PRODUCT BRIEF

AT A GLANCE

Symantec® Email Security.cloud offers a comprehensive solution for protecting both cloud-based email platforms.

KEY BENEFITS

- Enhanced protection against advanced threats
- Improved operational efficiency
- Cost-effective security solution
- Stronger compliance and data privacy
- Empowered user awareness

KEY FEATURES

- Advanced detection and prevention
- Threat isolation capabilities
- Comprehensive threat intelligence
- Integrated user education and analytics
- Seamless integration with security ecosystems

Email Security.cloud

Comprehensive Email Security for the Modern Threat Landscape

Overview

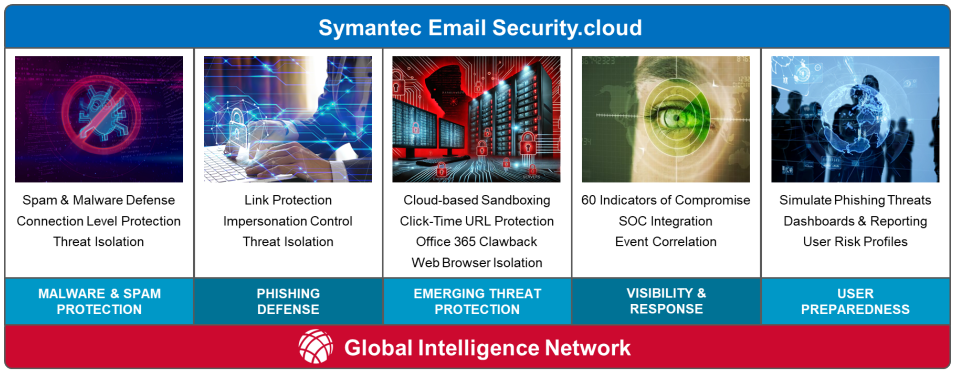
Email remains a top target for cyber attacks, exploited by criminals to deliver threats such as ransomware, business email compromise (BEC), and phishing. According to the 2024 Verizon Data Breach Investigations Report, email is the primary method for distributing ransomware and the second most common vector in breaches. The IBM 2023 Security Breach Report revealed the staggering costs of email-based attacks, averaging $4.67 million for BEC, $4.76 million for phishing, and $4.55 million for social engineering attacks.

Attackers increasingly employ sophisticated tactics like spear phishing, domain spoofing, and obfuscated links, bypassing traditional email defenses. Businesses migrating to cloud-based email systems such as Microsoft Office 365 and Google Workspace face heightened vulnerabilities as built-in security often falls short. Legacy email security solutions, limited by inadequate analytics and siloed operations, struggle to meet the demands of today's complex threat landscape. This creates gaps in protection, operational complexity, and rising risks of data leakage, compliance violations, and financial losses. Robust, integrated email security is now a necessity.

Introducing Symantec® Email Security.cloud Service (ESS)

Symantec ESS offers a comprehensive solution for protecting both cloud-based email platforms (Office 365, Google Workspace) and on-premises systems (Microsoft Exchange). Utilizing a multilayered defense, Symantec ESS blocks advanced threats such as ransomware, spear phishing, and BEC while enhancing visibility into attack campaigns with advanced analytics and integration with the Symantec Global Intelligence Network (GIN).

Figure 1: The Most Complete Protection in the Industry



This comprehensive email security solution provides end-to-end protection, starting with prevention, isolation, and response. It also emphasizes user preparation, interoperability, and compatibility to streamline the security stack and maximize return on investment.

Prevention: The First Line of Defense

The cornerstone of email security is prevention. Symantec ESS enhances the native security of email systems, effectively preventing malware and email threats with minimal false positives. Advanced detection technologies and telemetry from the GIN block sophisticated attacks such as ransomware, spear phishing, and BEC. By also filtering spam and unwanted emails, such as newsletters and marketing messages, Symantec ESS boosts user productivity while maintaining robust protection.

