PRODUCT BRIEF

Symantec® Email Security.cloud

Complete Email Security for the Cloud Generation

AT A GLANCE

- **Accurately defend against ransomware, BEC and emerging threats.**
  Stop new and sophisticated threats such as ransomware, spear phishing, and business email compromise with the most effective and accurate email security.
- **Stop spear phishing with comprehensive defense.**
  Shield your organization from spear phishing through a comprehensive defense that includes multiple layers of protection, strong isolation, deep visibility, and dynamic security awareness.
- **Accelerate your threat response with Integrated Cyber Defense.**
  Contain attacks and orchestrate response across endpoint security and web gateways by remediating attacks, block-listing threats, and correlating security analytics.
- **Ensure safe cloud adoption with the industry's strongest controls.**
  Fully secure Office 365 and G Suite through Symantec® Email Security.cloud, Cloud Access Security Broker (CASB), and Data Loss Prevention solutions.

Critical and Challenging Role of Email Security

Why is email still a threat vector of concern? Email is a common way for cyber criminals to launch and distribute threats. According to the 2023 Data Breach Investigations Report, Verizon, email is the top action vector for delivering ransomware, and email was the second most used action vector in both breaches and incidents. In the 2022 Internet Crime Report, the FBI explains that business email compromise (BEC) accounted for $2.7 billion of reported losses, representing 26% of all the reported losses experienced from cyber crime.[1]

As the volume of these attacks has increased, so has the level of sophistication. Advanced and zero-day threats are much more difficult to detect and stop than traditional malware, while standard signature-based antimalware tools have proven largely ineffective against them. Attackers now favor targeted spear phishing, especially in the form of BEC scams. These elusive and dangerous targeted attacks use sophisticated methods including domain spoofing and obfuscation of malicious links embedded in email messages.

At the same time, businesses are migrating their email from on-premises servers to cloud-based systems such as Microsoft Office 365 and Google G Suite. Unfortunately, the basic, built-in security of these systems cannot fully protect against email threats. Traditional email security solutions do not work either. Their rudimentary defenses fail to block new and sophisticated attacks, and their siloed approach to security allows advanced threats to slip through the cracks. Both types of security give organizations limited visibility and provide only basic analytics, which makes it harder to respond to threats.

Further complicating the landscape, vendors offer myriad point products that address only part of the security problem. These disjointed products—for email security, data loss prevention (DLP), endpoint protection, web security, and more—require costly, custom integrations and high management overhead. And again, a patchwork defense is leaky. Add in a shortage of trained IT security personnel and organizations end up with increased operational complexity and greater vulnerability.

Finally, as users increasingly share sensitive information over email, organizations are struggling to keep confidential data from being exposed. Data leakage undermines an organization's ability to meet its legal and compliance requirements. And it can result in damaged brand reputations, regulatory fines, and ultimately, financial losses.

1. 2022 Internet Crime Complaint Center (IC3) Annual Internet Crime Report, hosted on the IC3 website: www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Shut Down a Critical Threat Vector

Symantec Email Security.cloud is a complete email security solution that safeguards cloud email such as Office 365 and G Suite and on-premises email such as Microsoft Exchange. It blocks new and sophisticated email threats such as ransomware, spear phishing, and BEC with a multilayered defense and insights from the world's largest civilian global intelligence network.

Symantec Email Security.cloud repels spear phishing attacks with comprehensive defense that includes protection, isolation, visibility, sender authentication and user awareness. It also accelerates attack response with analytics that provide deep visibility into targeted attack campaigns. Symantec Information Centric Analytics correlates email, other security streams, and user behavior analytics to give even deeper visibility.

Finally, Email Security.cloud is part of the Symantec Integrated Cyber Defense Platform, which covers endpoint and web security, threat analytics, security orchestration and automation, and more.

