Symantec™ Advanced Threat Protection: Email

Data Sheet: Advanced Threat Protection

The Problem

Email remains a very popular and effective mechanism for advanced attacks to enter organizations. Attackers target chosen victims through email by attaching malicious files or embedding links to attacker-controlled websites. They employ sophisticated social engineering tactics to trick unsuspecting users into opening malicious emails, and will customize each attack campaign as needed to avoid detection and reach their targets.

And this problem is only getting worse. Five out of every six large companies were targeted with email-based spear phishing attacks in 2014, a 40 percent increase over the previous year. Small and medium-sized businesses also experienced an uptick in such attacks, seeing increases of 26 percent and 30 percent respectively.[1] Clearly, today's existing security solutions are inadequate to keep organizations safe from the newest generation of email-borne threats.

The Solution

Symantec™ Advanced Threat Protection: Email that uncovers advanced attacks entering your organization through email, by adding unique targeted attack identification and Symantec Cynic™ sandbox detection capabilities to existing installations of Symantec™ Email Security.cloud. In addition, you receive detailed information from Symantec analysts about new or unknown malware entering your organization through email, so that you can determine the severity and scope of any targeted attack campaign. And, if you add our endpoint or network modules, Symantec's Synapse™ correlation technology will automatically aggregate events across all installed control points to prioritize the most critical threats in your organization.

Uncover and Prioritize Advanced Attacks

Symantec Advanced Threat Protection: Email uncovers and prioritizes advanced threats that attempt to infiltrate an organization via email. The product leverages and enhances existing Symantec Email Security.cloud installations, adding a number of new critical capabilities to uncover targeted email-based threats.

Symantec Cynic™ Cloud-based Sandboxing and Payload Detonation Service

Symantec Advanced Protection: Email customers receive Symantec Cynic, an entirely new cloud-based sandboxing and payload detonation service built from the ground up to discover and prioritize today's most complex targeted attacks. Cynic leverages advanced machine learning-based analysis combined with Symantec's global intelligence to detect even the most stealthy and persistent threats. Cynic also provides the customer with the details of a file's capabilities and all of its execution actions, so that all relevant attack components can be quickly remediated. Today, 28 percent of advanced attacks are "virtual machine-

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

aware," that is, they don't reveal their suspicious behaviors when run in typical sandboxing systems.[2] To combat this, Cynic also executes suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies.

Symantec Synapse™ Correlation

Symantec Advanced Protection: Email is part of the full Advanced Protection offering, which also includes modules for network and endpoint control points. Symantec's new 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.

Targeted Attack Identification and Detailed Malware Reporting

Symantec Advanced Threat Protection: Email also directly leverages ongoing investigations by Symantec research analysts into new targeted attacks. The product will provide detailed reports on targeted attacks that have attempted to enter the organization via email, including information about the attack technology, volume of emails containing the attack, and information about the email sender and recipients. This new capability helps customers understand in-depth the full scope of any targeted attack on their environment.

Advanced Threat Protection: Email also provides detailed reports on every incoming malicious email, containing over 25 data points of in-depth insight into attack campaigns. These data points include information about source URLs of the 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. The Track and Trace feature provides the ability to search for further details about malicious URLs blocked by Email Security.cloud. This includes both the original link in the email and the ultimate destination link containing malware as determined by Real-Time Link Following.

Collectively, these capabilities allow security analysts to focus their efforts and resources on those attacks that pose the greatest danger to the organization.

Additional Data Correlation via SIEM

Symantec Advanced Threat Protection: Email allows for on-demand export of malware reporting data into third-party Security Incident and Event Management Systems (SIEMs). The latest raw CSV data 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.

A Consolidated View of Attacks Across Endpoints, Networks, and Email

Advanced Threat Protection: Email is part of Symantec™ Advanced Threat Protection, a unified 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.

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

Features and Benefits

- Detect complex and stealthy advanced attacks with the Symantec Cynic cloud-based sandboxing and payload detonation service
- Receive detailed reports on highly targeted email attacks against the organization
- Get comprehensive reporting on every malicious email entering the organization, including more than 25 specific data points about each attack
- Severity levels are provided for each attack, allowing for more focused response efforts to those threats of greatest importance

More Information

Visit our website

http://www.symantec.com/advanced-threat-protection

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.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

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

21349610-3 12/15