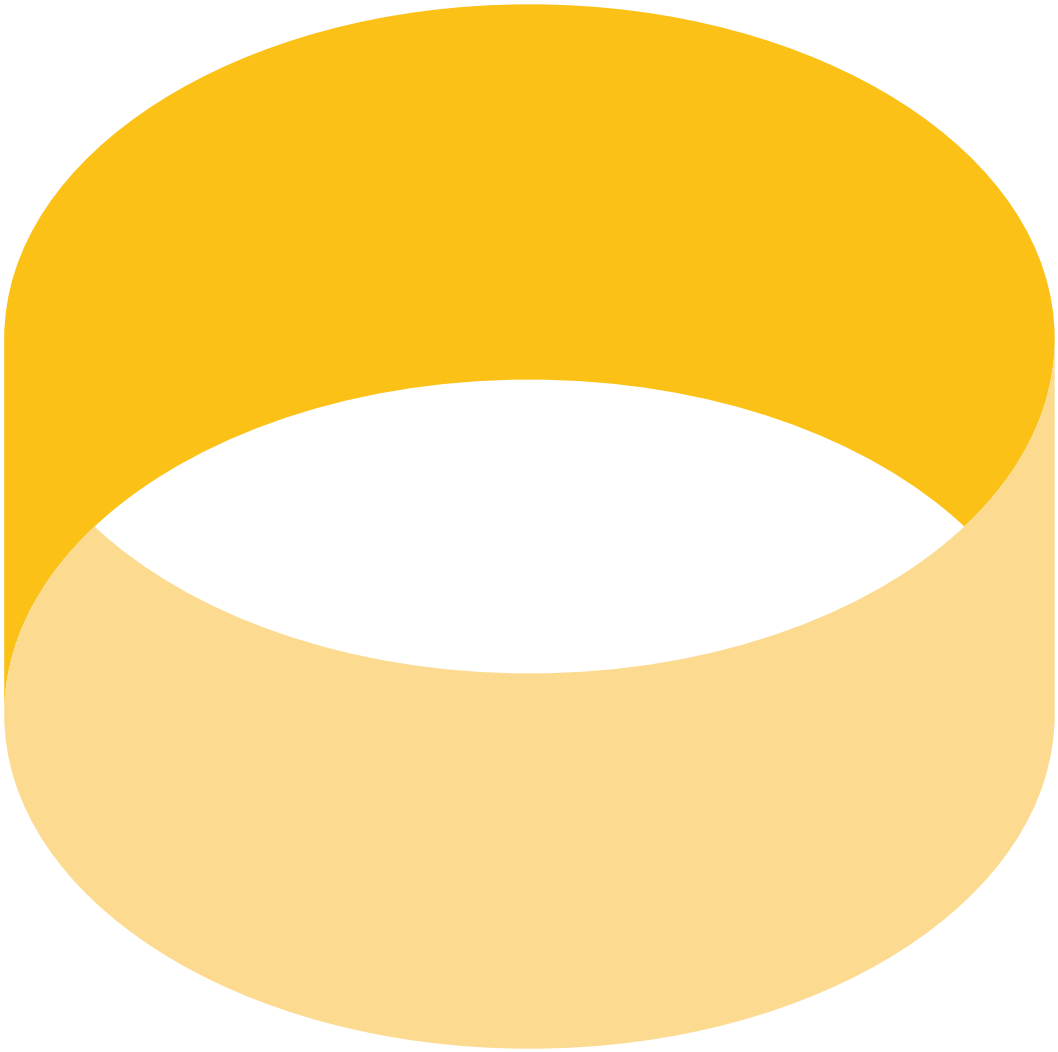


Email Security for the Enterprise

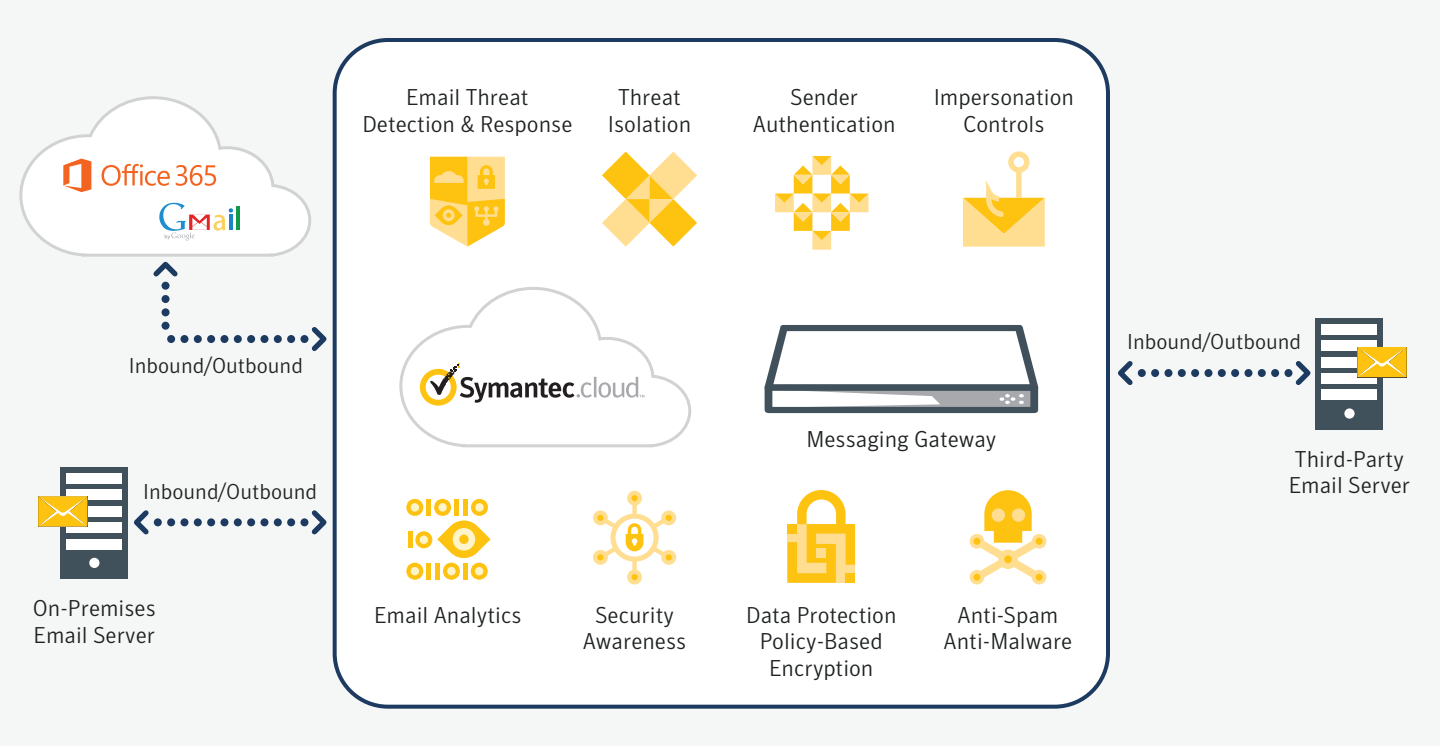
Multilayered Email Defense for the Cloud Generation

FAMILY BROCHURE

Symantec™

Cloud Generation Email Security Portfolio

Cloud Service or On-premises Appliance



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 2018 Symantec™ Internet Security Threat Report (ISTR), in 2017 one out of every 412 emails contained a malware attack, 7,710 organizations are hit by a Business Email Compromise Attack every month, and spear-phishing is the most widely used infection vector, being used by 71 percent of targeted attack groups.

