SOLUTION BRIEF

CHALLENGE

Legacy messaging security approaches have proven mainly ineffective against the increasingly advanced and sophisticated email threats launched by today's cyber criminals.

OPPORTUNITY

Symantec Email Security blocks common messaging threats through multilayered defense and insights distilled from the world's largest civilian threat intelligence network.

BENEFITS

Implementing the intelligent and comprehensive Symantec Email Security to complement the native security within your existing messaging platform significantly reduces your risk.

Email Security

Messaging Protection for the Enterprise

Overview

Email remains a primary target for cyber criminals to launch and distribute sophisticated threats like ransomware, spear phishing, and business email compromise (BEC) scams. As the volume and complexity of these attacks rise, traditional email defenses are increasingly ineffective. Attackers now use advanced tactics such as domain spoofing and link obfuscation to evade detection, making it much harder to stop these threats than conventional malware.

According to the 2024 Verizon Data Breach Investigations Report, email is the leading vector for ransomware and the second most common breach method. The 2023 IBM Security Breach Report highlights the staggering costs of email-based attacks, with BEC averaging $4.67 million, phishing $4.76 million, and social engineering $4.55 million.

Businesses transitioning to cloud-based email systems like Microsoft Office 365 or Google Workspace face even more significant risks, as native security often falls short. Legacy email security solutions, constrained by inadequate analytics and fragmented operations, fail to meet the challenges of today's evolving threat landscape, creating gaps in protection, increasing complexity, and exposing organizations to data leakage, compliance violations, and financial losses.

To counter these threats, enterprises need a comprehensive, intelligent email security platform that complements existing malware and spam protection. Whether on-premises, cloud-based, or hybrid, this robust solution is essential to safeguarding sensitive data and ensuring compliance in an era of advanced email threats.

Introducing Symantec® Email Security

Symantec® Email Security offers comprehensive capabilities to protect cloud and on-premise email systems. It defends against sophisticated threats like ransomware, spear phishing, and BEC scams with a multilayered approach enhanced by insights from the world's largest civilian global intelligence network. This solution prevents spear phishing with robust protection, isolation, visibility, sender authentication, and user awareness. Additionally, it accelerates attack response through advanced analytics, providing deep visibility into targeted attack campaigns. Symantec Email Security also monitors outbound emails, ensuring corporate data protection.

Symantec Email Security delivers superior flexibility by offering two deployment options:

- **Symantec Email Security.cloud** is a cloud-based service that is easy to implement and operate and scales quickly as messaging volume grows.
- **Symantec Messaging Gateway** is an on-premises email security solution deployed as a virtual or physical appliance.

The following sections explore each of these products in more detail.

MESSAGING PROTECTION FOR THE ENTERPRISE

Broadcom offers the industry's most comprehensive email security portfolio, combining cloud and on-premises solutions that enhance the native security features of most email platforms. Three key differentiators set this solution apart:

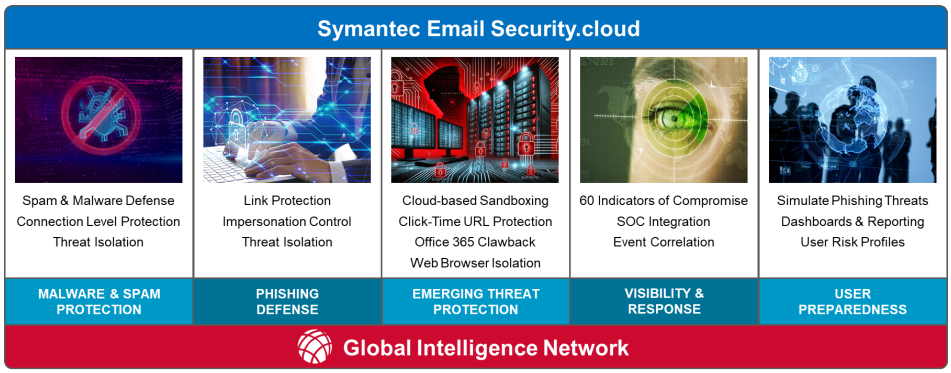
- Security powered by global intelligence
- Awareness to combat human error
- Insights to accelerate response

Introducing Symantec Email Security.cloud Service (ESS)

Symantec ESS provides a comprehensive solution for protecting both cloud-based email platforms (e.g., Office 365 and Google Workspace) and on-premise systems (e.g., Microsoft Exchange). With a multilayered defense, it blocks advanced threats such as ransomware, spear phishing, and BEC while offering enhanced visibility into attack campaigns through advanced analytics and integration with the Symantec Global Intelligence Network (GIN).

