly respond to targeted and advanced attacks, and keep information in your email secure and confidential.
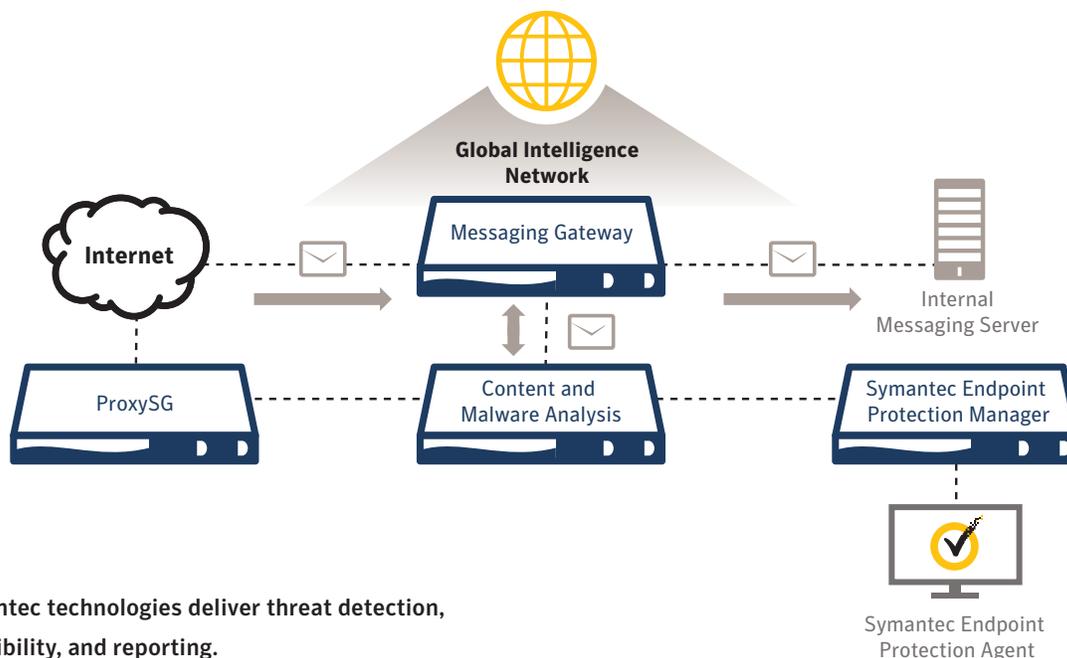

Figure 1: Symantec technologies deliver threat detection, prevention, visibility, and reporting.

✓Symantec.™

Advanced Detection Technology

Using advanced multilayered detection technologies, such as machine learning, behavior analysis, and sandbox detonation of suspicious files and URLs, Messaging Gateway delivers powerful protection against spear phishing, BEC, and other advanced threats. It provides visibility into emerging threats with real-time threat intelligence from the Symantec Global Intelligence Network, based on more than 175 million endpoints and 57 million attack sensors in 157 countries.
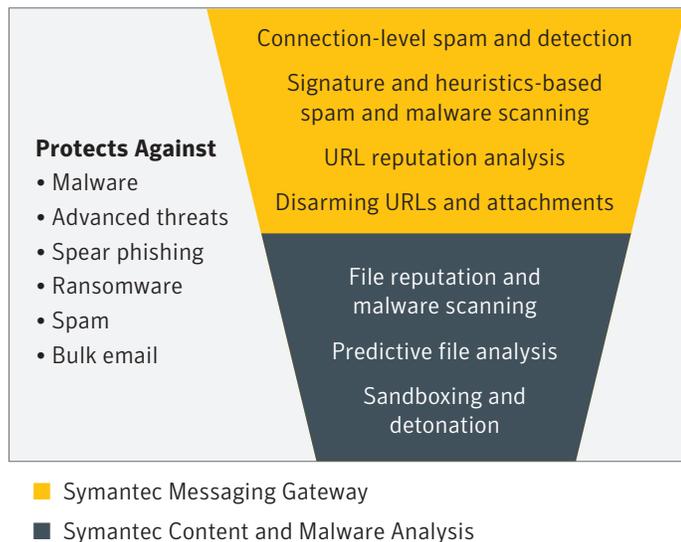
Protects Against
- Malware
- Advanced threats
- Spear phishing
- Ransomware
- Spam
- Bulk email