Malware and Spam Protection

- **Malware and spam defense:** Employ reputation analysis, antivirus engines, and antispam signatures to inspect links and attachments, effectively blocking spam and malware.
- **Connection-level protection:** Mitigate spam and malware risks by slowing and dropping anomalous SMTP connections.
- **Threat isolation:** Prevent ransomware and other malware from infecting users by isolating suspicious email attachments. This technology also isolates risky or unknown email links which host malware, keeping users and devices safe from infected downloads.

Phishing Defense

- **Link protection:** Scan links in real time before email delivery and again at the time of click, tracing them to their final destination—even when attackers use advanced evasion techniques. Advanced phishing variant detection identifies and blocks links similar to known phishing attacks.
- **Impersonation controls:** Provide strong protection against BEC and spoofing by using a sophisticated impersonation engine to block threats mimicking legitimate users or domains.
- **Threat isolation:** Open risky or unknown website links in read-only mode to keep users safe from phishing attacks.

Symantec ESS leverages global threat intelligence from the world's largest civilian global network for unparalleled visibility into the threat landscape. Telemetry from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors across 157 countries enables analysis of 8 billion threats daily, ensuring better security outcomes and proactive defense strategies.

Isolation: Enhance Prevention with Emerging Threat Detection

Symantec Email Threat Detection Response and Isolation (ETDRI), a cloud-based service, extends Symantec Email Security's capabilities by incorporating advanced technologies to neutralize email-based attacks before they can harm users or systems.

Key Capabilities

- **Cloud-based sandboxing:** Discover complex and advanced attacks with our cloud-based sandbox environment. This service employs techniques to mimic human behavior and execute suspicious files both virtually and on physical hardware to uncover attacks that evade detection by traditional sandboxing technologies.
- **Click-time URL protection:** Malicious links are blocked when they are clicked to protect users against attacks that weaponize a link after an email is delivered. This compliments real-time link following in ESS.
- **Office 365 clawback:** Move any delivered email that is later found to contain malware out of the end user's inbox.

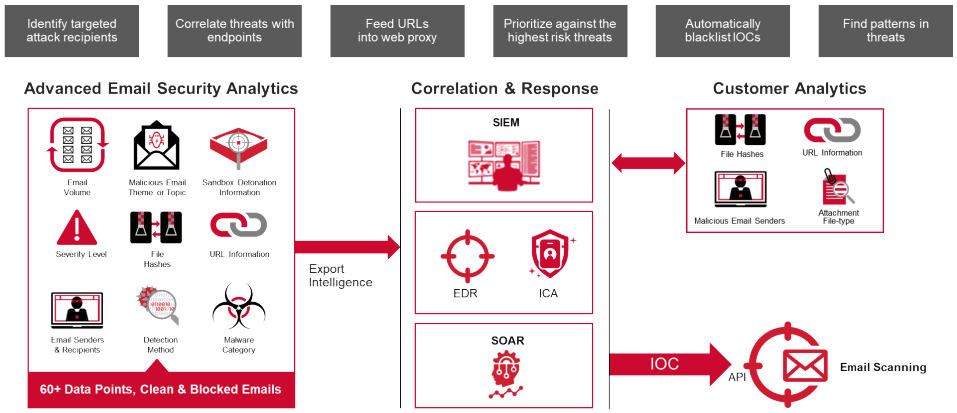
- **Web browser isolation:** Users are shielded from advanced email attacks such as spear phishing, credential theft, and ransomware by creating an insulated execution environment between users and email links, remotely rendering suspicious content and scanning potentially infected downloads before they are delivered.

Respond: Enhance Visibility and Accelerate Response

Effective email security extends beyond prevention and isolation by equipping organizations with the tools and insights needed to respond to email-based attack campaigns. Symantec ETDRI empowers this capability by providing deep visibility and analytics, enabling faster, more effective responses to targeted and advanced 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 targeted attack details.

Figure 2: The Deepest Visibility Into Advanced Email Attacks



This rich data stream can be seamlessly integrated into a Security Operations Center (SOC) through APIs, enabling compatibility with third-party Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems.

