DATA SHEET

Cloud-Based Email Security for the Federal Government

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 2017 Symantec Internet Security Threat Report (ISTR), one out of every 131 emails in 2016 contained a malware attack, and 61% of organizations were hit by a ransomware attack in 2016.

As federal government agencies look to strengthen their cybersecurity posture using public cloud across critical IT infrastructure such as email, selecting a FedRAMP Authorized email security service that provides strong protection against malicious threats should be at the forefront of your cybersecurity strategy.

Symantec Email Security Service – Government

Symantec Email Security Service – Government is a FedRAMP Authorized cloud service that provides inbound and outbound messaging security including powerful protection against the latest messaging threats for Microsoft O365 email, Microsoft Exchange, and Google Gmail. This service effectively blocks advanced threats including ransomware, spear phishing, and business email compromise, and catches more than 99 percent of spam with a less than 1 in 1 million false positives by effectively responding to new messaging threats with real-time automatic antispam and antimalware updates.

Stop Advanced Threats in Their Tracks

Email Security Service – Government 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.

- 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 90 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.

- Stops BEC attacks using advanced heuristics, a BEC scam analysis engine, and DMARC/DKIM/SPF email authentication to scan email, and domain intelligence to stop URL hijacking and identity spoofing.
- 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 reconstructed, reattached to the email, and sent to the end user.

Protect Sensitive Data in Email

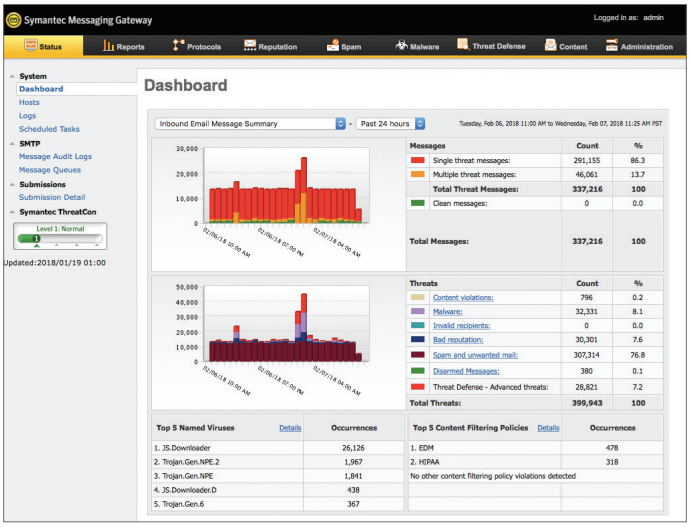
Email Security Service – Government provides built-in content filtering and data loss prevention controls that block or quarantine sensitive and unwanted email.

- 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 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.

- 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.



Symantec Email Security Service – Government Certifications

- FedRAMP Authorization – Moderate
- Common Criteria EAL2
- FIPS 140-2

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