Connection-level spam and detection

Signature and heuristics-based spam and malware scanning

URL reputation analysis

Disarming URLs and attachments

File reputation and malware scanning

Predictive file analysis

Sandboxing and detonation

■ Symantec Messaging Gateway

■ Symantec Content and Malware Analysis

Figure 2: Symantec threat detection technologies protect organizations from sophisticated attacks.

In-depth Threat Analysis and Reduced Response Time

Stop targeted and advanced threats from spreading with in-depth analysis of sophisticated attack campaigns on your network. This includes indicators of compromise (IOC), such as URL information, file hashes, threat risk scores, and targeted attack information. Integration with Symantec Endpoint Protection and the Symantec ProxySG™ secure web gateway adds threat analysis, blocking, and remediation across web, email, and endpoints. Your security analysts can quickly correlate information and respond to threats through integration with third-party security information and event management (SIEM) systems.

Data Loss Prevention

Prevent leakage of sensitive information and meet your compliance and privacy requirements with built-in granular data loss prevention (DLP) and policy-based encryption controls that block, quarantine, or encrypt email. Tight integration with Symantec Data Loss Prevention provides a monitoring and enforcement point for sensitive information shared in email.

Symantec Messaging Gateway Key Capabilities

Threat detection and prevention

- Detects and blocks spam, malware, and other inbound email threats.
- Protects users from targeted attacks by removing zero-day document threats from Microsoft Office® and PDF attachments, including never-before-seen threats, not just known malware.
- Provides signatures and heuristics, global and local sender reputation analysis, and URL reputation-based filtering to protect against sophisticated attacks and reduce email infrastructure costs by restricting unwanted connections.

Visibility and reporting

- Provides dashboard, summary, and detailed reports to highlight threat trends and potential compliance issues.
- Integrates with third-party SIEM tools enabled through export of Syslog data for further correlation analysis.

Data protection

- Uses advanced content filtering controls to prevent unwanted email from reaching users, with DLP technologies to protect and control sensitive data and build workflows to enforce regulatory compliance.
- Evaluates messages against customer-specified criteria and, if necessary, sends them to Symantec Gateway Email Encryption.
- Integrates with Symantec Data Loss Prevention to provide a monitoring and enforcement point for sensitive information communicated via email.

✓Symantec. | 2

Symantec Content and Malware Analysis Key Capabilities

Threat Detection and Prevention

- Provides additional antimalware and blacklist/whitelist engines using unique threat intelligence that rescans email from Messaging Gateway.
- Uses sophisticated static code file analysis, then classifies and acts on results—drops, delivers, or passes files on for sandboxing detonation.
- Offers a customizable virtualized sandbox to replicate production environments, and a bare-metal sandbox emulator for accurate analysis and detection of VM-evasive malware originating from URLs and files.

Visibility and Reporting

- Issues sandbox detonation reports that provide actionable intelligence such as key malicious indicators, detailed static and dynamic event activity, downloadable analysis of artifacts and resources, and generated threat risk score.
- Integrates with third-party SIEMs using rich APIs to export advanced threat information for further correlation and assessment.
- Integrates with Symantec Endpoint Protection and Symantec ProxySG to provide threat analysis and blocking and remediation across network, endpoint, and messaging channels.

Learn more about Symantec Messaging Gateway

Learn more about Symantec Content and Malware Analysis

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

"The Forrester Wave™: Automated Malware Analysis Q2 2016" identified Blue Coat as one of the most significant automated malware analysis providers.

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 Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com