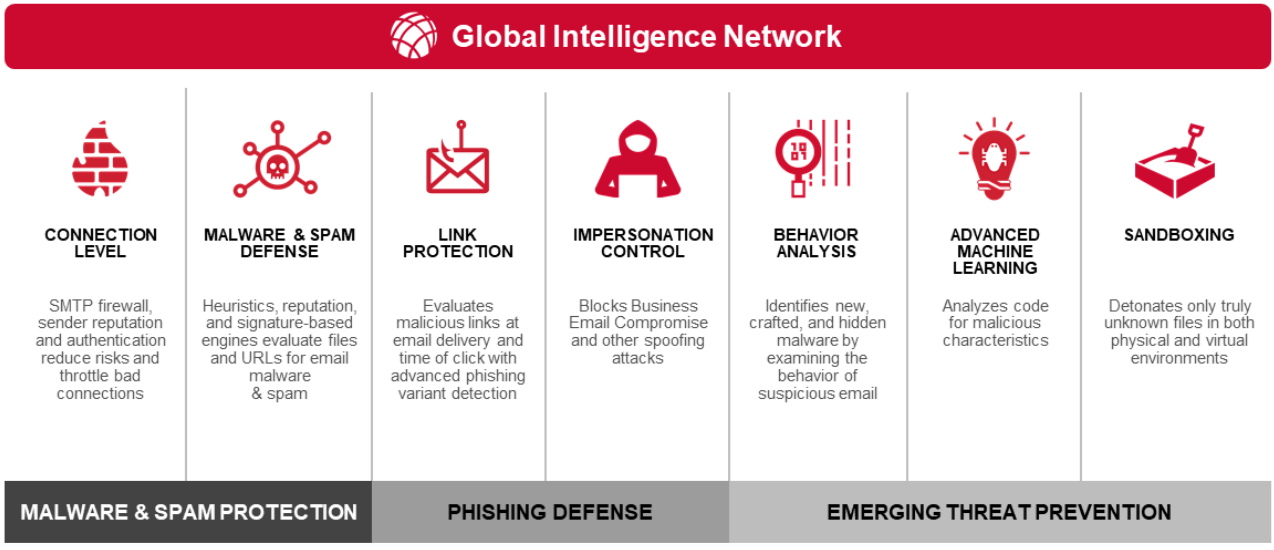
Prevent

Symantec Email Security.cloud supercharges the built-in security of cloud and on-premises email systems by preventing the most malware and email threats with the fewest false positives. This cloud-based solution repels sophisticated email attacks such as ransomware, spear phishing, and BEC with multiple, advanced detection technologies and telemetry from the Symantec Global Intelligence Network. It also improves user productivity by blocking spam and other unwanted email such as newsletters and marketing emails.

Emerging Threat Prevention

- **Sandboxing** uncovers targeted and advanced attacks by executing unknown files in physical and virtual environments. This helps catch 'virtual machine-aware' attacks, which are threats that do not exhibit suspicious behavior in virtual environments. The Symantec sandbox mimics human behavior to draw out attacks that appear malicious only in the presence of humans. In addition, our sandbox uses machine learning to detect stealthy, persistent threats by analyzing code for suspicious characteristics. And it utilizes network traffic analysis to identify malware that call command-and-control servers.
- **Behavior analysis** blocks new, crafted, and hidden ransomware by examining all email characteristics including delivery behavior, message attributes, attachments, and social engineering tricks. It also blocks new ransomware variants by determining if an email contains reused malicious code. Finally, it uses file decomposition techniques to spot and extract hidden ransomware within attachments.

Figure 1: The Most Complete Protection in the Industry



Phishing Defense

- **Link protection** probes and evaluates links in real time before email delivery and again at the time of click—unlike traditional email security solutions that rely on reactive block lists or signatures to block only known spear phishing links. Link protection follows links to their final destination, even when attackers try to bypass detection with sophisticated techniques. Moreover, because cyber criminals often reuse code in new attacks, we use advanced phishing variant detection to sniff out and block spear phishing links that are similar to known phishing attacks.
- **Impersonation controls** provide the strongest protection against BEC and other spoofing attacks by using a sophisticated impersonation engine to block threats that masquerade as a specific user or legitimate email domain in your organization.
- **Threat isolation** opens risky or unknown website links in read-only mode to keep users safe from phishing attacks.
- **Fraud protection** automates sender authentication by ensuring that your email domain can not be impersonated, in turn eliminating the risk of fraud for internal and external recipients.

Malware and Spam Protection

- **Malware and spam defense** stops spam and malware by inspecting links and attachments with technologies such as reputation analysis, antivirus engines, and antispam signatures.
- **Connection-level protection** reduces the risk of spam and malware by slowing and dropping anomalous SMTP connections.
- **Threat isolation** prevents 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.

Symantec Global Intelligence Network

Threat intelligence from the world's largest civilian network provides global visibility into the threat landscape and helps ensure better security outcomes. 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 and by analyzing 8 billion threats every day.

