Solution Brief

Protect with the Most Complete Endpoint Security in the World & Save Money, Too

Prevent, detect, and respond, all through a single agent

Innovative Threats Require Innovative Protection

Advanced attacks and the threats they deliver are more complex and varied than ever. According to the Symantec Internet Security Threat Report[1], nearly one million new pieces of malware are detected every day. Attackers use stealthier tactics to deliver malware that is harder to detect.

Customers seek endpoint security products that advance faster than the adversary to stop threats before they compromise endpoints. Because endpoints are vulnerable and relatively easy to infiltrate, the endpoint security market is crowded with point solution vendors filling gaps. These unintegrated point products increase complexity and the total cost of ownership, as customers must coordinate multiple vendors, numerous purchasing cycles, maintenance, and additional software and hardware.

Simply blocking threats is not enough of a defense, either. A recent report[2] indicates that 44 percent of companies still have compromised endpoints, even with endpoint security products. And a victimized business takes 146 days on average to detect the breach[3]. The consequence of a breach can be devastating, costing an on average $4 million[4] to remedy. To navigate the threat landscape, customers need to

- block the majority of threats
- detect anomalies
- respond to the stealthiest threats once they slip through

Complete Your Endpoint Security

Symantec provides the full cycle of endpoint security, from threat prevention to detection and response. It protects, detects, investigates, and remediates threats across all endpoints through a single agent by

- Blocking threats across the attack chain with few false positives
- Detecting anomalies and investigating suspicious events
- Remediating complex attacks in minutes, with one click
- Optimizing existing investments without adding new agents

Block Threats Across the Attack Chain

Blocking advanced threats before they infect your endpoint is the key to a secure infrastructure. Symantec Endpoint Protection 14 is designed to outpace a dynamic threat landscape. Powered by advanced machine learning, exploit mitigation, and real-time behavioral analysis, Symantec Endpoint Protection 14 effectively stops advanced threats before they execute. It applies the collective wisdom of Symantec's Global Intelligence Network, the world's largest civilian threat intelligence network, to stop malicious threats with very few false positives. All of these protection layers are integrated into a single lightweight agent working with the other products in your infrastructure for orchestrated response at the endpoint.

Symantec

Detect and Investigate Suspicious Events

After detection, you need to investigate suspicious activities, eliminate threats, and any artifacts they leave behind. With Symantec Advanced Threat Protection: Endpoint, our endpoint detection and response (EDR) solution, you can complete every step.

Uncover More Anomalies

Symantec exposes complex targeted attacks with cloud-based sandboxing and payload detonation. With Symantec EDR, you can look up or submit any suspicious file. Once in our sandbox environment, we apply advanced machine learning, file reputation, static based detection, network traffic analysis, and global threat intelligence to uncover even the most persistent threats. A detailed detonation report, with all relevant information, is available to incident responders from a single console.

Currently, 28 percent of advanced attacks are 'virtual machine-aware'.[5] To combat this, Symantec's cloud sandbox has built-in anti-evasion technology that mimics human behavior and executes suspicious files on both physical and virtual hardware, uncovering attacks that would otherwise evade traditional sandbox detection.

Investigate Suspicious Events

Should a threat slip through your defenses, Symantec EDR solution allows you to further investigate suspicious activities. By combining global intelligence from the world's largest civilian threat network with local customer context across endpoints, Symantec EDR provides granular details of any threat that manages to hit an endpoint. These details include:

- how a threat entered the organization
- a list of compromised machines
- what new files the threat created
- what files it downloaded, and more

Symantec EDR automatically searches for indicators of compromise (IoCs) and alerts security analysts if their organization is under a targeted attack, allowing them to respond to threats more sharply. Analysts can also hunt for any attack artifact and sweep all endpoints for a particular IoC to quickly retrieve a file from any endpoint.

Remediate Complex Attacks in Minutes

Once a malicious threat is identified, Symantec EDR allows containment and remediation of all instances in minutes. Through blacklisting, you will quickly remove or block further execution of all attack components across all endpoints with a single click of a button. And you can isolate an endpoint from communicating, either internally or externally.

Symantec EDR provides unique visualization of related IoCs of an attack, including a complete graphical view of how they connect. Security analysts can see all files, registry keys, IP addresses, and URLs used in a particular attack, then determine the impact of an incident.

Optimize Existing Investments

With Symantec EDR, you can optimize your existing investments in Symantec and non-Symantec products:

- It enhances your existing Symantec Endpoint Protection investment by adding EDR capabilities; no new endpoint agent is required.
- Symantec EDR lets you export rich intelligence into third-party security information and event management systems (SIEMs) to conduct investigations.
- It is also integrated with Splunk® and ServiceNow®, popular SIEM and workflow products that use out-of-the-box APIs. These integrations allow you to customize your own incident response flow.

Complete Security with Fewer Costs

Advanced attacks are relentless, growing in frequency and complexity. Blocking threats is simply not enough of a defense. You need unparalleled endpoint security that

- blocks the majority of threats before endpoint infection
- detects anomalies and investigates suspicious events if malware slips past
- swiftly remediates every attack artifact across all endpoints

The most effective defense against advanced attacks is a layered one that completes the full security cycle. Symantec offers the strongest threat prevention available, validated by 3rd party tests, and powerful endpoint detection and response. All with lower total cost of ownership.

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

[1] Symantec ISTR 2017
[2] Gartner MQ for Endpoint Protection Platform, February 2016
[3] FireEye M-Trend Report 2016
[4] Cost of Data Breach Study, Ponemon Institute for IBM, June 2016
[5] Symantec ISTR 2016