DATA SHEET

Messaging Gateway with Advanced Threat & Data Protection

Introduction

The frequent use of email makes it the #1 target for attacks by hackers who want to compromise your security. The widespread adoption of email security solutions has forced attackers to seek more sophisticated ways to infiltrate organizations. Basic blocking tools will not protect you from targeted ransomware, spear phishing, business email compromise (BEC), and other sophisticated email attacks. Organizations must augment traditional email security technologies with a multi-layered approach based on the latest prevention technologies such as machine learning, link isolation, and behavior analysis with efficient sandboxing and file detonation.

Messaging Security Solution

Symantec's on-premises email security solution begins with Messaging Gateway which provides essential 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 automatic antispam and antimalware updates.

Messaging Gateway combines multilayer protection technologies that effectively detect, block, and quarantine suspicious email:

- Stops BEC attacks using advanced heuristics, BEC scam analysis, email sender authentication protocols (DMARC*, DKIM, and SPF), and domain intelligence to block typo squatting and identity spoofing.
- Prevents 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.
- Advanced content filtering controls prevent unwanted email such as newsletters and other marketing content from reaching users.
- Defends against malicious links used in spear phishing campaigns with URL reputation filtering from Symantec's global database, which includes advanced phishing variant detection technology that sniffs out spear phishing links that are similar to known phishing attacks.
- Protects users from targeted attacks such as ransomware by disabling URLs and zero-day document threats from Microsoft Office and PDF attachments. Potentially malicious active content from an attachment is removed and a clean document is reconstructed, reattached to a clean email, and sent to the end user.

Messaging Gateway integrates with Symantec™ Content Analysis and Symantec Email Threat Isolation to provide additional advanced threat protection and threat analysis capabilities. Together, they effectively block evolving and unknown threats, and empower organizations to quickly respond to targeted and advanced attacks.

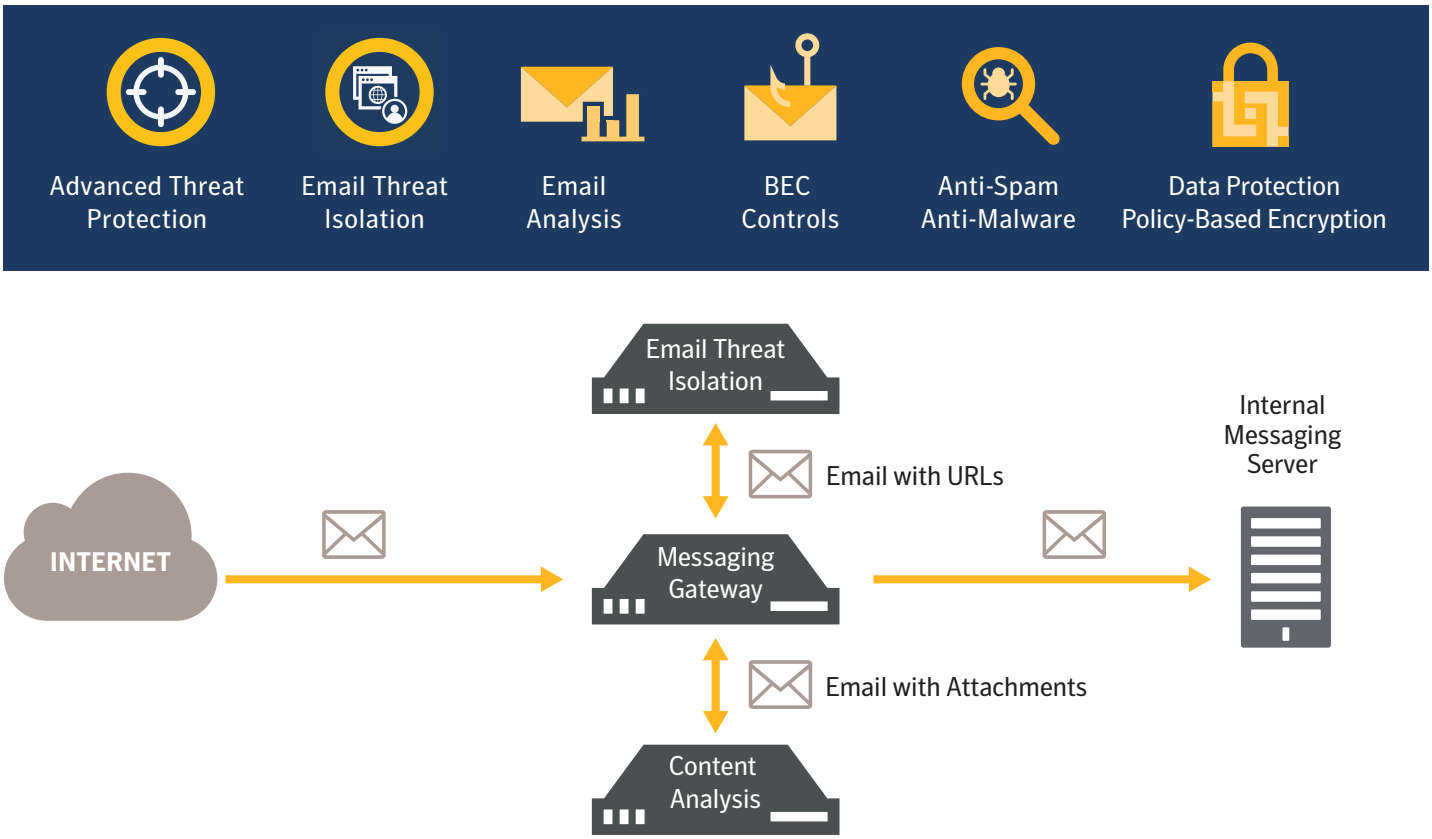
This protection is powered by insights from the world's largest civilian threat intelligence network, the Symantec Global Intelligence Network (GIN), which offers visibility into the threat landscape worldwide. The GIN helps ensure better security outcomes through telemetry distilled from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors in 157 countries.

