# Symantec ATP:Email Datasheet

**Data Sheet: Advanced Threat Protection**

## The Problem

Email remains a very popular and effective mechanism for targeted & advanced attacks to enter organizations. Attackers target specific victims through email by attaching malicious files or embedding links to attacker-controlled websites. They employ sophisticated social engineering techniques to trick unsuspecting users into opening malicious emails, and will customize each attack campaign as needed to avoid detection and reach their targets through targeted spear phishing attacks. They even leverage these social engineering techniques to get recipients to carry out large wire transfers or send over sensitive information via Business Email Compromise scams.

And this problem is only getting worse. The number of email-based spear phishing campaigns targeting employees increased by 55% while the number of recipients per campaign decreased by 39% in 2015.[1] Small and medium-sized businesses also experienced an uptick in such attacks, seeing increases of 26 percent and 30 percent respectively.[2] Traditional email security solutions try to stop these threats, but they lack the deep visibility and rich intelligence needed to uncover and respond to targeted & advanced attacks. Moreover, it is also difficult or even impossible to export threat intelligence from these solutions into third-party Security Information and Event Management (SIEM) systems, which are needed for threat investigation and response. Clearly, traditional security solutions are inadequate to keep organizations safe from the newest generation of email-borne threats, which are becoming increasingly targeted and advanced.

## The Solution

Symantec™ Advanced Threat Protection: Email is a cloud-based service that uncovers and prioritizes advanced attacks entering your organization through email by adding Symantec Cynic™ cloud-based sandboxing, spear phishing protection from Symantec Click-Time URL Protection, and unique targeted attack identification capabilities to the Symantec Email Security.cloud service. In addition, it provides the deepest visibility into targeted & advanced attack campaigns with more indicators of compromise than anybody else, including data points such as URL information, 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, Symantec Synapse™ correlation automatically aggregates events across all installed control points to prioritize the most critical threats in your organization.


### *Symantec Cynic Cloud-based Sandboxing and Payload Detonation*

Advanced Threat Protection: Email customers benefit from the Symantec Cynic cloud-based sandboxing and payload detonation service, which is built from the ground up to discover and prioritize today's most complex targeted attacks. Cynic leverages advanced machine learning-based analysis and insights from the Symantec Global Intelligence Network, one of the world's largest threat intelligence networks, to

1. Symantec™ Internet Security Threat Report, Volume 21, April, 2016
2. Symantec™ Internet Security Threat Report, Volume 20, April, 2015

detect even the most stealthy and persistent threats. 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 endpoints and 57 million attack sensors in 157 countries. Cynic also provides you the details of malicious files and their execution actions, so that all relevant attack components can be quickly 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.[3] To combat this, Cynic 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.

### *Symantec Click-Time URL Protection*


The newest addition to Advanced Threat Protection: Email, Symantec 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 Symantec Real-Time Link Following technology in 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 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, whether the link is in the body of an email or inside an attachment. This deep evaluation tracks 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 Click-Time URL Protection and Real-Time Link Following, which enable Symantec to provide the most effective protection against spear phishing, targeted attacks, and other advanced threats that contain malicious links.

### *Deep Visibility into Targeted & Advanced Threats*

Advanced Threat Protection: Email provides the deepest visibility into targeted & advanced attack campaigns with detailed reporting on every incoming malicious email. This reporting include data points such as source URLs of an attack, malware categorization, 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. This rich threat intelligence gives comprehensive insights into targeted & advanced threats against your organization with more indicators of compromise than any other email vendor. 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.

3. Symantec™ Internet Security Threat Report, Volume 20, April, 2015

### *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. This results in detailed reporting on targeted attacks, including information about the attack technology, volume of emails containing the attack, and information about the email senders and recipients to provide an in-depth understanding of any targeted attack on your environment. Together with the rich threat intelligence 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.

### *Security Operations Center Integration*

Advanced Threat Protection: Email enables you to easily export the rich threat intelligence on malicious emails to your Security Operations Center through integration with third-party SIEMs. Threat intelligence data is streamed directly to your SIEM 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.

### *Symantec Synapse™ Correlation*

Advanced Threat Protection: Email is part of Symantec Advanced Threat Protection, a unified solution that helps customers uncover, prioritize, and quickly remediate the most complex attacks and which also includes modules for endpoint, network and web control points. It comes with Symantec Synapse correlation, 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: 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.

## Features and Benefits

- Detect complex and stealthy advanced attacks with Symantec Cynic cloud-based sandboxing and payload detonation
- Stop malicious links weaponized after email delivery with Click-Time URL Protection for the strongest protection against spear phishing, targeted attacks, and other advanced threats
- Gain deep visibility into targeted and advanced attacks through rich threat intelligence on every malicious email entering your organization
- Receive detailed reporting on highly targeted email attacks against your organization through machine learning analysis and review from Symantec research analysts
- Quickly correlate and respond to threats by exporting rich threat intelligence to your Security Operations Center through integration with third-party SIEMs
- Correlate suspicious activity across all control points to identify and prioritize 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 without adding new agents

21349610-3 10/16