DATA SHEET

Symantec Advanced Threat Protection for Email

Protect against the most sophisticated email threats and gain comprehensive insights into targeted & advanced email attacks

Prevent the Most Advanced Email Attacks

Symantec Advanced Threat Protection for Email is a cloud-based service that uncovers and prioritizes advanced attacks entering your organization through email by adding cloud-based sandboxing, additional spear phishing protection, and unique targeted attack identification capabilities to the Symantec Email Security.cloud service. In addition, it helps accelerate your response to targeted & advanced threats with advanced email security analytics that provide the deepest visibility into targeted & advanced attack campaigns. This intelligence includes insights into both clean and malicious emails as well as more Indicators of Compromise (IOCs) than any other vendor, with 60+ data points such as URLs, file hashes, and targeted attack information. You can export this data to your Security Operations Center to quickly determine the severity and scope of any targeted or advanced attack. And when combined with Symantec Advanced Threat Protection endpoint, network, or web modules, you can automatically aggregate events across all installed control points to prioritize the most critical threats in your organization.

Cloud-based Sandboxing and Payload Detonation

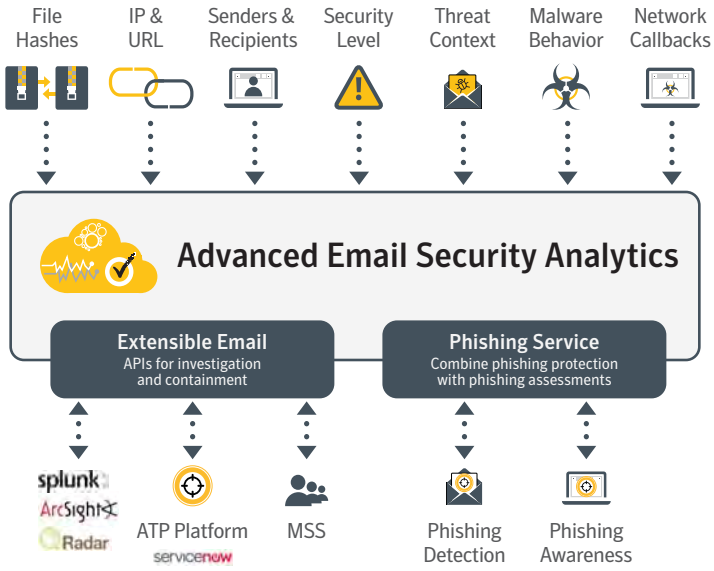
Advanced Threat Protection for Email customers can leverage cloud-based sandboxing and payload detonation capabilities to discover and prioritize today's most complex targeted & advanced attacks. This service uses advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. In addition, it's infused with security telemetry from the Symantec Global Intelligence Network, the world's largest civilian threat intelligence network. The Symantec Global Intelligence Network provides comprehensive visibility into the threat landscape and delivers better security outcomes by collecting and analyzing security telemetry from more than 175 million endpoint, 80 million web proxy users, and 57 million attack sensors in 157 countries. Our cloud-based sandboxing also provides you the details of malicious files and their execution actions, so that all relevant attack components can be quickly investigated and remediated. Today, 28 percent of advanced attacks are "virtual machine-aware," which means they don't reveal suspicious behavior when run in typical sandboxing systems.[1] To combat this, Symantec employs techniques to mimic human behavior and also executes suspicious files both virtually and on physical hardware to uncover attacks that evade detection by traditional sandboxing technologies.

Click-Time URL Protection

Click-Time URL Protection blocks malicious links by analyzing them when they are clicked by end-users to protect against spear phishing attacks that weaponize a link after an email is delivered. This complements Real-Time Link Following technology in Symantec Email Security.cloud, which blocks malicious links used in spear phishing attacks before an email is delivered. Unlike other solutions that rely on reactive blacklists or signatures to stop spear phishing attacks, Symantec proactively stops both new and known spear phishing attacks that employ malicious links by performing deep evaluation of links in real-time. This deep evaluation follows links to their final destination, even when attackers use sophisticated techniques such as multiple redirects, shortened URLs, hijacked URLs, and time-based delays that bypass detection by traditional security solutions. Any files found at the destination URL are downloaded and deep heuristic analysis is performed to determine whether they are malware. This deep link evaluation powers both Click-Time URL Protection and Real-Time Link Following, which enables Symantec to provide the most effective protection against spear phishing, targeted attacks, and other advanced threats that contain malicious links.