Symantec Messaging Gateway

Symantec Content Analysis

Symantec Email Threat Isolation

*Available May 2018



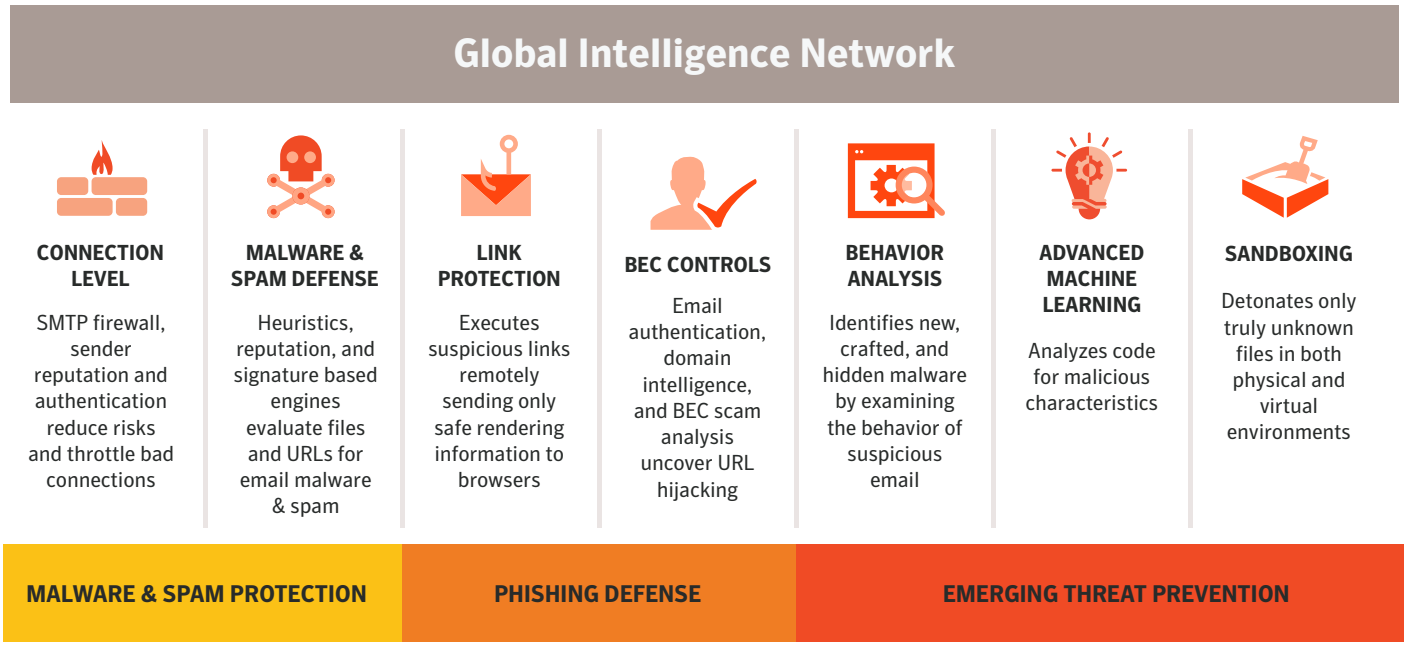
Graphic: Symantec Messaging Gateway, Content Analysis, and Email Threat Isolation Integration

