SOLUTION BRIEF

Symantec Endpoint Security

Complete Endpoint Defense

Implementing a cohesive endpoint security strategy is more important than ever

Endpoints are a primary target for cyber attackers. In 2018 new endpoint threats significantly increased[1], mobile malware variants surged[2], and attack frequency rose.[3]

In response, many companies try to bolster their overall defense by adding multiple endpoint protection products. Unfortunately, this approach actually weakens an organization's security posture.

Ponemon Institute found organizations install, on average, seven different endpoint agents to support IT management and security.[4] Each agent operates independently with its own console and set of rules and policies—all of which need to be configured, rolled out, managed, and maintained. In addition to creating more IT overhead and costs, multiple products introduce defense gaps and errors, increasing the chances you'll miss a threat. We see the evidence of this in rising attack dwell times, which now average over 190 days.[5]

Yet organizations with fewer endpoint agents may also suffer as they settle for 'less than' security. That is because virtually every broad endpoint defense delivered by a single vendor does not offer the best available capabilities across all security categories.

With Symantec, you can end the compromises. Why choose between the best security and the greatest simplicity when you can have both?

Introducing Symantec Endpoint Security

Symantec delivers the most complete, integrated endpoint security platform on the planet. As an on-premises or cloud-based solution, the single-agent Symantec platform protects all your traditional and mobile endpoint devices, providing interlocking defenses at the device, application, and network level and using artificial intelligence (AI) to optimize security decisions. A single cloud-based management system simplifies protection, detecting and responding to all the advanced threats targeting your endpoints. Symantec also offers AI-guided policy management, unique add-on security for modern operating system (OS) devices, and robust endpoint hardening technologies such as application isolation, application control, and Active Directory (AD) protection.

Symantec Endpoint Security ensures you get complete endpoint defense—in a single, integrated solution—to simply and efficiently protect your endpoints.

Prevent threats

Symantec multilayer endpoint defense immediately and effectively protects against file-based and fileless attack vectors and methods. Its machine learning and artificial intelligence uses advanced device and cloud-based detection schemes to identify evolving threats across device types, operating systems, and applications. Attacks are blocked in real-time, so your endpoints maintain integrity and you avoid negative impacts.

[1, 3] *"The 2018 State of Endpoint Security," Ponemon Institute, October 2018.*
[2] *"Internet Security Threat Report – Volume 23," Symantec, 2018.*
[4] *"The 2017 State of Endpoint Security Risk," Ponemon Institute LLC, November 2017.*
[5] *"2017 Cost of Data Breach Study," Ponemon Institute, June 2017.*

Symantec™

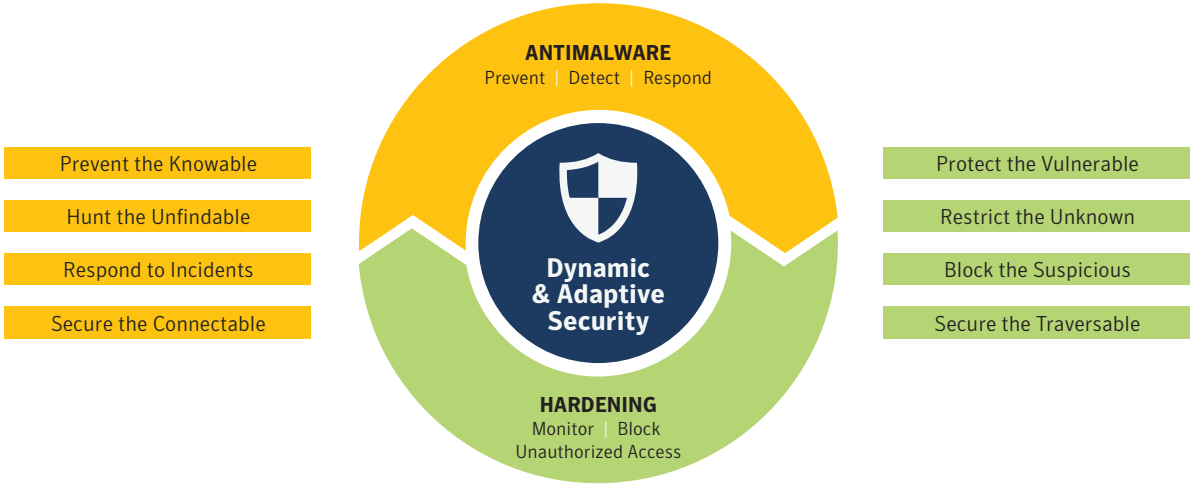


Figure 1. Symantec Endpoint Technology Approach

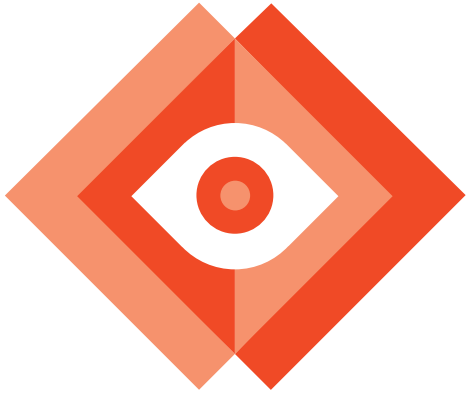
Symantec threat prevention capabilities include:

