Maximize Endpoint Protection with Symantec Advanced Threat Protection

Solution Overview: Advanced Threat Protection

Your endpoints are being targeted

Security breaches are increasing in frequency and complexity, and endpoint systems are frequent targets for attackers. In 2014, five out of six large companies were targeted for attack, and 60 percent of all attacks were aimed at small- and medium-size organizations.[1] And once inside a victim's infrastructure, targeted attacks use endpoint systems to traverse the network, steal credentials, and connect with command-and-control servers, all with the goal of compromising an organization's most critical systems and data.

Today's advanced threats are also increasingly stealthy and difficult to detect, with the result that many organizations don't know when they are being attacked. In 2014, it cost impacted companies an average of $3.8 million to recover from these breaches and 27.7 days to remediate web-based attacks.[2]

And as quickly as organizations respond, hackers refine their techniques to avoid detection. As just one example, according to the *Symantec Internet Security Threat Report*, 28 percent of malware in 2014 was virtual-machine aware, meaning they don't reveal their suspicious behaviors when run in typical sandboxing systems.

Difficulties in detection and remediation

A critical step in enterprise security today is endpoint defense. The average IT security architecture uses at least three security products on each endpoint, but these products generate thousands of security events that security analysts must manually correlate to get visibility into suspicious activity in their environment. Or, they may need to export log files from various products into a 3rd-party Security Incident and Event Manager (SIEM) and create complex rules in an effort to uncover new threat activity.

Once a security team does learn about an attack inside their organization, it can require days, weeks, or even months to completely remediate it. Remediation often requires manually hunting through hundreds or thousands of systems to find all of the attack artifacts and remove all attack components. Security analysts also must deploy new blocking rules to all of their endpoints and gateways to ensure that the attack can't breach the organization again in the future, which can take significant time and resources.

The solution

Symantec™ Advanced Threat Protection: Endpoint is a new solution to uncover, prioritize, and remediate advanced attacks across all of your endpoints, leveraging your existing investment in Symantec™ Endpoint Protection. With one click of a button, you can search for, discover, and remediate any attack artifacts across all of your endpoint systems.

Hunt for any Indicators-of-Compromise by searching every endpoint in your organization from a single console. Security analysts can also quickly retrieve a particular file from any endpoint for further analysis. And because Symantec Advanced

1. Symantec Internet Security Threat Report, Volume 20, April, 2015
2. Ponemon Institute 2015 Cost of a Data Breach Study, https://securityintelligence.com/cost-of-a-data-breach-2015/

Symantec

Threat Protection: Endpoint leverages your existing installation of Symantec Endpoint Protection, this can all be accomplished without installing any new endpoint agents.

Uncover and prioritize advanced attacks

Symantec™ Advanced Threat Protection: Endpoint combines global telemetry from one of the world's largest cyber threat intelligence networks with local customer context across endpoints to uncover attacks that would otherwise evade detection. A security analyst can see all of the endpoint attack components in one place, including how a threat entered the organization, a list of machines that have the threat, what new files the threat created, and what files it downloaded.

With Symantec Advanced Protection: Endpoint, you can submit any suspicious file to 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.

If you add Symantec™ Advanced Threat Protection: Network or Symantec™ Email Security.cloud, Symantec's Synapse™ correlation technology will automatically aggregate events across all Symantec-protected control points to prioritize the most critical threats in your organization. Based on Symantec research, we believe that correlating network and email events with endpoint detections in this way will significantly reduce the number of incidents a typical security analyst needs to examine, allowing the analyst to respond more quickly to the highest-risk threats.

Remediate fast

Once any attack component has been identified as malicious, Symantec Advanced Threat Protection: Endpoint remediates fast, allowing you to quickly remove and block further execution of any attack components across all endpoints. Compromised endpoints can also be quarantined to prevent the infection from spreading. Symantec Advanced Threat Protection: Endpoint also provides unique visualization of related Indicators-of-Compromise of an attack, including a complete graphical view of how all Indicators-of-Compromise are connected to each other. An analyst can see all files used in a particular attack, including all IP addresses where the file was downloaded from, all installed registry keys, and other processes initiated by the attack. The analyst can then remediate any of these attack components across all endpoints, with the click of a button.

A consolidated view of attacks across endpoints, networks, and email

Advanced Threat Protection: Endpoint 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.

Next steps

Contact a Symantec sales representative and learn how you can add Advanced Threat Protection to your existing Endpoint Protection implementation 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

21362575-1 12/15