Symantec Advanced Threat Protection 2.3: Network

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.

This problem is only growing. Over 430[1] million new pieces of malware were found in 2015. In addition, Symantec saw a 125% increase in zero-day vulnerabilities and 55% increase in targeted attacks from 2015. Today, preventing threats is simply not enough. Attackers are moving faster. At some point, they will find their way through. A recent report[2] shows that it can take organizations 120 days on average to remediate found vulnerabilities. Undetected threats and slow remediation can leave customers' organization exposed and result in significant cost, including but not limited to the loss of intellectual property and sensitive data, financial losses, reputation damage. On top of that, significant amount of alerts and the user impact from infection could raise IT overhead and disrupt customers' business

Solution Overview

Symantec Advanced Threat Protection Network

Symantec Advanced Threat Protection: Network is one module of the broader Symantec Advanced Threat Protection (ATP) solution that **Uncovers, Prioritizes, Investigates, and Remediates** advanced threats across endpoint, network, email, and web traffic in a single console. It is available in either a hardware appliance or virtual machine form factor. Symantec ATP: Network fuses intelligence from Symantec's massive global sensor network, to uncover and investigate threats that evade individual point products. By monitoring all traffic coming into or out of the network, it is able to inspect traffic using the multiple advanced detection technologies.

The product automatically sends suspicious files to Symantec Cynic™ sandboxing system for rapid detection of even the most complex and the stealthiest advanced attacks. And, if customers also have Symantec Advanced Threat Protection: Endpoint module, Email module, or Roaming module, Symantec ATP can correlate threat events detected from these control points and prioritize incidents so that customers can focus on what matters the most. Symantec's Synapse™ correlation technology automatically aggregates related events across all Symantec-protected control points in customers' organization, providing a consolidated view of advanced attack activity in one place.

Symantec

Key Features and Benefits

- Takes less than an hour to install Symantec Advanced Threat Protection: Network and start uncovering targeted attacks
- Prioritizes what matters the most by correlating across events from other Symantec-protected control points to greatly reduce the number of incidents that a security analyst needs to examine
- Uncover stealthy threats that others miss with multiple technologies, including reputation analysis, IPS, and our unique cloud-based sandboxing and detonation
- Blacklist or whitelist files and URLs once they are identified malicious
- Customize your own incident response flow with open APIs and third-party SIEM and workflow tools integration
- Available in either a hardware appliance or a virtual machine (VM) form factor

Uncover Advanced Attacks

Best Detection and Accuracy in Its Class[3]

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 heavily on sandboxing capabilities to find attacks. By contrast, Symantec Advanced Threat Protection: Network includes a complete set of protection technologies in addition to the innovative Cynic sandboxing and detonation.

Powered by Symantec Insight reputation-based technology, Symantec ATP: Network identifies suspicious files based on when they were first seen, their prevalence across the Internet, as well as a number of other sophisticated techniques. It also identifies suspicious incoming network traffic and helps locate machines inside the network that are communicating with malicious Command-and-Control servers. Customers have the most up-to-date visibility into new attack sources on the internet as Symantec leverages one of the world's largest civilian threat intelligence networks as well as data feeds from Symantec DeepSight™

Sandbox with both physical and virtual execution

Symantec uncovers today's most complex targeted attacks with our Cynic™ technology, a cloud-based sandboxing and payload detonation capability built from the ground up. Symantec ATP: Network automatically submits all suspicious files entering the organization to Cynic, which leverages advanced machine learning-based analysis combined with global threat intelligence to uncover even the stealthiest and the most persistent threats. It provides a detailed detonation report consisting of process and stack trace as well as any network trace, including command and control call traffic information, so that all relevant information is available to the incident responder from a single pane of glass and attack components can be quickly remediated. Today, 28 percent of advanced attacks are "virtual machine-aware," that is, they don't reveal their suspicious behaviors when run in typical sandboxing systems. To combat this, Cynic has built-in anti-evasion technology that can mimic human behavior. It can also execute suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies.

Quick search for Indicators-of-Compromise

A new feature, Dynamic Adversary Intelligence, is also included in Symantec Advanced Threat Protection. It is a high-value feed of actionable intelligence data extracted from comprehensive investigations into targeted attacks. It can quickly identify whether customers' organizations are being targeted by threat actors, so that they can respond to targeted attacks more appropriately. The new Dynamic Adversary Intelligence feed automatically searches for known Indicators-of-Compromise across the entire environment, reducing the time for customers to uncover targeted attacks.

Automatically Prioritize Critical Events

Symantec Advanced Threat Protection: Network is part of the full Symantec Advanced Threat Protection offering, which also includes endpoint, email, and roaming modules. Powered by Symantec Synapse correlation technology, Symantec ATP aggregates suspicious activities across all installed control points by leveraging existing installations of Symantec Endpoint Protection and Symantec Email Security.cloud.

Symantec's correlation technology automatically prioritizes threats based on various attributes, including the type, scope, complexity of a threat and more. For example, a customer's traditional network security product detects that a suspicious file was delivered to an employee's machine in the organization. Traditionally, 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, drastically reducing the number of security events analysts need to examine.

Leverage Existing Investments

Customers often have existing security products for incident response and security monitoring. With public API, they can leverage the products they have already invested in to conduct investigations. Symantec Advanced Threat Protection is also now integrated with Splunk and ServiceNow, the two popular SIEM and workflow products, to facilitate out-of-the-box use of our APIs. Hence, customers can optimize and customize their own incident response flow, maximizing their existing investment.

Customers can 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 traditional security data such as "virus BAD.EXE detected." In addition, Symantec Advanced Threat Protection: Network can be monitored by Symantec Managed Security 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
THROUGHPUT	500Mbps	2Gbps
NETWORK INTERFACE CARDS	Four Gigabit Ethernet ports: 1 WAN / LAN pair 1 Management port 1 Monitor port	Four 10Gigabit Ethernet ports Two 1Gigabit Ethernet ports 2 WAN / LAN pairs (10Gigabit) 1 Management port (1Gigabit) 1 Monitor port (1Gigabit)

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 our Services Page at: **go.symantec.com/services**

Footnotes

1. Symantec Internet Threat Report, Volume 21, April, 2016

2. Kenna Security Report, 2015

3. Dennis Technology Lab, Dec. 2015

About Symantec

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