Product Brief

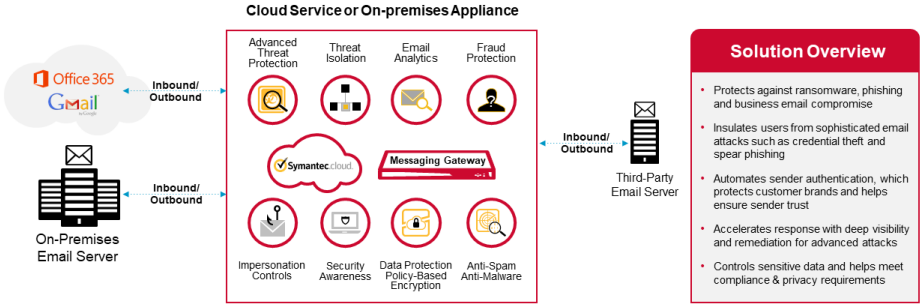
Email Security for the Enterprise

Multilayered Email Defense for the Cloud Generation

Table of Contents

Cloud Generation Email Security Portfolio

Figure 1: Advanced Policy Based Encryption



Facing the Challenges of Securing the Cloud Generation

Intelligent, across-the-board email security—whether for on-premises, cloud-based, or hybrid email systems—begins with a clear, realistic understanding of what you're up against. Email is the most common way for cyber criminals to launch and distribute threats. According to the 2020 Data Breach Investigations Report, Verizon, most malware is delivered through email, with 46% of organizations getting almost all their malware this way. The 2019 Internet Crime Report, FBI shows that Business Email Compromise (BEC) accounted for half the reported losses experienced from all cyber crime ($1.77Bn).

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 business email compromise (BEC) scams. These elusive and dangerous targeted attacks use sophisticated methods including domain spoofing and obfuscation of malicious links embedded in email messages.

The losses from these attacks amounted to $26Bn in July 2019, over double the losses reported in May 2018.[1]

High-value targets, such as executives or finance teams, are most at risk as they typically have access to sensitive data and systems. Moreover, users unaware of email threats are susceptible to advanced attacks, which increases security risks for their organization.

The rapid adoption of Microsoft Office 365 and Google G Suite is transforming the way IT departments deliver messaging services to their organizations. Compared to traditional on-premises email, such cloud-based email services cut costs significantly by lowering operational overhead. And both providers point out that their email comes with included malware and spam protection. But how complete and effective are these built-in capabilities? What security issues should you consider as your organization prepares to migrate to cloud-based email?

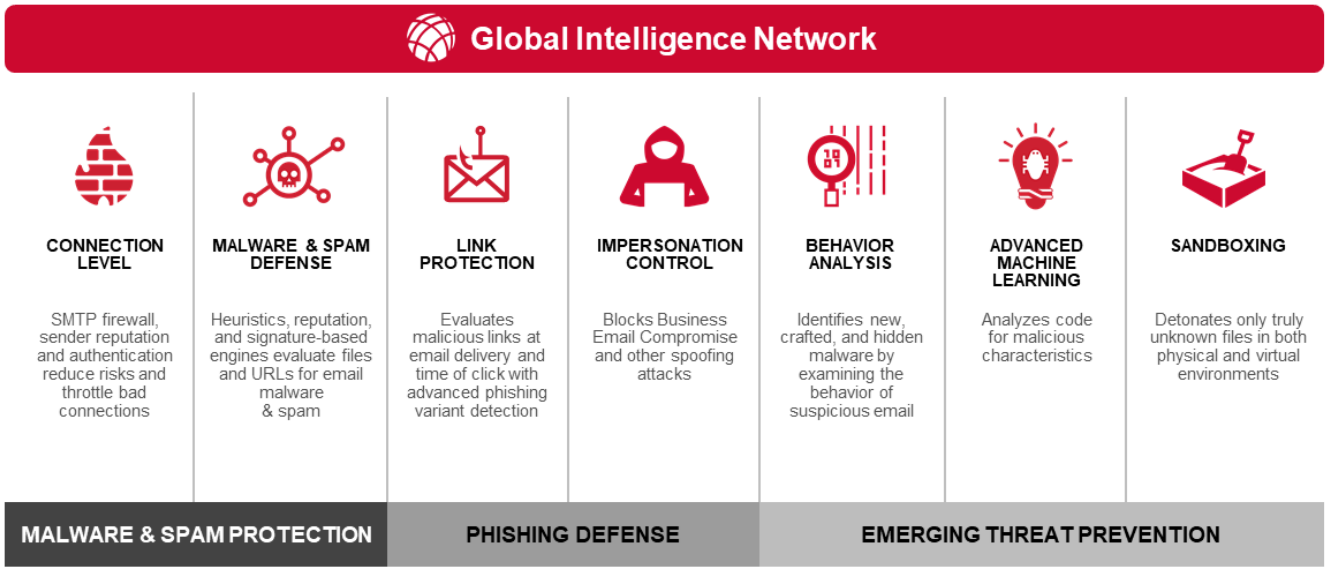
Organizations are having a hard time piecing together a complete, integrated email security solution out of multiple point products that solve only a portion of the email security problem. Worse, most email security solutions do not integrate with the rest of your security infrastructure (such as endpoint security, network security, SIEMs, and SOCs), leaving the burden of a complex integration to IT security teams. All the above, combined with a shortage of trained IT security talent, leaves organizations with operational complexity, gaps in their security architecture—and vulnerable to sophisticated multivector attacks.

