Symantec™ Advanced Threat Protection: Network

Data Sheet: Advanced Threat Protection

The Problem

Today's advanced attacks hide themselves on legitimate websites, leverage new and unknown vulnerabilities, and enter targeted organizations through a variety of network-based protocols. These attacks are designed to evade typical network-based security approaches, allowing them to infiltrate the victim's infrastructure, where they can then compromise critical systems and data. And even in the case where a network security product is aware of such an attack, the specific attack details are often buried in a long list of lower-priority alerts from the product, making it very challenging for an analyst to discover the true problem.

And this issue is only getting worse. Almost all companies, large and small, are at risk from targeted attacks. Five out of every six large companies (2,500+ employees) were targeted with 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]

The Solution

Symantec™ Advanced Threat Protection: Network is a new solution, available in either a hardware appliance or virtual machine (VM) form factor, which uncovers and prioritizes advanced attacks entering the organization through the network. The product automatically sends all suspicious files to the new Symantec Cynic™ sandboxing system for rapid detection of even the most complex and stealthy advanced attacks. And, if you have Symantec™ Endpoint Protection or Symantec™ Email Security.cloud, Symantec's Synapse™ correlation technology will automatically aggregate related events across all Symantec-protected control points. Symantec Advanced Threat Protection: Network also integrates with our Symantec™ Advanced Threat Protection: Endpoint and Symantec™ Advanced Threat Protection: Email offerings to provide a consolidated view of advanced attack activity across the organization.

Uncover and Prioritize Advanced Attacks

Symantec Advanced Threat Protection: Network uncovers advanced threats that attempt to infiltrate the organization through common network protocols. Today's network protection solutions typically rely almost entirely on sandboxing capabilities to find attacks. By contrast, Symantec Advanced Threat Protection: Network includes a complete set of protection capabilities in addition to our innovative new Cynic sandboxing service. The product includes Symantec™ Insight reputation-based technology, which can identify suspicious files based on when they were

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

first seen, their prevalence across the Internet, as well as a number of other sophisticated techniques. Symantec™ Vantage can identify suspicious incoming network traffic, as well as help locate machines inside the network that are communicating with malicious Command-and-Control servers. The product also leverages intelligence from Symantec's massive sensor network, one of the largest cyber intelligence networks in the world, as well as data feeds from Symantec DeepSight™, assuring that it always has the most up-to-date visibility into new attack sources on the Internet.

Symantec Advanced Protection: Network also includes Symantec's new Synapse cross-control point correlation capability, which allows security analysts to zero in on the most important incidents.

Symantec Cynic™ Cloud-based Sandboxing and Payload Detonation Service

Symantec Advanced Threat Protection: Network will automatically submit all suspicious files entering the organization to 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-aware,"[2] that is, they don't reveal their suspicious behaviors when run in typical sandboxing systems. 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's new Synapse correlation technology leverages existing installations of Symantec Endpoint Protection and Email Security.cloud to prioritize events across control points. Suppose for example that a customer's traditional network security product detects that a suspicious file was delivered to an employee's machine in the organization. With existing products, the security analyst would need to manually visit the endpoint machine that received the suspicious file to ensure that it was properly blocked or removed from this computer. In contrast, if Symantec Advanced Threat Protection: Network detects the network ingress of a potential threat, the product will leverage Synapse correlation technology to automatically determine if that threat was blocked by Symantec Endpoint Protection on the endpoint. If so, the attack will be prioritized much lower on the list for the analyst. This capability drastically reduces the number of security events analysts need to examine, allowing them to zero in on just those suspicious activities of greatest risk to the organization. Synapse will also aggregate and correlate all suspicious activity across Symantec-protected endpoints, networks, and email, and fuse this with data from Symantec's massive global sensor network to identify and prioritize those critical events that pose the greatest potential danger across the organization.

Leverage Existing Symantec Investments

Symantec Advanced Threat Protection: Network leverages existing Symantec Endpoint Protection and Email Security.cloud investments. Customers can literally deploy a new installation of Symantec Advanced Threat Protection: Network and discover attacks in under an hour. The product will also export rich intelligence into third-party Security Incident and Event Management Systems (SIEMs). For example, the product can export rich data such as "computer A downloaded file B.EXE from website C.COM," rather than just traditional security data such as "virus BAD.EXE detected." In addition, Symantec Advanced Threat Protection: Network can be monitored by Symantec™ Managed Security Services.

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

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

Symantec Advanced Threat Protection: Network 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.

Key Features and Benefits

- It takes less than an hour to install Symantec™ Advanced Threat Protection: Network and start uncovering attacks
- Correlates across events from existing installations of Symantec™ Endpoint Protection and Symantec™ Email Security.cloud to greatly reduce the number of incidents that a security analyst needs to examine
- Sends all suspicious files to the new Cynic cloud-based sandboxing and detonation service
- Available in either a hardware appliance or a virtual machine (VM) form factor

Optimize Security, Minimize Risk, Maximize Return with Symantec Services

Access security experts who can provide training on Symantec Advanced Threat Protection, proactive planning and risk management as well as deployment, configuration and assessment solutions for your enterprise. To learn more, visit http://go.symantec.com/services

System Requirements

Browser Clients for the UI

Microsoft Internet Explorer 11 or later

Mozilla Firefox 26 or later

Google Chrome 32 or later

Virtual Appliance Deployment

VMware® ESXi 5.5, 6.0

Intel virtualization technology enabled

Virtual Machine (VM) Requirements

- Four CPUs (physical or logical)
- At least 32 GB memory
- At least 500 GB disk space

Physical Appliance Deployment

	Appliance Model 8840	**Appliance Model 8880**
Form Factor	1U Rack Mount	2U Rack Mount
CPU	Single, Intel Xeon Six-core	2 x 12 core Intel Xeon
Memory	32 GB	96 GB
Hard Drive	1 x 1TB drive	RAID 5 4 x 300GB
Power Supply	Non-redundant PSU	2 x 750W Redundant power supply
Network Interface Cards	Four Gigabit Ethernet ports:	Four 10Gigabit Ethernet ports Two 1Gigabit Ethernet ports
	1 WAN / LAN pair 1 Management port 1 Monitor port	2 WAN / LAN pairs (10Gigabit) 1 Management port (1Gigabit) 1 Monitor port (1Gigabit)

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

21349720-2 10/15