DATA SHEET

Symantec Endpoint Detection and Response – ATP: Endpoint

Detect and Resolve Advanced Threats with a Single Agent

At-A-Glance

Detect and Expose – Reduce time to breach discovery and quickly expose scope

- Apply Machine Learning and Behavioral Analytics to expose suspicious activity, detect and prioritize incidents
- Real-time queries collect evidence of comprise data, directly communicating to the endpoint agent
- Automatically identify and create incidents for suspicious scripts and memory exploits

Investigate and Contain – Increase incident responder productivity and ensure threat containment

- Ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint processes
- Hunt for threats by searching for indicators of compromise across all endpoints in real-time
- Contain potentially compromised endpoints during investigation with endpoint quarantine

Resolve – Rapidly fix endpoints and ensure the threat does not return

- Delete malicious files and associated artifacts on all impacted endpoints
- Blacklist and whitelist files at the endpoint
- Enhanced reporting allows any table to be exported for incident resolution reports

Enhance Security Investments – Pre-built integrations and Public API's

- Easily extend ticketing and service automation workflow into existing processes with ServiceNow app
- Visualize EDR data alongside other security information using pre-built apps for Splunk and QRadar
- Smooth integrations with other security products with Open API's

Introduction

Enterprise's are increasingly under threat from sophisticated attacks. In fact, research has found that threats dwell in a customer's environment an average of 190 days[1]. These Advanced Persistent Threats use stealthy techniques to evade detection and bypass traditional security defenses. Once an advanced attack gains access to a customer environment the attacker has many tools to evade detection and begin to exploit valuable resources and data. Security teams face multiple challenges when attempting to detect and fully expose the extent of an advanced attack including manual searches through large and disparate data sources, lack of visibility into critical control points, alert fatigue from false positives, and difficulty identifying and fixing impacted endpoints.

Advanced Threat Protection (ATP): Endpoint Overview

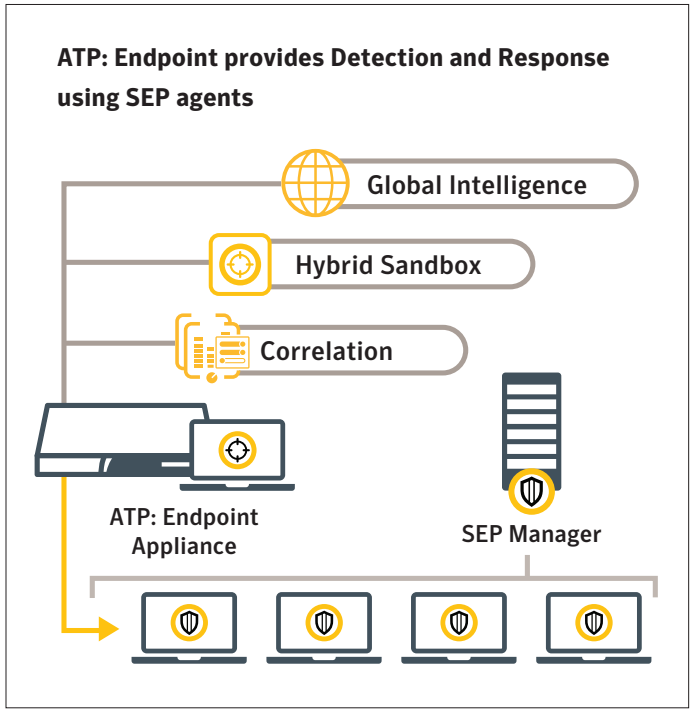
Symantec ATP: Endpoint leverages the integrated Endpoint Detection and Response (EDR) capabilities in Symantec Endpoint Protection (SEP) and can be deployed within an hour

[1] Ponemon 2017 Cost of Data Breach Study: United States

without the need for additional agents. It gives investigators the tools to expose, contain and resolve breaches resulting from advanced attacks. ATP: Endpoint exposes advanced attacks with precision machine learning and behavioral analytics. It minimizes false positives and helps ensure high levels of productivity for security teams powered by the world's largest civilian global threat intelligence network (GIN). ATP: Endpoint capabilities allow incident responders to quickly search, identify and contain impacted endpoints while investigating threats using either on-premises or cloud-based sandboxing. In addition, continuous recording of system activity supports full endpoint visibility and real-time queries. And ATP: Endpoint ensures breach resolution by deleting malware and associated artifacts from impacted endpoints from a single console with a single click.

