WHITE PAPER:
SYMANTEC ADVANCED THREAT PROTECTION

Prevent and Detect Malware with Symantec™ Advanced Threat Protection: Network

Who should read this paper

This white paper is intended for CIOs, CISOs, and security professionals tasked with protecting their organization from targeted attacks and advanced threats.

Symantec

Content

Preventing Threats in the Network

Symantec™ Advanced Threat Protection: Network provides revolutionary protection in a gateway appliance. So how does this combine with other Symantec products like Symantec™ Endpoint Protection to help you get better visibility into the current threats your company is facing? What new visibility should you expect from Advanced Threat Protection: Network?

As a network appliance, Advanced Threat Protection: Network has the ability to monitor all the devices on your network. Many organizations have non-compliant machines where endpoint protection wasn't installed, and Advanced Threat Protection: Network protects these machines.

With the rise of Bring Your Own Device, many networks have employee or visitor-owned phones, tablets, and laptops on the company's network. Each of these are potential ways for attackers to enter your environment. Advanced Threat Protection: Network monitors traffic for each of these machines for threats, such as Command and Control activity, without the need to install additional software on any of these devices.

Advanced Threat Protection: Network leverages Symantec's industry-leading Insight, SONAR, and Vantage Network Intrusion Prevention technologies. These technologies are implemented just inside the firewall, which allows them be to tuned very aggressively without the risk of false positives on internal use only applications, resulting in unparalleled detection of both known and unknown threats.

Advanced Malware Analysis with Symantec Cynic™

Advanced Threat Protection: Network offers the brand new Symantec Cynic™ anti-malware service. Suspicious files are dynamically analyzed for malicious activity using Symantec Workspace Virtualization to allow detonation against a wide variety of vulnerable applications, including the latest versions as well as older, more vulnerable versions, using aggressively tuned versions of Symantec's SONAR and Vantage engines.

The most advanced malware attempts to evade advanced protection by not running in virtualized environments. Cynic detects even this cutting-edge malware by detonating such malware on bare metal physical machines and by leveraging Symantec Skeptic™ static analysis to find malware in ways undetectable by even advanced malware attempting to evade security or virtualization

But Cynic is far more than a static and dynamic malware detonation system. Cynic leverages intelligence gathered from Symantec's vast intelligence network of over 100 million machines, using over 4 petabytes of data and trillions of records. By leveraging this intelligence, Cynic can identify not just malicious files but also attribute never-before-seen malware to worldwide families. This is done by observing the behavior of malware all over the world. Malware authors, of course, recompile their code, re-obfuscate their code, and repack their code, resulting in unique binaries every time. However, even the most advanced attackers have large investments in their code base and reuse this code in different attacks. Since Cynic has this huge database of malware behaviors across the world, it can identify that a brand new binary is a member of a known malware family given the behavior patterns that exist despite their evasive techniques.

This intelligence provides global context to individual attacks. Not only does Cynic give visibility into what the malware did, but based on Symantec's global intelligence, Cynic can determine where else in the world this malware has been seen, the source of the attack, and the infection vectors used.

Better Visibility Through Correlation

Advanced Threat Protection: Network not only identifies threats inside your organization, but it also points out the larger patterns in the attacks, such as internal machines continually seeing malicious activity, external actors repeatedly attempting to breach your defenses, and similar exploit attempts probing your network. This shows the bigger picture and enables you to see the whole battlefield instead of an individual skirmish.

Advanced Threat Protection: Network uses Symantec Synapse™ to correlate with Symantec™ Endpoint Protection and Symantec™ Email Security.cloud to further increase this vision, showing what other activities occurred on the endpoint or how a spear phishing email participated in larger attacks.

Advanced Threat Protection: Network combines proven and cutting-edge technologies to give better insight into attacks on organizations. Visibility is vastly improved both for organizations that utilize Symantec Endpoint Protection and those without.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

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

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