Symantec Advanced Threat Protection 2.3: Endpoint

Advanced Threat Protection

The Problem

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. Over 4301 million new pieces of malware were found in 2015. In addition, Symantec saw a 125% increase in zero-day vulnerability and 55% increase in targeted attacks. Today, preventing threats is simply not enough. Attackers are moving faster. At some point, they will find their way through. A recent report2 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 Endpoint

Symantec Advanced Threat Protection: Endpoint is Symantec's Endpoint Detection and Response (EDR) solution. It is also one module of the broader Symantec Advanced Threat Protection (ATP) offering that **Uncovers, Prioritizes, Investigates, and Remediates** advanced threats across endpoint, network, email, and web traffic in a single console. Symantec's EDR solution provides full visibility across all endpoints, allowing customers to investigate suspicious events and get every threat detail. Customers can conduct an instant search for indicators-of-compromise and remediate all instances of threats across all endpoints in minutes. The product provides customers with EDR capability without the need for them to deploy new endpoint agents.

Key Features and Benefits

- Investigate suspicious events and provide full endpoint visibility by combining global intelligence from one of the world's largest civilian threat intelligence networks with local customer context
- Quick search for any attack artifact and sweep endpoints for Indicators-of-Compromise
- Remediate every instance of threat across all endpoints in minutes, with a single click
- •Get Endpoint Detection and Response (EDR) capability without new endpoint agent to deploy
- Prioritizes what matters the most by correlating across events from other Symantec-protected control points for complete visibility and faster remediation of advanced attacks
- Customize incident response flow with third-party SIEM and workflow tools integration

Uncover and Investigate Potential Threats

Investigate suspicious events

When a stealthy threat slips through, Symantec's EDR solution enables customers to uncover and further investigate suspicious activities. Combining global intelligence from one of the world's largest civilian threat intelligence networks and local customer context across endpoints, Symantec's EDR provides granular details of threats that hit the endpoint– 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. Customers can do a quick search for any attack artifact and sweep endpoints for any Indicators-of-Compromise (IoC) by searching every endpoint in the organization. For example, customers can search for every machine that has the file BAD.EXE, or that has registry key X, setting Y, and has connected to website Z.com. All of the endpoint attack components are shown in one place.

Sandbox with both physical and virtual awareness

Symantec uncovers today's most complex targeted attacks with our Cynic™ technology, an innovative cloud-based sandboxing and payload detonation capability built from the ground up. With Symantec's EDR solution, customers can look up or submit any suspicious file to Cynic, which leverages file reputation, static based detection, network traffic analysis, and global threat intelligence to uncover even the stealthiest and the most persistent threats. Cynic 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

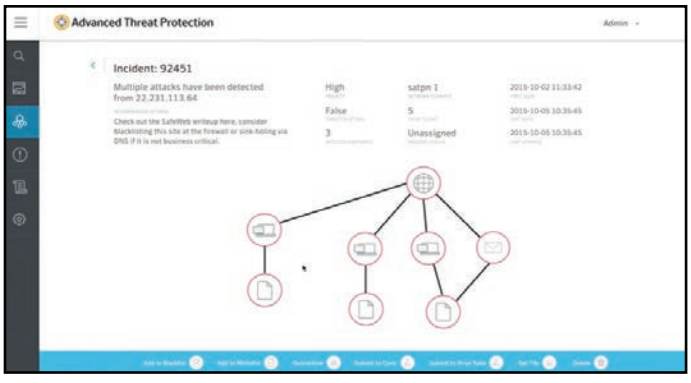
Symantec

Automatically Prioritize Critical Events

Symantec Advanced Threat Protection: Endpoint is part of the full Symantec Advanced Threat Protection offering, which also includes network, email, and roaming modules. Powered by Symantec Synapse™ correlation technology, Symantec aggregates suspicious activities across all installed control points. It automatically prioritizes threats based on various attributes, including the type, scope, complexity of a threat and more. It cuts through the noise from the significant amount of alerts, allowing customers to focus on what matters the most and "zero in" on just those specific endpoint events of importance. Customers will also be immediately alerted if there are systems that remain compromised and require immediate actions.

Remediate Complex Attacks in Minutes

Once an event has been identified as malicious, customers can contain and remediate all instances of the threat in minutes. With a single click of a button, customers can quickly delete or blacklist a file, or isolate an endpoint from communicating to the rest of the organization and the internet. Symantec's EDR solution 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 easily find out the impact of an incident and see all files used in a particular attack, all IP addresses and URLs where the file was downloaded from, and all affected registry keys with the graphical view. He can then remediate any of these attack artifacts as desired across all endpoints, with a single click, effectively containing the spread of an attack.



Leverage Existing Investments

Maximize your Symantec investments

Symantec's EDR solution leverages and enhances customers' existing Symantec Endpoint Protection investment. With Symantec Endpoint Protection installed, Symantec Advanced Threat Protection: Endpoint customers can get Endpoint Detection and Response capability without deploying any new endpoint agent. In under an hour, customers can deploy a new installation of Symantec Advanced Threat Protection: Endpoint and get full visibility across all of their endpoints. In addition, it can be monitored by Symantec™ Managed Security Services.

Leverage existing Non-Symantec investments

Customers often have existing security products for incident response and security monitoring. Symantec Advanced Threat Protection allows customers to export rich intelligence into third-party Security Information and Event Management systems (SIEMs), sending data such as "computer A downloaded file B.EXE from website C.com," rather than traditional security data such as "virus BAD.EXE detected." With public APIs, customers 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.

Symantec.

Connection™ we solve IT™

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
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 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.

Footnotes

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

2. Kenna Security Report, 2015

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.