Isolate

Symantec Email Threat Isolation shields users from advanced email attacks such as spear phishing, credential theft, and ransomware by isolating suspicious links and attachments while stopping credential theft by safely rendering risky web pages. Email threat isolation takes prevention up a notch by creating an insulated execution environment between users and their email links, rendering suspicious links remotely and showing only inoculated web content to users, while scanning potentially infected downloads before delivery. Therefore attacks meant to be delivered via malicious links are simply neutralized.

Credential phishing attacks are also stopped with Symantec Email Threat Isolation. When a suspected phishing website is opened via an email link, the site is rendered in read-only mode, which prevents users from entering sensitive information such as corporate passwords.

Thirdly, advanced attacks that use attachments which link to ransomware and other malware are stopped from infecting users by isolating email attachments. When a potentially risky attachment is found, email threat isolation capabilities render these documents in a secure remote environment, which creates a virtual *air gap* between files and user devices. As a result, ransomware and other advanced attacks that hide malware in email attachments cannot infect users.

- Prevent spear phishing attacks by isolating malicious links and downloads
- Stop credential theft by safely rendering webpages in read-only mode
- Prevent ransomware and other malware from infecting users by isolating email attachments

Respond

Symantec Email Security.cloud accelerates attack response with analytics that provide the deepest visibility into targeted and advanced attack campaigns. This intelligence includes insights into both clean and malicious emails, and provides more Indicators of Compromise (60+ data points including URLs, file hashes, and targeted attack information) than any other vendor. This can all be streamed to your Security Operations Center through API integration with third-party Security Information and Event Management (SIEM) systems,Symantec Information Centric Analytics or Symantec Integrated Cyber Defense Exchange.

Respond (cont.)

This enables you to hunt for threats across your environment and quickly determine an attack's severity and scope. When used alongside Symantec Endpoint Detection and Response and the Secure Web Gateway family to detect advanced threats, you can automatically correlate events across all control points. You can then remediate threats and orchestrate response by containing attacks and block-listing attacks across your security environment.

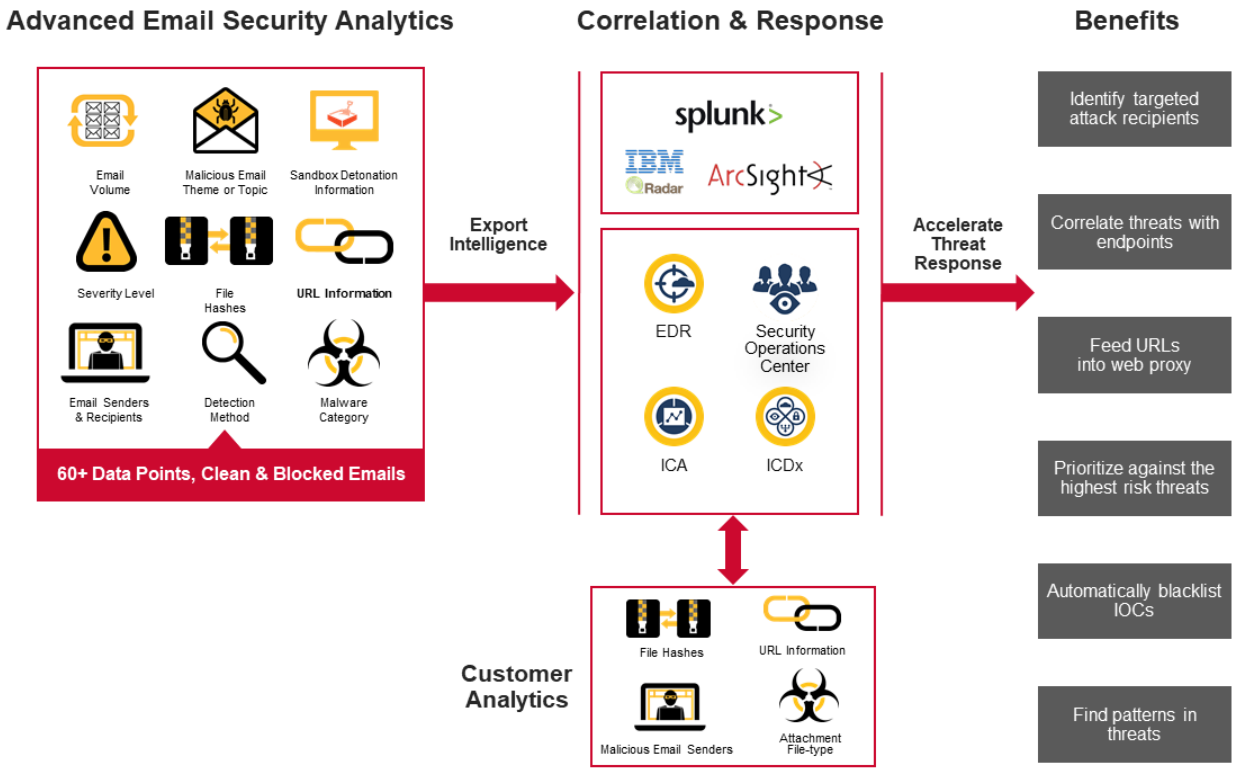
- Accelerate your attack response
- Hunt threats across your environment
- Remediate threats and orchestrate your response