Finally, organizations are struggling to prevent sensitive data from being exposed as users share sensitive information over email. This data must be kept secure and private to meet security, legal, and compliance requirements. Exposure can result in damaged brands and reputations, regulatory fines, and, ultimately, financial losses.

Gain the Most Complete Protection in the Industry

The Symantec™ Enterprise Division provides the industry's most complete cloud and on-premises email security portfolio. This protection comprises multiple layers of security technologies. And it is powered by insights from the world's largest civilian threat intelligence network, the Symantec™ Global Intelligence Network (GIN), which offers visibility into the threat landscape worldwide. 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. Symantec email security is part of our Integrated Cyber Defense Platform, covering and integrating Web, endpoint, and email security, threat analytics, security orchestration and automation, and more.

Figure 2: Worldwide Visibility into the Threat Landscape

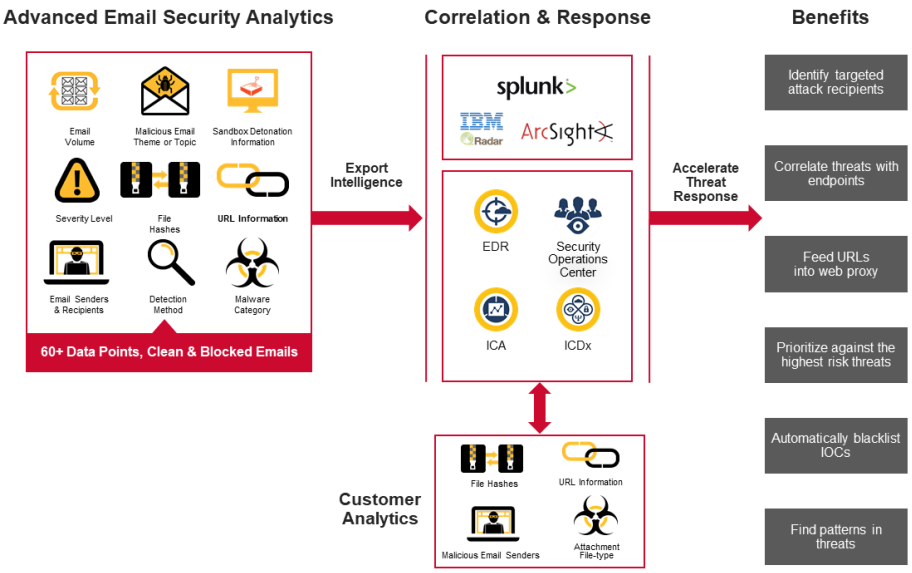


Symantec™ Email Security Capabilities

The Symantec email security portfolio enables you to:

- **Prevent evolving and zero-day threats**
  - Block spam, malware, and advanced email threats such as spear phishing, ransomware, and business email compromise by leveraging multilayered defense that includes machine learning, behavioral analysis, and impersonation controls. Multiple scanning engines stop unwanted email such as spam, newsletters, and marketing emails.
  - Prevent the most complex, persistent email threats with virtual machineaware sandboxing and payload detonation powered by advanced machine learning, network traffic analysis, and behavioral analysis.
  - Block advanced phishing attacks, which weaponize a link after an email is delivered. Link protection probes and evaluates links in real time, both before email delivery and at the time of click. 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.
- **Isolate email links and attachments for the ultimate protection**
  - Defend users from spear phishing and advanced attacks with the industry's first email threat isolation technology; remotely execute and render suspicious Web links in a secure execution environment while scanning downloads from these sites before they're delivered to the user's device.
  - Prevent credential theft by rendering suspicious websites in read-only mode, which stops users from submitting sensitive data such as corporate passwords.
  - Stop ransomware and other malware hidden in files from infecting users by isolating suspicious email attachments in a secure remote environment.
- **Respond quickly to security threats**
  - Act on the deepest visibility into targeted and advanced email attacks with detailed reporting on every incoming malicious and clean email scanned: 60+ data points such as URLs, file hashes, sender/recipient data, and targeted attack information.
  - Accelerate response to targeted and advanced attacks with rich threat intelligence exported to your Security Operations Center through API integration with third-party SIEMs, Symantec Information Centric Symantec Information Centric Analytics or Symantec Integrated Cyber Defense Exchange.
  - Correlate email, endpoint, Web and other security control points alongside user behavior to fully understand the highest risks you face in order to prioritize the right response.

Figure 3: Quick Response to Security Threats



- **Prepare users to avoid threats with security awareness and training**
  - Evaluate employee readiness to detect phishing attacks with security assessments that mimic real-world threats; assessments can be customized to meet the needs of your organization, and match the evolving threat landscape.
  - Track progress of employee security awareness over time with repeated assessments and detailed reporting.
  - Create user risk profiles by combining assessment results with email security analytics.
- **Protect sensitive data in email**
  - Protect sensitive data and address legal and compliance requirements with built-in data loss prevention controls; enforce regulatory compliance and prevent data leakage by choosing from an extensive list of prebuilt, easily customizable templates.
  - Safeguard the security and privacy of confidential email with policy-based encryption controls that automatically encrypt specific outbound email.
- **Integrate with Symantec and IT security ecosystem**
  - Symantec Email Security is an integral part of the Symantec Integrated Cyber Defense Platform, which delivers complete multichannel protection—threat analysis, blocking, remediation, and more—across Web, endpoint, email, and cloud apps; backed by the Symantec GIN telemetry feeds aggregated and distilled from Symantec products.
  - Tight integration with Symantec Data Loss Prevention provides an email channel enforcement point for data protection policies.
  - Extensive API library enables integration with third-party SIEM and IT ticketing tools, enhancing security operation processes for maximum efficiency and an orchestrated response.

Symantec™ Email Security Products

Symantec Email Security.cloud
Symantec Email Security.cloud is a complete email security solution that safeguards cloud email, such as Microsoft Office 365 and Google Gmail, as well as on-premises email such as Microsoft Exchange.

It blocks new and sophisticated email threats such as ransomware, spear phishing, and business email compromise through a multilayered defense and insights distilled from the world's largest civilian threat intelligence network. When combined with Symantec Email Threat Isolation and Email Threat Detection and Response, it offers the strongest protection against spear phishing attacks with comprehensive defense that includes link protection, isolation, threat visibility, and user awareness training. Moreover, Symantec Email Fraud Protection enables organizations to automate Sender Authentication using DMARC, protecting all recipients from impersonation attacks.