Advanced Email Security Analytics

Advanced Threat Protection for Email helps accelerate your response to targeted & advanced threats with advanced email security analytics that provide the deepest visibility into email attack campaigns. This rich intelligence includes detailed reporting on every clean and malicious email entering your organization. These reports include 60+ data points including IOCs such as source URLs of an attack, targeted attack information, malware categorization, sender & recipient information, method of detection, and detailed information about file hashes. Each attack is assigned a threat category, such as Trojan or Infostealer, and a severity level of low, medium, or high to indicate the level of sophistication of an attack. You can even search and find detailed information about blocked emails, including both the original link in an email and the final destination link containing malware as determined by Real-Time Link Following. These advanced analytics give comprehensive insights into targeted & advanced threats against your organization by offering more Indicators of Compromise than any other email vendor.



Security Operations Center Integration

Advanced Threat Protection for Email enables you to easily export the advanced email security analytics on clean and malicious emails to your Security Operations Center through integration with third-party SIEMs such as Splunk, IBM QRadar, HPE ArcSight, and more. Threat intelligence data is streamed directly to your SIEM via a granular, API-driven feed to give your security team rapid visibility into threats. Security analysts can leverage this data to quickly correlate and analyze threats when investigating and responding to threats. Moreover, you can easily respond to email threats with a free

Splunk application, which allows you to export the advanced email security analytics directly to Splunk. This application provides deep visibility into the threat landscape with data points such as malicious URLs and file hashes as well as information such as high risk users, a geographical view of incoming attacks, and a timeline of email malware. You can even speed-up detection and response of targeted & advanced threats by exporting our advanced email security analytics to Symantec Managed Security Services, which monitors email security logs via the API-driven feed.

Targeted Attack Identification

Advanced Threat Protection: Email directly leverages machine learning and ongoing investigations by Symantec research analysts into new targeted attacks to provide detailed reports on email attacks targeting your organization. Machine learning analyzes emails that are potentially malicious and human analysts feed in new malware behavior and other unknowns into this algorithm to keep detection of new targeted threats sharp and help identify new targeted threats that traditional email security solutions typically miss. Together with the advanced email security analytics on targeted & advanced threats, targeted attack identification allows you to focus efforts and resources on those attacks that pose the greatest danger to your organization.

Threat Prioritization Across Multiple Control Points

Advanced Threat Protection for Email is part of Symantec Advanced Threat Protection, a unified solution that helps customers uncover, prioritize, investigate, and quickly remediate the most complex attacks and which also includes modules for endpoint, network and web control points. It comes with threat correlation capabilities, which quickly identifies and prioritizes compromised systems that require immediate remediation by aggregating suspicious activity across all installed control points.

Consolidated View Across Endpoints, Networks, Web, and Email

As part of the Symantec Advanced Threat Protection offering, Advanced Threat Protection for Email combines insights from endpoints, networks, web traffic, and emails, as well as Symantec's massive global intelligence network, to find threats that evade individual point products. And with one click of a button, Symantec Advanced Threat Protection will search for, discover, and remediate attack components across your organization, all with no new agents.

Key Capabilities

- Detect complex and stealthy advanced attacks with cloud-based sandboxing and payload detonation capabilities
- Stop malicious links weaponized after email delivery with Click-Time URL Protection, which helps provide the strongest protection against spear phishing, targeted attacks, and other advanced threats
- Accelerate response to targeted and advanced attacks through advanced email security analytics that provide the deepest visibility into email attack campaigns with 60+ data points on every clean and malicious email
- Quickly correlate and respond to threats by exporting advanced email security analytics to your Security Operations Center through integration with third-party SIEMs and Symantec Managed Security Services
- Gain deep visibility into the threat landscape with a free Splunk application that enables you to directly export advanced email security analytics to Splunk
- Receive detailed reporting on highly targeted email attacks against your organization through machine learning analysis and review from Symantec research analysts
- Correlate suspicious activity across all control points to identify and prioritize security events that pose the most risk you
- Get a single prioritized view of all advanced attack activity in your organization across your email, endpoints, networks, and web traffic in a single solution

[1] Symantec™ Internet Security Threat Report, Volume 20, April, 2015

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**