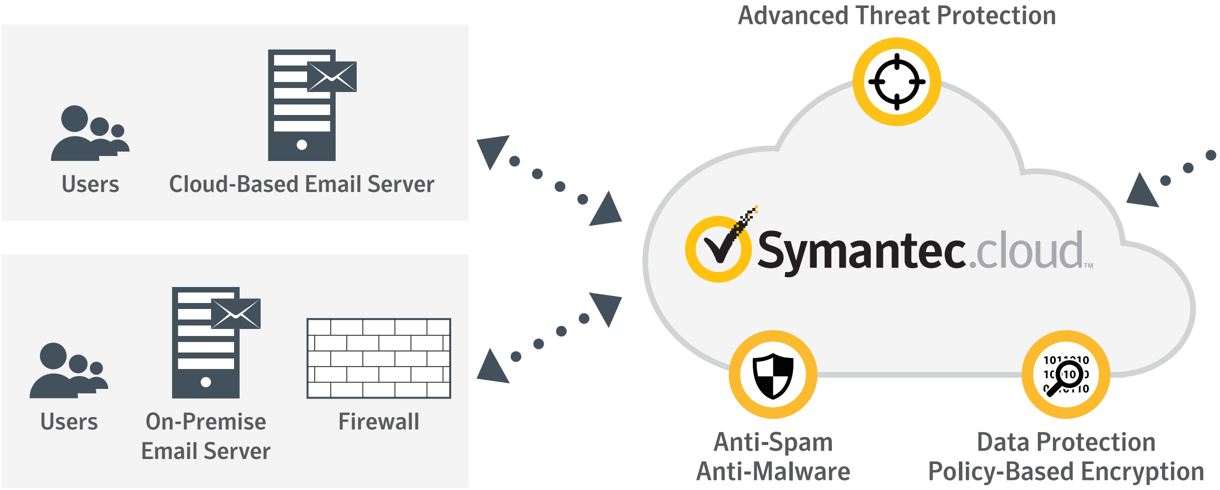
DATA SHEET

# Symantec Email Security.cloud

Safeguard your email with our industry-leading threat and anti-spam protection for Office 365, Google Apps, and more.

## Defend Against New and Sophisticated Email Attacks

Symantec Email Security.cloud is a comprehensive, cloud-based service that safeguards your email while strengthening the built-in security of cloud-based productivity tools such as Office 365 and G Suite. It blocks new and sophisticated email threats such as spear phishing, ransomware, and Business Email Compromise with the highest effectiveness and accuracy through multi-layered detection technologies and insights from the world's largest civilian threat intelligence network. This includes the strongest protection against spear phishing attacks since Symantec Email Security.cloud follows and evaluates malicious links in real-time before email delivery, even when threats try to use smokescreen techniques to evade detection



Symantec Email Security.cloud also keeps your emails secure and confidential with granular data loss prevention (DLP) and policy-based encryption controls. This includes tight integration with the market-leading Symantec DLP solution, which helps you move email to the cloud with confidence by extending, content-aware data loss prevention capabilities to Office 365, G Suite and Microsoft Exchange. This solution also offers advanced detection technologies that discover, monitor, and protect data across all of your cloud, mobile, network, endpoint, and storage systems.

Symantec provides additional protection and visibility into targeted & advanced attacks with Symantec Advanced Threat Protection for Email, a cloud-based service. This service prevents the most stealthy, advanced email threats with cloud-based sandboxing and blocks spear phishing attacks that weaponize a link after an email is delivered via click-time protection for malicious URLs. In addition, Advanced Threat Protection for Email helps accelerate response to targeted & advanced attacks through advanced email security analytics that provide the deepest visibility into targeted attack campaigns. This intelligence includes insights into both malicious and clean emails as well as more Indicators of Compromise (IOC) than anybody else with data points such as URLs, file hashes, and targeted attack information.

Symantec Email Security.cloud and Symantec Advanced Threat Protection for Email are part of the Symantec Cloud Email Security solution, which blocks malware and sophisticated email threats including spear phishing, ransomware, and Business Email Compromise. This solution also stops unwanted email such as spam, newsletters, and marketing emails from cluttering user inboxes. Symantec Cloud Email Security is backed by punitive, industry-leading service-level agreements of 100% protection from viruses, more than 99% spam effectiveness, and 100% email uptime.