With this level of integration, organizations can accomplish the following:

- **Hunt for threats:** Analyze your environment to identify potential risks and assess the severity and scope of attacks.
- **Correlate events:** Combine insights from Symantec Endpoint Detection and Response (EDR) and Secure Web Gateway solutions to detect advanced threats across multiple control points.
- **Remediate and orchestrate responses:** Contain threats by block-listing attacks and automating responses across your security ecosystem.

By integrating Symantec ETDRI with a broader security framework, you gain a unified approach to identifying, analyzing, and neutralizing threats, ensuring your organization remains resilient against evolving email-based attacks.

User Preparation: Strengthen the Human Element

In any security strategy, the human element is often the weakest link. Attackers excel at social engineering, making it challenging for users to recognize threats until it's too late. Symantec ETDRI addresses this challenge by providing robust security awareness and education capabilities designed to reduce risks and empower users to identify and respond to email threats effectively.

Symantec ETDRI enables organizations as follows:

- **Evaluate readiness:** Simulate real-world phishing threats with customizable security assessments tailored to your organization's needs.
- **Track and benchmark progress:** Use executive dashboards and detailed reporting to gain visibility into user behavior. Repeat assessments help identify trends and measure improvements over time.
- **Prioritize protection:** Develop user risk profiles by combining insights from Symantec email security analytics with Information Centric Analytics, enabling admins to focus on the most vulnerable users.

Training notifications and educational content prepare employees to recognize and report sophisticated email attacks. By equipping users with the knowledge and skills to detect phishing attempts, Symantec ETDRI builds a culture of security awareness, reducing the likelihood of successful attacks and enhancing the overall resilience of your organization.

Interoperability and Compatibility: Seamless Integration for Enhanced Security

Streamline your security stack and maximize return on investment by integrating Symantec ESS with your broader security infrastructure, including data loss prevention (DLP), encryption controls, and endpoint, network, and cloud security solutions.

Symantec ESS enhances compliance and privacy efforts with built-in DLP and policy-based encryption controls:

- **Data loss prevention (DLP):** Flexible policies identify and control sensitive emails using over 100 predefined keyword dictionaries, regular expressions, and MIME type lists.
- **Policy-based encryption:** Confidential emails are kept private by automatically encrypting messages into password-protected PDFs for a mobile-friendly push encryption experience.

As part of the Symantec Integrated Cyber Defense Platform, Symantec ESS extends its DLP capabilities through integration with Symantec Data Loss Prevention, enabling comprehensive data protection across email, endpoint, network, cloud, mobile, and storage systems. Advanced encryption needs are met with Symantec Policy-Based Encryption Advanced, a customizable cloud-based add-on service that enables administrators to establish flexible, policy-driven encryption rules to protect information in alignment with organizational compliance requirements. With this hosted solution, organizations can quickly deploy robust encryption capabilities to secure sensitive data shared via email without the complexity of managing digital certificates or encryption keys.

The solution also integrates seamlessly with other Symantec products to bolster security across endpoints, web, and messaging applications. When used with Symantec Endpoint Security, email intelligence gathered from emerging threats can be distributed as blocklists to endpoints, preventing

infections across an organization. This compatibility extends protection to modern collaboration and messaging platforms—both cloud-based and on-premises—including Slack, Salesforce, and Box, ensuring a cohesive and fortified security posture.

By uniting email security with your existing security ecosystem, Symantec ESS simplifies management, enhances threat response, and strengthens protection across all digital touchpoints.

Summary

Symantec ESS offers unparalleled protection against sophisticated email threats by integrating advanced detection, isolation, analytics, and user education. This solution empowers organizations to stay ahead of evolving cyber risks while seamlessly integrating into broader security ecosystems to enhance compliance, reduce operational complexity, and fortify overall security posture.

With high effectiveness, strong accuracy, and industry-leading SLAs, Symantec ESS is easy to deploy, operate, and scale as messaging volume grows. Backed by the Symantec Integrated Cyber Defense Platform, it provides unmatched protection, operational efficiency, and a low total cost of ownership, making it the ideal choice for safeguarding your email infrastructure against even the most advanced attacks.

BROADCOM®
connecting everything®

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

SED-email-security-cloud-PB102 February 6, 2025