Advanced Threat Protection for Malicious Links and Files

Advanced protection against malicious links used in spear phishing and targeted attack campaigns is provided by Email Threat Isolation which executes suspicious links remotely. This technology sends only safe rendering information to browsers, thereby preventing any zero-day malware delivered via email links from reaching your users. Email Threat Isolation also stops credential phishing by rendering suspicious websites in read-only mode, blocking users from submitting sensitive information such as corporate credentials and passwords.

Advanced threat protection for file based attacks is provided by Content Analysis which automatically escalates and brokers zero day threats utilizing advanced technologies such as machine learning, predictive file analysis, and virtual machine aware sandboxing to reveal malicious behavior and safely detonate suspicious files:

- Uses sophisticated predictive file analysis and machine learning to classify and act on results— drop, deliver, or pass files on for behavior analysis and detonation in a sandbox.
- Offers a customizable virtual machine or emulation-based sandbox to replicate production environments for accurate analysis and detection of virtual machine evasive malware originating from files.



Graphic: multi-layered threat detection technologies

Respond Faster to Targeted Attacks with Threat Analytics

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 file hashes and file artifacts, threat risk scores, and attack technology used. Security analysts can quickly correlate information and respond to threats using a native dashboard or through integration with third-party security information and event management (SIEM) systems. Messaging Gateway and Content Analysis provide the following threat intelligence to help accelerate threat investigation and response:

- Content Analysis 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.
- Messaging Gateway dashboard summary and detailed reports highlight threat trends, attack statistics and potential compliance issues. Automatic alerts provide real-time notification on virus outbreaks, policy violations, and email quarantine information.
- Find trends in attacks and identify targeted attack recipients using third party SIEMs to correlate advanced threat information from Content Analysis with Syslog data from Messaging Gateway.
- Accelerate threat analysis, blocking and remediation across network, endpoint, and messaging channels with Symantec Endpoint Protection and Symantec ProxySG integrations.

Data Loss Prevention

Prevent leakage of sensitive information and meet your compliance and privacy requirements with Messaging Gateway's built-in, data loss prevention (DLP) and integrated policy-based encryption controls that make it easier to safeguard company data within messages or attachments.

- 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. Over 100 pre-built dictionaries, patterns, and policy templates help you implement automated data protection and enforcement policies easily.
- Automatic SMTP over TLS encryption ensures all email communications in transit are secure.
- Policy-based email encryption evaluates messages against customer-specified criteria. If encryption is necessary, messages can be sent to Symantec Content Encryption, an available add-on.
- Tight integration with market leading Symantec Data Loss Prevention provides a monitoring and enforcement point for sensitive information shared in email.

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

Symantec Selected as the Top Leader in the "Advanced Persistent Threat (APT) Protection - Market Quadrant 2017", Radicati

Learn more about Symantec Messaging Gateway

Learn more about Symantec Content Analysis

Learn more about Symantec Email Threat Isolation

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.

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

18D155270_ds_On-Premises_Email_Security_with_ATP.indd