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 now stands at $12.5bn and grew by 136% over 17 months[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.

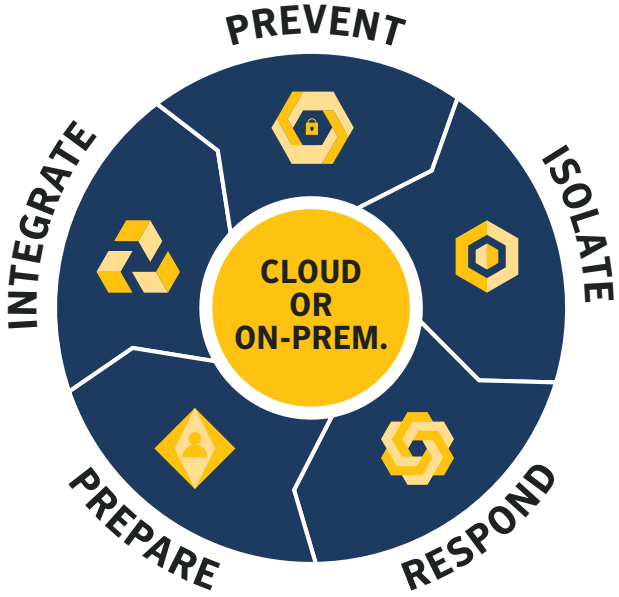
The rapid adoption of Microsoft Office 365 and Google G Suite is transforming the way IT departments deliver messaging services to their organizations. Compared to traditional on-premises email, such cloud-based email services cut costs significantly by lowering operational overhead. And both providers point out that their email comes with free 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 and even financial destruction.

Gain the most complete protection in the industry

Symantec 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. 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.