Detect Threats – Even Ones That 'Hide In Plain Sight'

ATP: Endpoint uses multiple approaches to detect advanced threats. Advance machine learning and Behavioral analysis identifies bad and suspicious files. And ATP: Endpoint detects file-less attacks that make use of memory exploits and PowerShell scripts.

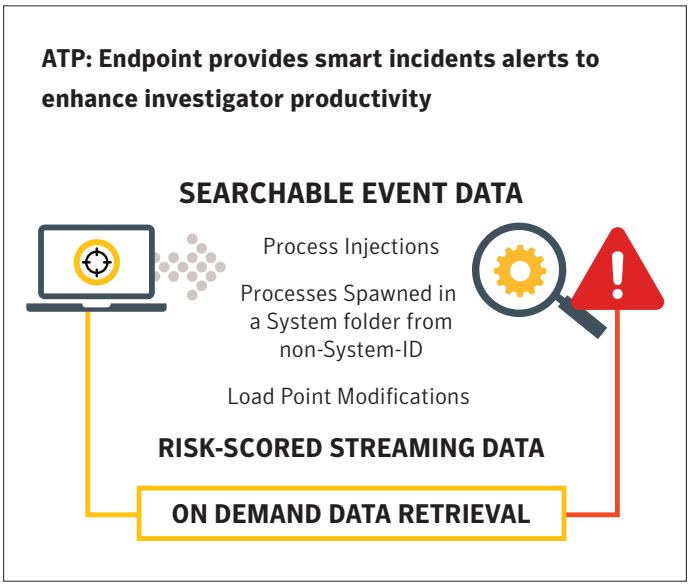


Increase Investigator Productivity

ATP: Endpoint increases investigator productivity by prioritizing incidents by risk. And ATP: Endpoint automatically generates incidents for targeted attacks identified through Symantec's Dynamic Adversary Intelligence.

In addition, investigators can take advantage of Endpoint Activity Recording to hunt for Indicators of Attack and perform endpoint analysis. ATP: Endpoint supports on-demand retrieval for a wide range of events including session, process, module load point modifications, file and folder operations, registry changes and network connection activity.

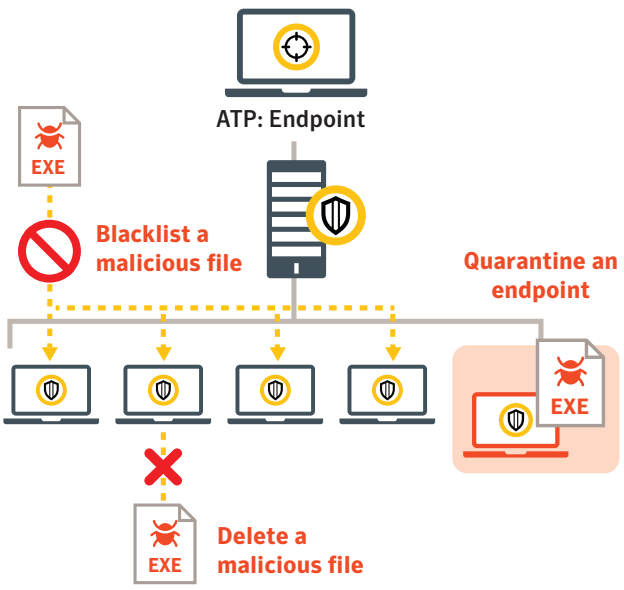
According to Symantec Internet Safety and Threat Report (ISTR), more than 20% of the malware is VM-aware which means they evade detection in a traditional sandbox. ATP: Endpoint can detect such VM-aware threats by employing advanced techniques that include mimicking human behavior and if necessary using physical servers for detonation.



