Maximize Email Security with Symantec Advanced Threat Protection

Solution Overview: Advanced Threat Protection

Email is a prime target for attackers

Email is the threat vector cybercriminals use most often to launch and distribute attacks. As documented in the *Symantec Internet Security Threat Report,*[1] one out of every 244 emails in 2014 contained a malware attack, and five out of six large enterprises were targeted by email-based spear-phishing campaigns. Attackers employ sophisticated social engineering tactics to trick users into opening these malicious emails, which often contain zero-day or other complex malware designed to evade traditional security systems. This includes virtual machine-aware malware that doesn't reveal suspicious behavior when run in typical sandboxing systems. According to the *Symantec Internet Security Threat Report*, 28 percent of malware in 2014 was virtual machine-aware. Detecting this type of malware in your organization can be difficult and can lead to long remediation times when an infection does occur.

Uncover and prioritize advanced attacks

Symantec™ Advanced Threat Protection: Email uncovers and prioritizes advanced threats that attempt to infiltrate an organization via email. It leverages and enhances your existing Symantec™ Email Security.cloud installation, adding a number of new critical capabilities to uncover targeted email-based threats with easy administration from the existing Symantec.cloud management portal.

Symantec Advanced Threat Protection: Email leverages investigations by Symantec research analysts into targeted attacks and provides detailed data on targeted attacks that have attempted to enter your organization via email. Symantec analysts look at the message theme and topic, recipients, technologies used, and statistics such as the number of emails included in a run to differentiate targeted attacks from typical spam containing malware. For example, a targeted email might contain a topic of interest to the recipient, be sent to individuals in a specific organization or industry, use a zero-day vulnerability, and be part of a low-volume run.

Symantec Advanced Threat Protection: Email customers also receive Symantec Cynic™, an entirely new cloud-based sandboxing and payload detonation service built from the ground up to detect and prioritize today's most sophisticated targeted attacks. Cynic leverages advanced machine learning-based analysis combined with Symantec's global intelligence to detect even the most stealthy and persistent threats. In addition to virtual execution, Cynic executes suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies.

Improve visibility into advanced threats

Messages identified by Symantec Advanced Threat Protection: Email as malicious, including targeted attacks, are shown in the Advanced Threat Incidents dashboard. Those messages classified as targeted attacks are then categorized into three types of attacks, ranging from highly targeted attacks that leverage new exploits and specific themes customized for each recipient to broader campaigns that target a common industry or region. Every malicious message is assigned a threat category, such as Trojan or Infostealer, and a severity level of low, medium, high, or critical to indicate the level of sophistication of the threat. The message subject, recipients, source IP, and message status are also displayed to aid further investigation and remediation.

1. Symantec Internet Security Threat Report, Volume 20, April, 2015

Symantec

Symantec Advanced Protection: Email can also generate detailed reports on all incoming malicious emails, whether they were detected by Email Security.cloud or Cynic. More than 25 available data points include information about the source URLs of the attack, malware category, method of detection, and detailed information about file hashes. These Advanced Threat Protection reports are customizable and can be requested through the same interface in the Symantec.cloud management portal as your existing Email Security.cloud reports.

Symantec Advanced Threat Protection: Email enhances the Email Security.cloud Track and Trace feature by providing the ability to search for malicious URLs blocked by Email Security.cloud. This search feature includes both the original link in the email and the ultimate destination link containing malware as determined by Real-Time Link Following.

Export data for SIEM correlation

Symantec Advanced Threat Protection: Email allows for on-demand export of malware reporting data from Email Security.cloud into third-party Security Incident and Event Management Systems (SIEMs). The latest raw CSV data available through the detailed reporting feature can be securely pulled in near real-time via an authenticated URL. The extracted information contains all data that arrived between the previous data request time and the current request time to allow for easy differential analysis.

Correlate events across endpoints, networks, and email

Symantec Advanced Threat Protection: Email is part of Symantec™ Advanced Threat Protection, which also includes modules for network and endpoint. New Symantec Synapse™ correlation technology aggregates suspicious activity across all installed control points to quickly identify and prioritize those systems that remain compromised and require immediate remediation.

Symantec Advanced Threat Protection is a single solution to help customers uncover, prioritize, and quickly remediate today's most complex attacks. It combines intelligence from endpoints, networks, and email, as well as Symantec's massive global sensor network, to find threats that evade individual point products, all from a single console. 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 endpoint agents.

Don't wait to secure your email

Contact a Symantec sales representative and learn how you can add Advanced Threat Protection to your existing Email Security.cloud deployment or visit http://atp.symantec.com.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

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

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

21362573 02/16