Symantec Email Security: Capabilities

The Symantec email security portfolio enables you to:

Prevent evolving and zero-day threats

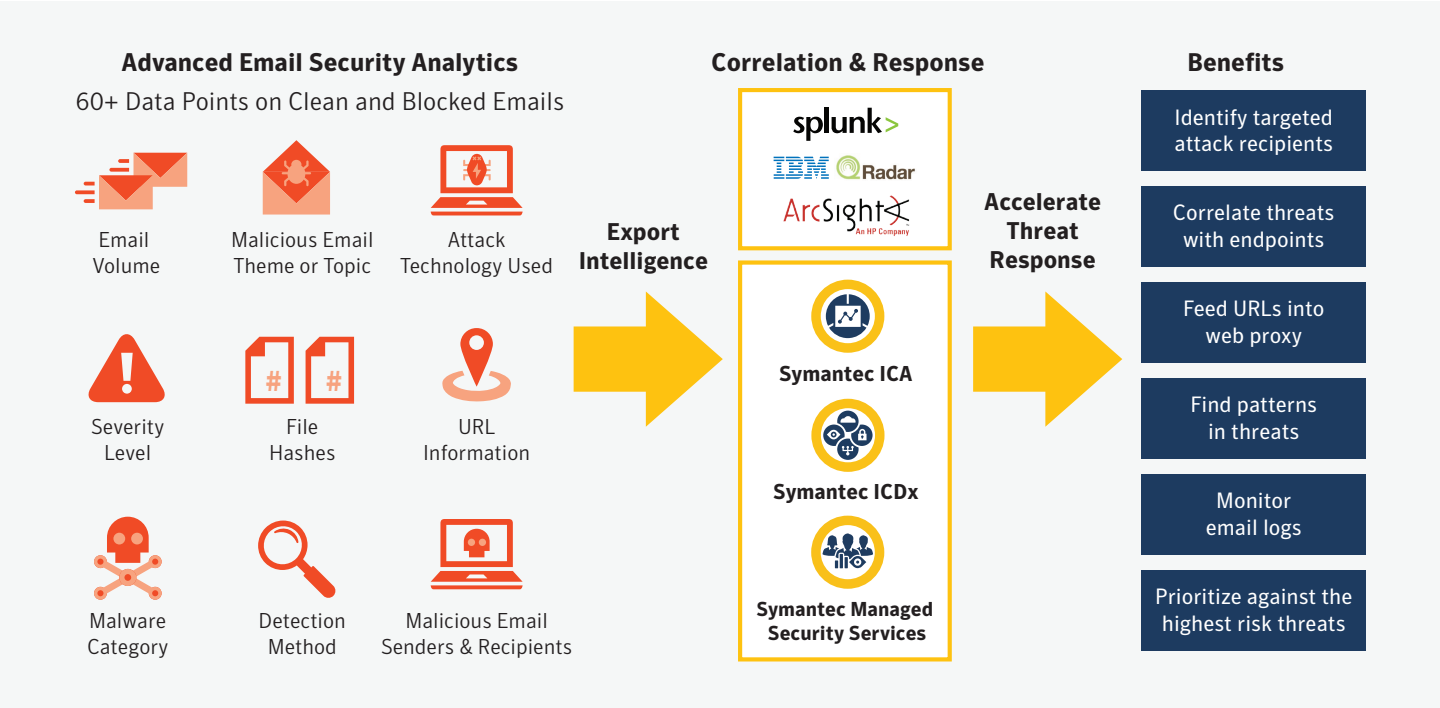
- Block spam, malware, and advanced email threats such as spear phishing, ransomware, and business email compromise by leveraging multilayered detection technologies such as machine learning, behavioral analysis, user and domain impersonation controls, and sender, file, and IP reputation. Multiple scanning engines stop unwanted email such as spam, newsletters, and marketing emails.
- Prevent the most complex, persistent email threats with virtual machine-aware 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 URLs in email for ultimate link 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.

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 via API integration with third-party SIEMs, or monitoring by Symantec Managed Security Services.
- 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.



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 Thread Detection & Response, it offers the strongest protection against spear phishing attacks with comprehensive defense that includes link protection, link 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].

No wonder we back it with the strongest, money-back guaranteed security SLAs: 100-percent protection from viruses, 100-percent service availability, and 100-percent email delivery.

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 protection.

Learn more about **Symantec Messaging Gateways**.

Symantec Phishing Readiness

Symantec Phishing Readiness is a cloud-delivered service that enables organizations to carry out simulated phishing attacks from a simple, central platform. Create and send targeted emails, analyze employee behavior, and assess your organization's susceptibility to phishing attacks with detailed metrics including email open rate, link clicks, attachment open rate, and data exposure.

Learn more about **Symantec Phishing Readiness**.

Symantec Email Security Service – Government

Symantec Email Security Service – Government is a FedRAMP-authorized cloud-hosted service that provides inbound and outbound messaging security including powerful protection against the latest messaging threats. Email Security Service – Government effectively blocks known malware, phishing and targeted attacks, spam, and unwanted bulk email. Built-in TLS encryption and data protection capabilities help control sensitive information sent via email. The service 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.

Learn more about **Email Security Service – Government**.

To learn more about Symantec's email security solutions, visit symantec.com/products/messaging-security

[1] FBI, Public Service Announcement, https://www.ic3.gov/media/2018/180712.aspx, July 2018
[2] Symantec Blog: "How Does Symantec Email Security Stack Up Against the Competition?" November 28, 2017

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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

19D210734_FB_Email_Security_Enterprise_EN