As shown in Figure 1, this end-to-end email security solution begins with robust malware and spam protection and phishing defense. The Symantec Email Threat Detection, Response, and Isolation (ETDRI) service further strengthens security by delivering emerging threat protection, real-time visibility, and user preparedness.

Figure 1: The Most Complete Protection in the Industry



Malware and Spam Protection

The cornerstone of email security is prevention. Symantec ESS strengthens the native security of email systems by utilizing reputation analysis, antivirus engines, and antispam signatures to inspect links and attachments, effectively blocking spam and malware. It further mitigates risks by providing connection-level protection, which slows or drops anomalous SMTP connections. When ETDRI is deployed, Symantec ESS prevents ransomware and other malware infections by isolating suspicious email attachments. Additionally, it isolates risky or unknown email links that host malware, ensuring users and devices remain safe from infected downloads.

Phishing Defense

Symantec ESS delivers effective phishing defense by scanning links in real-time before email delivery and again at the time of the click, tracing them to their final destination—even when attackers employ advanced evasion techniques. Its advanced phishing variant detection identifies and blocks links resembling known phishing attacks. The service also protects against BEC and spoofing, using a sophisticated impersonation engine to block threats that mimic legitimate users or domains. Additionally, when deployed with ETDRI, Symantec ESS opens risky or unknown website links in read-only mode, further safeguarding users from phishing attacks.

Emerging Threat Protection

Symantec ETDRI strengthens email security by integrating these advanced detection technologies into the Symantec ESS platform:

- **Cloud-based sandboxing** identifies complex and advanced attacks by mimicking human behavior to execute suspicious files both virtually and on physical hardware, uncovering threats that bypass traditional sandboxing.

SYMANTEC EMAIL SECURITY.CLOUD SERVICE (ESS)

A comprehensive solution for protecting both cloud-based email platforms and on-premise systems, ESS leverages a multilayered defense:

- Malware and spam protection
- Phishing defense
- Emerging threat protection
- Visibility and response
- User preparedness

SYMANTEC MESSAGING GATEWAY (SMG)

An on-premises email security solution designed to scale easily as spam volume increases, SMG ensures both inbound and outbound messaging security with a range of advanced capabilities:

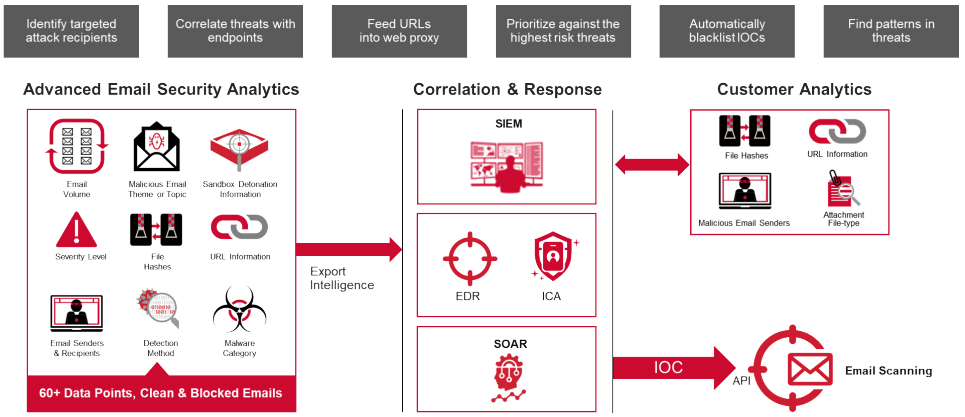
- Multilayer detection technologies
- Data loss protection
- Detailed auditing and reporting

- **Click-time URL protection** blocks malicious links when clicked, preventing attacks that weaponize links after email delivery. This complements initial predelivery link scanning.
- **Office 365 Clawback** moves any email found to contain malware out of users' inboxes, removing dangerous messages before they can be accidentally opened.
- **Web browser isolation** protects users from advanced email threats such as spear phishing, credential theft, and ransomware by creating a secure environment between users and email links. It remotely renders suspicious content and scans potentially infected downloads before they reach the device.

Visibility and Response

Effective email security extends beyond prevention and isolation by providing organizations with the tools and insights needed to respond to email-based attack campaigns. Symantec ETDRI enhances this capability with deep visibility and analytics, enabling faster and more effective responses to targeted threats. As shown in Figure 2, Symantec ETDRI delivers unmatched intelligence by analyzing both clean and malicious emails, offering over 60 indicators of compromise (IOCs), including URLs, file hashes, and attack details.