In addition, advanced email security analytics provides deep visibility into targeted attack campaigns, with further context available when integrated into Symantec ICDx. Integrated DLP and encryption controls keep your business email secure and confidential.

In our testing, Symantec Email Security.cloud offers the highest effectiveness and accuracy of any email security on the market today—it blocks the most threats with the fewest false positives.[2]

Learn more about Symantec Email Security.cloud.

Symantec Messaging Gateway
On-premises messaging isn't going away any time soon thanks to strict industry regulations, data sovereignty, and company mandates to retain complete control over email infrastructure. For many organizations, security solutions for on-premises email are just as important as they are for cloud-delivered email.

Symantec Messaging Gateway provides inbound and outbound on-premises messaging security that includes powerful protection against the latest messaging threats and built-in data protection capabilities to keep your email secure and confidential. It catches 99+ percent of spam, registers fewer than 1 in 1 million false positives, and effectively responds to new messaging threats with real-time automatic antispam and antimalware updates. Messaging Gateway integrates with Symantec Content Analysis to deliver advanced protection against malicious files, and with Symantec Web Isolation for additional levels of link and attachment protection.

Learn more about Symantec Messaging Gateway.

Symantec Email Fraud Protection
Symantec Email Fraud Protection is a cloud-based service that provides additional protection against Business Email Compromise and other fraudulent email attacks. The service simplifies and automates compliance with email sender authentication standards, helping you achieve DMARC enforcement and protecting your email brand(s) from being used fraudulently.

Learn more about Symantec Email Fraud Protection

Symantec Email Threat Detection and Response
Symantec Email Threat Detection and Response adds advanced detection technologies such as cloud-based sandboxing and click-time URL protection to the Symantec Email Security.cloud service. In addition, it supplies Email Security Analytics on over 60+ data points for both clean and malicious email to equip security teams to proactively find threats and remediate them faster. With the included Symantec Phishing Readiness module you can assess and educate your staff about the risks of email attacks.

Advanced Threat protection capabilities can also be added to the Symantec Messaging Gateway by integrating it with Symantec Content Analysis System.

Learn more about Symantec Email Threat Detection and Response

Symantec Email Threat Isolation
Symantec Email Threat Isolation insulates users who click on email links to risky or uncategorized Web pages. By isolation such Web pages, ransomware and other malware attacks are prevented, and read-only protection stops spear phishing and credential theft. Risk email attachments can also be opened in an isolated container to reduce malware risk. Email Threat Isolation is simple to administer as security policies are set using Symantec threat intelligence and this capability is available for both cloud and on-premises solutions.

Learn more about Symantec Email Threat Isolation

Symantec Policy Based Encryption Advanced
Symantec Policy Based Encryption Advanced (PBE Advanced) extends the Data Protection policies available in Symantec Email Security.cloud or Symantec Messaging Gateway. Using PBE Advanced, your organization's email can be analyzed, and based on your policies certain email messages will be encrypted (for example based on key words or credit card information). Several delivery methods are available that enable recipients to read encrypted emails.

Learn more about Symantec Policy Based Encryption Advanced

To learn more about Symantec's email security solutions, visit
www.broadcom.com/products/cyber-security/network/messaging-security

About Symantec Enterprise Division

Broadcom's Symantec Enterprise Division, the global leader in cyber security, helps organizations and governments secure identities and information wherever they live. Organizations across the world look to Broadcom's Symantec Enterprise Division for strategic, integrated solutions to defend against sophisticated attacks across endpoints, identities, and infrastructure, whether on-premises, in the cloud, or both. For additional information please visit www.broadcom.com/symantec or subscribe to our blogs.

1 FBI, Public Service Announcement,Alert Number: I-071218-PSA, https://www.ic3.gov/Media/Y2018/PSA180712, July 2018, and FBI, Public Service Announcement, Alert Number: I-091019-PSA, https://www.ic3.gov/Media/Y2019/PSA190910, September 2019

2 Symantec Blog: "Independent Tests Prove Effectiveness of Symantec's Email Security" February 19, 2019

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-email-security-PB100 October 27, 2020