Prepare

Symantec Email Security.cloud provides broad security awareness and education capabilities that reduce business risks by preparing users to recognize phishing attacks and helping organizations prioritize protection for the most vulnerable users. Evaluate employee readiness with security assessments that mimic real-world threats, which can be easily customized to meet the needs of your organization. Executive dashboards and detailed reporting help benchmark your organization's security awareness by giving visibility into user behavior and repeat assessments identify key trends by comparing results to previous evaluations. Admins can even develop user risk profiles and prioritize risky users by combining these insights with Symantec email security analytics or correlating user behavior using Information Centric Analytics. This security awareness and education prepares employees to recognize and report email attacks with training notifications that teach users to spot the latest, sophisticated email attacks.

- Assess employee readiness with real-world simulations
- Track progress with repeat assessments and detailed reporting
- Educate users to recognize email attacks

Figure 2: The Deepest Visibility Into Advanced Email Attacks



Integrate

Simplify your security stack and increase return on investment by integrating email security with the rest of your security infrastructure, including DLP and encryption controls as well as endpoint, network, and cloud security.

Symantec Email Security.cloud prevents data leakage and helps meet compliance and privacy requirements with built-in DLP and policy-based encryption controls. Flexible DLP policies identify and control sensitive emails with over 100 pre-defined lists of keyword dictionaries, regular expression, and MIME type lists. Policy-based encryption controls keep confidential emails private by automatically encrypting emails via a password-protected PDF for a mobile-friendly "push" encryption experience.

Email Security.cloud is a part of the Symantec Integrated Cyber Defense Platform, so its built-in DLP controls are strengthened through integration with Symantec Data Loss Prevention, which prevents data loss across your entire environment—email, endpoint, network, cloud, mobile, and storage systems. Moreover, you can meet advanced encryption needs and get customizable branding with Symantec Policy-Based Encryption Advanced, a cloud-based add-on service.

Symantec Email Security.cloud also integrates with other Symantec products to protect endpoints, web, and messaging apps, which strengthen your overall security posture. Use it with Symantec Endpoint Security to accelerate your response to emerging threats. For example, intelligence gathered from threats in the email channel can be pushed out as block lists to all endpoints, preventing infection across your environment. This extends protection to the latest collaboration and messaging apps—in the cloud and on premises—such as Slack, Salesforce, and Box.

Add-ons to Symantec Email Security.cloud

The core Symantec Email Security.cloud offers enhanced protection through the following add-ons:

- **Email Threat Detection Response and Isolation:** Protects against advanced threats while providing deep visibility and rapid response to targeted attack campaigns. This add-on also includes Phishing Readiness security awareness training capabilities. Isolation allows you to open suspicious email links and attachments in an isolated container, allowing users to interact with potentially risky websites, files, and downloads while blocking malware or phishing attacks.
- **Email Fraud Protection:** Simplifies the process of achieving and maintaining sender authentication enforcement by using automation to support various standards (for example, DMARC, DKIM, SPF).

Gain High Operational Efficiency at a Low TCO

Symantec Email Security.cloud is easy to deploy and operate, and scales quickly as messaging volume grows. When you add up its high effectiveness and accuracy, strong SLAs, and the Symantec Integrated Cyber Defense Platform, your organization will decrease operational complexity, enjoy a lower total cost of ownership, and get unmatched protection from even the most sophisticated email attacks.

BROADCOM
connecting everything®

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

SED-email-security-cloud-PB101 November 30, 2023