Rapidly Fix Endpoints

ATP: Endpoint supports rapid remediation of impacted endpoints including file deletion, blacklisting and endpoint quarantine. Using ATP: Endpoint responders can take action from a single console and with one click apply a fix across multiple endpoints.

ATP: Endpoint allows security teams to respond to advanced attacks in minutes



Correlation Across Critical Control Points

ATP: Endpoint is part of a broader Advanced Threat Protection (ATP) platform that includes visibility and correlation of events from network and email modules. The ATP: Endpoint appliance automatically correlates events from SEP, email and network activity. Symantec's ATP modules (ATP: Endpoint, ATP: Network and ATP: Email) detect and prioritize threats from a single agent and one console.

Symantec Advanced Threat Protection	**ENDPOINT**	Expose, investigate, and resolve attack impacts across all endpoints	Leverage Symantec Endpoint Protection
	NETWORK	Protect and detect advanced threats entering the network using multiple layers of technology	Virtual or Physical appliance
	EMAIL	Protect and detect advanced threats entering via email, identifies targeted attacks.	Leverage sandbox and Email Security Cloud

Highlighted 3.0 Features

Endpoint Activity Recorder

Continuous visibility across SEP endpoints

- Records critical system activity including file operations, registry key changes, process activity, load point changes and user login and logoff
- Events of interest are selected for further analysis and incident generation based on heuristics and expert rules

Endpoint Analysis

Search, filter and retrieve events for specific endpoints

- Search EDR database and endpoints directly
- Incident investigators can quickly filter for specific attributes, identify uncommon values and pivot to relevant entity page
- Retrieve process events for a specific endpoint for analysis

File-less Threat Detection

Detect and view suspicious script and memory exploits

- View PowerShell processes, rules-based detection identifies and creates incidents for suspicious scripts
- Memory Exploits blocked by Symantec Endpoint Protection will automatically generate incidents for investigator to analyze for associated artifacts

Hybrid Sandboxing

Detonate files on-premises or in the cloud

- Detonate suspicious files using cloud-based or on-premises sandboxing
- Supports physical and virtual suspicious file awareness
- Leverage file reputation, network traffic analysis and global telemetry

Enhanced Public APIs and New Integrations

Ease custom integrations and leverage pre-built components

- New Public APIs support new features including Endpoint Activity Recorder capabilities
- Pre-built components for popular SIEM and ITSM solutions (Splunk, QRadar, ServiceNow)
- Use Active Directory users and groups for console access

Requirements

Symantec Endpoint Protection 14.X, Symantec Endpoint Protection 12.1 RU6 MP7 (Recorder only supported with ATP: Endpoint for SEP 14 and above)

Server Specifications			
Form Factor	**8880-30**	**8840***	**VMware ESXi**
	2U Rack Mount	1U Rack Mount	Virtual Machine
CPU	2 x Intel Xeon E5-2697 v4, 2.3GHz, 18Core, 145W	Intel Xeon E3-1270 V5, 3.6GHZ, 4C/8T, 80W	12 CPUs
Memory	192 GB	32 GB	48 GB
Hard Drive	RAID 10, 4 x 300GB 15K SAS RAID 10, 4 x 1.8TB 10K SAS	2 x 1TB 7.2K RPM NLSAS 12Gbps 2.5" (400-ALUN)	500 GB (should be extended for an additional 1TB to support Endpoint Activity Recording)
Network Interface Card	4 x 1 Gigabit Ethernet Ports 4 x 10 Gigabit Ethernet Ports with Bypass	2 x 1 Gigabit Ethernet Ports 2 x 1 Gigabit Ethernet Ports with Bypass	2 x 1 Gigabit Ethernet Ports
DVD-ROM	DVD ROM, SATA	DVD ROM, SATA	NA
Power Supply	2 x 750W Redundant Power Supply	2 x 350W Redundant Power Supply	NA

*8840 appliance does not support endpoint activity recording

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, 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 and LifeLock product suites to protect their digital lives at home and across 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.

Symantec

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