Symantec™ Advanced Threat Protection: Endpoint

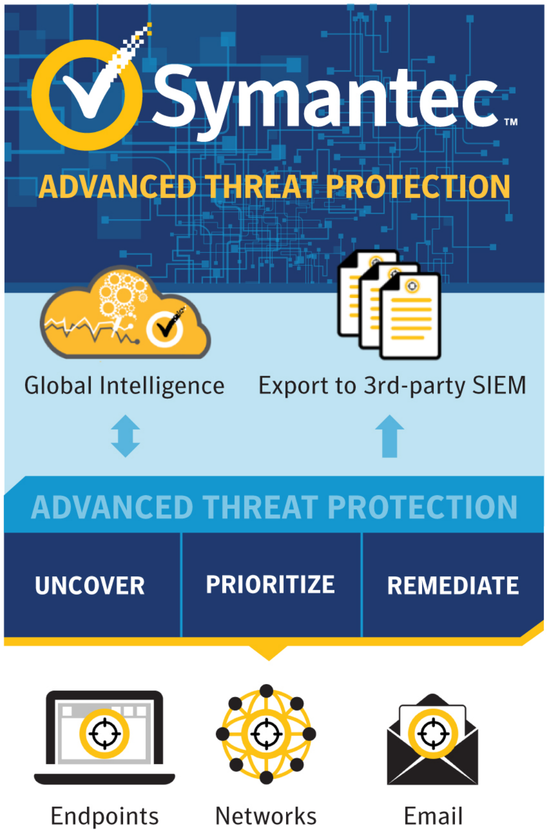
Data Sheet: Advanced Threat Protection

The Problem

Virtually all of today's advanced persistent threats leverage endpoint systems in order to infiltrate their target organizations, whether by exploiting vulnerabilities, through social engineering, via phishing websites, or some combination of all of these. And once inside the 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 the organizations' most critical systems and data.

This problem is only growing. In 2014, five out of every six large companies (2,500+ employees) were victims of targeted attacks, and 60% of all targeted attacks were launched against small-and-medium-sized organizations. Today's methods of security are clearly not keeping up, putting organizations of all sizes and in all geographies at risk.[1]

The Solution



Symantec™ Advanced Threat Protection: Endpoint is a new solution to uncover, prioritize, and remediate advanced attacks across all of your endpoints, leveraging existing investments 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. And, if you have 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.

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 – how a threat entered the organization, a list of machines that have the threat, what new files the threat created, what files it downloaded, etc. Analysts can also hunt for any Indicators-of-Compromise by searching every endpoint in the organization. For example, a security analyst can ask the product, "Show me every machine that has the file BAD.EXE," or "Show me every machine that has registry key X, setting Y, and has connected to website Z.com." And because Symantec Advanced Threat Protection: Endpoint leverages installations of Symantec Endpoint Protection, this can all be accomplished without installing any new endpoint agents.

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

Next, Symantec Advanced Threat Protection: Endpoint prioritizes what matters most, allowing security analysts to zero in" on just those specific endpoint events of importance.

Symantec Cynic™ Cloud-based Sandboxing and Payload Detonation Service

Symantec Advanced Protection: Endpoint customers 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. 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 Advanced Protection: Endpoint is part of the full Symantec Advanced Threat Protection offering, which also includes modules for network and email 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.

Remediate Fast

Once any attack component has been identified as malicious, Advanced Threat Protection: Endpoint remediates fast – with a single click of a button, customers can quickly remove and block further execution of any attack components across all endpoints. The product 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, all IP addresses where the file was downloaded from, all installed registry keys, etc. The analyst can then remediate any of these attack components as desired across all endpoints, with the click of a button.

Leverage Existing Symantec Investments

Symantec Advanced Threat Protection: Endpoint leverages and enhances your existing Symantec Endpoint Protection investments and does not require the deployment of any new endpoint agents. In under an hour, customers can deploy a new installation of Symantec Advanced Threat Protection: Endpoint and discover attacks. The product will also export rich intelligence into third-party Security Incident and Event Management Systems (SIEMs), sending 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: Endpoint can be monitored by Symantec™ Managed Security Services.

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.

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

Key Features and Benefits

- Combines global telemetry from one of the world's largest cyber intelligence networks, with local customer context, to uncover attacks that would otherwise evade detection
- With one click of a button, search for, discover, and remediate any artifacts across all endpoints in your organization.
- Leverages existing Symantec Endpoint Protection installations, requires no new endpoint agents
- Integrates with Symantec™ Advanced Threat Protection: Network, Symantec™ Email Security.cloud, and Symantec™ Advanced Threat Protection: Email, for complete cross-control point visibility and remediation of advanced attacks.

Optimize Security, Minimize Risk, Maximize Return with Symantec Services

Access Symantec's most experienced security experts who can provide Advanced Threat Protection training, proactive planning and risk management as well as deployment, configuration and assessment solutions for your enterprise. To learn more, visit our Services Page at: 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
- VMFS-5 datastore; or VMFS-3 with a minimum 2 MB block size

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