Figure 2: The Deepest Visibility Into Advanced Email Attacks



This rich data stream can be seamlessly integrated into your Security Operations Center (SOC) via APIs, ensuring compatibility with third-party security information and event management (SIEM) and security orchestration, automation, and response (SOAR) systems. Integrating Symantec ETDRI into a broader security framework gives you a unified approach to identifying, analyzing, and neutralizing threats, strengthening an organization's resilience against evolving email-based attacks.

User Preparedness

In any security strategy, the human element is often the weakest link. Today's attackers excel at social engineering, making it difficult for users to recognize threats until it's too late. Symantec ETDRI tackles this challenge by offering robust security awareness and education tools designed to reduce risks and empower users to identify and respond to email threats effectively. By equipping users with the knowledge and skills to detect phishing attempts, Symantec ETDRI fosters a culture of security awareness, lowering the likelihood of successful attacks and strengthening an organization's overall resilience.

Introducing Symantec Messaging Gateway (SMG)

Symantec Messaging Gateway (SMG) is an on-premises email security solution, available as a virtual or physical appliance, designed to scale easily as spam volume increases. SMG ensures both inbound and outbound messaging security with a range of advanced capabilities:

Multilayer Detection Technologies

- **Business email compromise (BEC):** SMG employs advanced heuristics, a BEC scam analysis engine, sender authentication, and domain intelligence to stop URL hijacking and identity spoofing.
- **Spear phishing:** The solution defends against malicious links in spear phishing campaigns by using URL reputation filtering based on the Symantec global database, which identifies links similar to known phishing attacks.
- **Ransomware:** SMG protects users from targeted ransomware by removing zero-day document threats in Microsoft Office and PDF attachments. It strips out malicious active content, reconstructs a clean document, and sends it to the user.
- **Directory harvesting:** By leveraging Symantec global and local sender reputation databases, heuristics, and customer-specific spam rules, SMG blocks up to 99% of unwanted emails before they reach your network. Outbound sender throttling also prevents spam attacks from compromised internal users.
- **Advanced content filtering:** SMG content filtering capabilities block unwanted emails, such as newsletters and marketing content, from reaching users.

Data Loss Protection

SMG includes built-in data loss prevention (DLP) policies that safeguard company data within messages and attachments. Administrators can create flexible policies using 100 prebuilt dictionaries, patterns, and templates, ensuring automated protection and enforcement. SMG also provides automatic SMTP over TLS encryption, ensuring secure email communications in transit.

Detailed Auditing and Reporting

SMG offers a comprehensive web-based console for granular policy configuration, reporting, and monitoring. This console provides a unified view of threat trends, attack statistics, and non-compliance incidents.

- **Auditing Tools:** The solution includes a dashboard, summary, and detailed reports, with 50 customizable preset reports highlighting threat trends and potential compliance issues. Reports can be scheduled based on content and frequency.
- **SIEM Integration:** Syslog data can be exported to third-SIEM systems for further analysis and correlation.
- **User-Friendly:** The SMG graphical message-audit interface simplifies message tracking, allowing administrators to determine message disposition and delivery status quickly.

Summary

Email remains the top threat vector for organizations, serving as the primary delivery mechanism for social engineering, BEC, phishing, and ransomware attacks. Broadcom offers the industry's most comprehensive email security portfolio, combining cloud and on-premises solutions that enhance the native security features of most email platforms. Three key differentiators set this solution apart:

- **Security powered by global intelligence:** Symantec Email Security leverages insights from the Symantec Global Intelligence Network (GIN), the world's largest civilian threat intelligence network. With visibility into over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors across 157 countries, the GIN analyzes 8 billion threats daily to ensure better security outcomes.
- **Awareness to combat human error:** Symantec Email Security offers extensive security awareness tools, reducing business risks by preparing users to recognize phishing and other email attacks. Security assessments, customizable to your needs, simulate real-world threats and executive dashboards provide visibility into user behavior. Repeat assessments help track trends, ensuring employees can identify and report sophisticated threats.
- **Insights to accelerate response:** Symantec Email Security delivers deep analytics that enhance response times by offering unparalleled visibility into both clean and malicious emails. With over 60 IOCs, such as URLs, file hashes, and targeted attack data, this solution provides richer intelligence than any other vendor. API connections to third-party SIEM systems can seamlessly integrate this data into your SOC.

BROADCOM®
connecting everything®

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

Copyright © 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

SYM-Email-Security-SB100 March 5, 2025