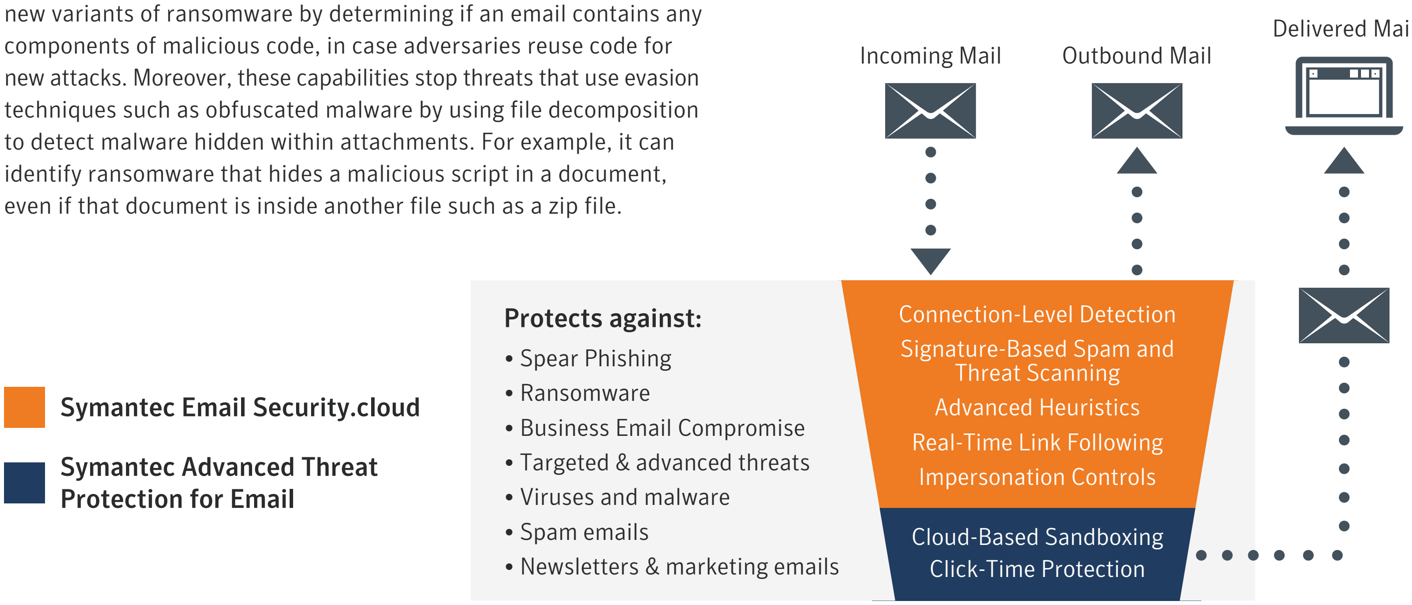
# Block Threats with the Highest Effectiveness and Accuracy

Symantec Email Security.cloud has the most effective and accurate email security solution since it uses multi-layered detection technologies such as advanced heuristics, real-time link following, & impersonation controls to combat new and sophisticated email threats such as spear phishing, ransomware, and Business Email Compromise. This protection is powered by insights from the world's largest civilian threat intelligence network, which offers global visibility into the threat landscape and helps deliver better security outcomes through telemetry from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors across 157 countries.

Advanced heuristics block ransomware, targeted attacks, and the latest emerging threats that typically evade detection by traditional email security solutions. These predictive heuristic technologies use every characteristic of an email to identify new or crafted attacks, including delivery behavior, message attributes, attachments, and social engineering tricks. This includes deep code analysis that blocks new variants of ransomware by determining if an email contains any components of malicious code, in case adversaries reuse code for new attacks. Moreover, these capabilities stop threats that use evasion techniques such as obfuscated malware by using file decomposition to detect malware hidden within attachments. For example, it can identify ransomware that hides a malicious script in a document, even if that document is inside another file such as a zip file.

Real-time link following stops malicious links used in spear phishing, targeted attacks, and other advanced threats before an email is delivered. Unlike traditional email security solutions that rely on reactive blacklists or signatures to block malicious links, this technology analyzes suspicious links in real-time, whether the link is in the body of an email or inside an attachment. As a result, Symantec effectively blocks both new and known malicious links used in spear phishing attacks. Links are followed to their final destination, even when attackers try to use sophisticated techniques such as multiple redirects, shortened URLs, and time-based delays to bypass detection. Any content found at the destination URL is downloaded and deep heuristic analysis is performed to determine whether they are malicious.

New impersonation controls provide the strongest protection against Business Email Compromise (BEC), spear phishing, and other spoofing attacks by blocking threats that impersonate a user or domain in your organization. These controls identify and prevent BEC scams by using a sophisticated impersonation engine to sniff out attacks that masquerade as a specific user or spoof a legitimate email domain. This includes the ability to protect only certain senior executives or email domains from BEC fraud as well as whitelist trusted users, domains, and IP addresses. Additionally, you can get complete visibility into BEC attacks through detailed reporting on these threats.


