Symantec Email Security.cloud

Complete Email Security for the Cloud Generation

At a Glance

Block ransomware and emerging threats with the highest effectiveness and accuracy

- 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 and blacklisting threats.

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.

The critical and challenging role of email security

Why is email today's No. 1 threat vector? Email is ubiquitous, impersonating a credible sender is simple, unaware users are easily fooled, and email attacks make cybercriminals a lot of money with little effort. Where once we were concerned with basic spam and phishing emails, now we're on guard for highly targeted and sophisticated attacks including spear phishing, ransomware, and business email compromise (BEC).

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 don't 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.

Shut down the No. 1 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 business email compromise with a multilayered defense and insights from the world's largest civilian global intelligence network. And it does all this with the industry's **highest effectiveness and accuracy.**

Email Security.cloud repels spear phishing attacks with comprehensive defense that includes protection, isolation, visibility, and user awareness. It also accelerates your attack response with analytics that provide the deepest visibility into targeted attack campaigns. In addition, Symantec keeps your email secure and confidential with built-in, granular DLP and encryption controls, as well as tight integration with Symantec Data Loss Prevention.

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.

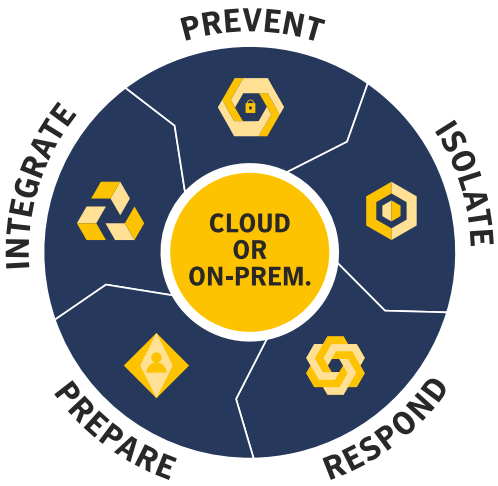

Figure 1

Prevent

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 business email compromise 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. Email Security.cloud is backed by the industry's strongest service-level agreements: 100 percent virus protection, more than 99 percent spam filtering, and 100 percent email uptime.

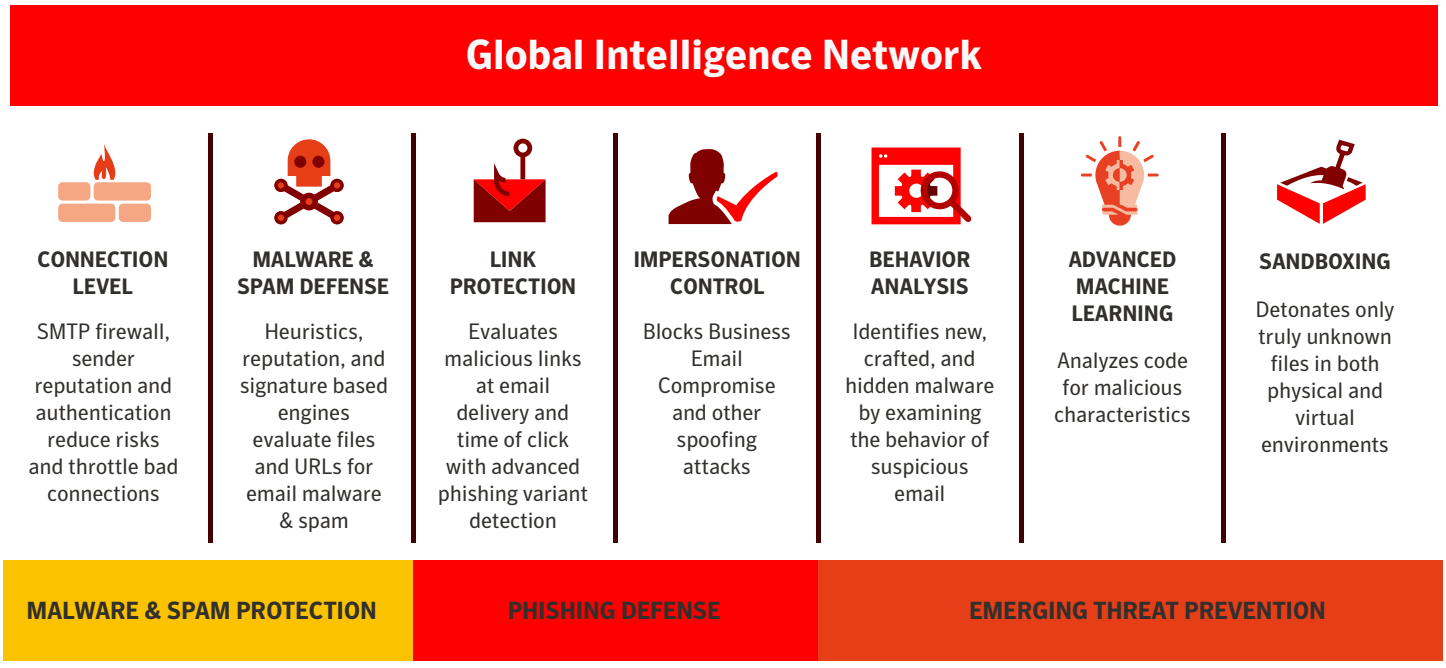

Figure 2: Symantec: Most Complete Protection In The Industry

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 don't 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.

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 blacklists 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.