Incoming Mail
Outbound Mail
Delivered Mail
🟧 Symantec Email Security.cloud
🟦 Symantec Advanced Threat Protection for Email
Protects against:
• Spear Phishing
• Ransomware
• Business Email Compromise
• Targeted & advanced threats
• Viruses and malware
• Spam emails
• Newsletters & marketing emails
Connection-Level Detection
Signature-Based Spam and Threat Scanning
Advanced Heuristics
Real-Time Link Following
Impersonation Controls
Cloud-Based Sandboxing
Click-Time Protection

# Keep Your Emails Secure and Confidential

Symantec Email Security.cloud prevents leakage of sensitive information and helps you address your compliance & privacy requirements with built-in data loss prevention (DLP) and policy-based encryption controls that block, quarantine, or encrypt sensitive emails. These controls are strengthened through integration with the industry-leading Symantec DLP solution, which discovers, monitors and protects sensitive data across your entire environment.

Flexible, built-in DLP policies identify and control sensitive emails coming into or going out of your organization with over 100 pre-defined lists of keyword dictionaries, regular expression and MIME type lists. Simple, out-of-the-box policy templates make it easy to comply with complex regulatory requirements such as HIPAA, PCI, and ITAR. These policies can be customized to meet your needs with granular rules & conditions and actions such as blocking, quarantining, redirecting, or tagging emails can be triggered when emails containing confidential content are found.

Policy-based encryption controls safeguard the security and privacy of confidential emails by automatically and seamlessly encrypting specific outbound emails. These policies perform secure encryption of email messages and any attachments via a password-protected PDF that provides a mobile-friendly "push" encryption experience. Additional encryption methods and customization are available in the Symantec Policy-Based Encryption Advanced add-on service.

Tight integration with the industry-leading Symantec DLP solution prevents data loss that other solutions typically miss. This solution inspects the content and context of emails sent via Office 365, G Suite, and Microsoft Exchange in real-time by leveraging its built-in intelligence and content detection capabilities to analyze both the message content and its metadata. As a result, you can accurately identify sensitive data with minimal false positives, so you can focus on the real incidents. Symantec DLP also offers advanced detection technologies such as Exact Data Matching (EDM), Indexed Document Matching (IDM), and Vector Machine Learning (VML) that protect data across all of your emails, endpoints, cloud-based services, mobile devices, networks, and storage systems.

# Get Dependable Service From the Cloud

Nearly two decades have been spent delivering and continuously improving the most accurate, effective, and dependable cloud email security service. As a result, Symantec Email Security.cloud is backed by comprehensive, punitive service level agreements (SLA) that demonstrate our confidence in our solution and our seriousness about providing the most dependable email security service. We give complete transparency into our service by continually publishing and measuring our performance against these robust SLAs. These SLAs have an aggressive set of metrics by which the service is monitored. Since our SLAs are punitive, we pay out a service credit if we don't meet the following performance targets:

- **Threat Effectiveness:** 100% protection against known & unknown viruses. We provide a 100% service credit after just one infection during a calendar month.
- **Spam Effectiveness:** More than 99% spam capture rate. Symantec is the only email security provider to guarantee spam capture in English and other languages.
- **Threat Accuracy:** No more than 0.0001% virus false positives.
- **Spam Accuracy:** No more than 0.0003% spam false positives.
- **Email Availability:** 100% service uptime. Symantec offers a full cancellation clause if our email availability falls below 95%.
- **Email Delivery:** 100% email delivery. Symantec is the only vendor that guarantees 100% delivery of emails sent to or from customers, assuming the email was received by Symantec and did not contain a virus, spam or other filtered content.
- **Email Latency:** Average email scanning time within 60 seconds. We give you a partial service credit if email latency averages more than a 1 min round trip and a full service credit if email latency exceeds an average of a 3 min round trip.

## Key Capabilities

- Block new & sophisticated email threats such as spear phishing, ransomware, and Business Email Compromise with the highest effectiveness and the accuracy through multi-layered detection technologies such as advanced heuristics, real-time link following, and impersonation controls
- Gain comprehensive visibility into the global threat landscape and achieve better security outcomes with telemetry from the world's largest civilian threat intelligence network
- Stop sensitive data loss and help meet your security, legal & compliance requirements with granular DLP and encryption controls, including integration with the market-leading Symantec DLP solution
- Achieve peace of mind with industry-leading, punitive SLAs that provide guaranteed performance for email threats, spam, and availability with 100% protection from viruses, more than 99% spam effectiveness, and 100% email uptime.
- Protect cloud-based productivity tools such as Office 365 and G Suite from targeted attacks and sensitive data loss by stopping new & sophisticated email attacks and preventing leakage of confidential information

## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, 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 suite of products for protection at home and across all of 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**