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.

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. It is powered by telemetry from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors in 157 countries.

Isolate

Symantec is the first and currently only vendor to offer email threat isolation capabilities, giving our customers unparalleled protection from sophisticated email attacks. No other vendor can match this level of security.

Email Security.cloud shields users from spear phishing, ransomware, and other advanced email attacks 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. Attacks meant to be delivered via malicious links simply cannot be delivered.

In addition, Symantec shields trusted applications from weaponized documents through attachment isolation, which is available through the Symantec Endpoint Protection Hardening add-on. These capabilities run trusted applications in 'castle mode' to prevent weaponized documents from performing suspicious behavior.

Symantec also stops credential phishing with email threat isolation capabilities. 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.

- Prevent spear phishing attacks by isolating malicious links.
- Shut down ransomware by shielding trusted applications from weaponized attachments.
- Stop credential theft by safely rendering webpages in read-only mode.

Respond

Email Security.cloud accelerates your 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 (SOC) via integrations with third-party Security Information and Event Management (SIEM) systems and Symantec Managed Security Services. This enables you to hunt for threats across your environment and quickly determine an attack's severity and scope.

When you add Symantec Advanced Threat Protection endpoint or network modules, you can automatically correlate events across all control points. This enables you to quickly prioritize the most critical threats. You can then remediate threats and orchestrate response by containing attacks and blacklisting attacks across your security environment.

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

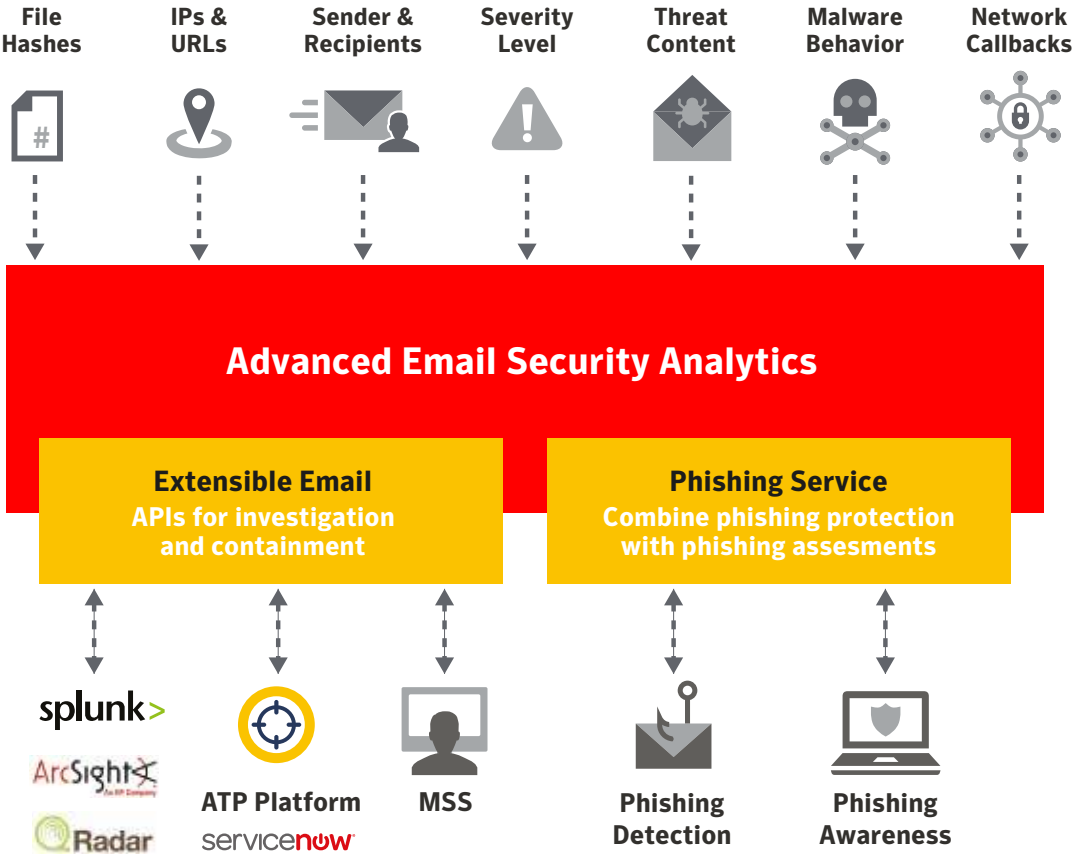

Figure 3: Symantec Provides the Deepest Visibility Into Advanced Email Attacks

Prepare

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. You can 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. 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.

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.

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.

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 blacklists to all endpoints, preventing infection across your environment. And Symantec extends protection to the latest collaboration and messaging apps—in the cloud and on premises—such as Slack, Salesforce, and Box.

Gain high operational efficiency at a low TCO

After nearly two decades of continuous improvement, Email Security.cloud now offers the industry's **most effective (98.77% blocked) and accurate (0.00% false positives)** email security. It is also the most dependable cloud email security service: We back it with broad **service level agreements (SLAs)** that demonstrate our commitment to you. We monitor these SLAs using an aggressive set of metrics. For complete transparency, **we continually publish and measure our performance** against these SLAs—and we pay out a service credit if we don't meet performance targets.

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, our 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.

Threatscape

Want to find out more?

To learn more, contact us via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland)

Symantec

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

18D151302_ds_Cloud_Email_Security.indd