- **Fileless attack protection**—Block malicious behaviors, whether they're known to be bad or merely appear suspicious.
- **Application isolation**—Safely download and use any application; shield productivity tools from vulnerability exploits and isolate suspicious and malicious applications so they can't execute privileged operations.
- **Reduced endpoint attack surface**—Block unauthorized and unwanted applications from running (Endpoint Application Control).
- **Enhanced mobile application security**—Analyze mobile apps to guard against vulnerabilities, sensitive data loss, and privacy invasive actions (Endpoint Protection Mobile).
- **Advanced persistent threat defenses**—Disrupt attack reconnaissance and stop lateral movements (unique Threat Defense for Active Directory).
- **Active protection for cloud-connected users**—Keep users safe from threats such as rogue Wi-Fi, malicious apps, and OS vulnerabilities (Cloud Connect Defense).
- **Ecosystem integration**—Extend endpoint security across partner solutions and the Symantec product portfolio to improve your overall security infrastructure.

Rapidly discover and resolve threats

Quickly detect, expose, and resolve threats to thwart attacks and avoid a damaging data breach. The Symantec zero-trust approach uniquely combines endpoint detection and response (EDR) technologies and unmatched security operations center (SOC) analyst expertise, giving you the tools you need to quickly close out endpoint incidents and minimize attack impacts.

Symantec Endpoint Security integrates EDR capabilities in a single-agent architecture that precisely detects advanced attacks, provides real-time analytics, and enables you to actively hunt threats and pursue forensic investigations. Its built-in, automated playbooks, which include MITRE cyber analytics that recommend investigations based on the MITRE ATT&CK model, make security analysts more productive.



Symantec EDR capabilities include:

- **Contextual analysis**—Gain the context you need (with easy-to-read explanations) to quickly make optimal security decisions when confronting an advanced endpoint attack.
- **Cloud-based analytics**—Detect known adversaries as well as new attack patterns with analytics continuously trained by global telemetry.
- **Resolution guidance**—Boost SOC productivity and remediate attacks faster and more completely.
- **Complete, risk-scored endpoint activity recording**—Quickly analyze the entire attack chain to rapidly remediate systems.
- **Orchestration**—Efficiently and effectively protect your endpoints with EDR capabilities that work in concert with Symantec network and content analytics.
- **Pre-built integrations**—Enhance your existing infrastructure [including your security incident and event management (SIEM), orchestration, and ticketing systems] and streamline SOC operations.

Are you short on in-house security personnel or expertise? Symantec Managed Endpoint Detection and Response (Symantec Managed EDR) fortifies SOC teams, or outsourced EDR operations, to swiftly discover and resolve threats.

Symantec Managed EDR services include:

- **Designated GIAC-certified SOC analyst teams**—Access help around the clock; teams are assigned based on geography and industry.
- **Fast, no-cost onboarding**—Enjoy a smooth startup and fast time to value.
- **Active threat hunting**—Head off trouble with SOC expertise and global threat intelligence.
- **Pre-authorized endpoint containment**—Disrupt attacks in progress.

Enhance operational efficiency

Easily secure your dynamic endpoint environment. A single-agent stack reduces your endpoint security footprint while integrating (and coordinating) the best available prevention, detection and response, deception, and hardening technologies. Manage everything from a single system, minimizing the time, resources, and effort required to configure, roll out, manage, and maintain your security posture. Everything you need is accessible with a click or two, improving administrator productivity and speeding response times to quickly close out security events.

Symantec Endpoint Security provides:

- **AI-guided security management**—More accurately update policies, with fewer misconfigurations, to improve your security hygiene.
- **Simplified workflows**—Ensure everything works in concert to increase performance, efficiency, and productivity.
- **Context-aware recommendations**—Achieve optimal performance by eliminating routine tasks and making better decisions.
- **Autonomous security management**—Continuously learn from administrator and user behaviors to improve threat assessments, tune responses, and strengthen your overall security posture.

The Symantec complete endpoint defense difference

Symantec Endpoint Security consolidates endpoint security tools, reduces management complexity, and improves operational efficiency—all while improving your endpoint defense.

SEP 15

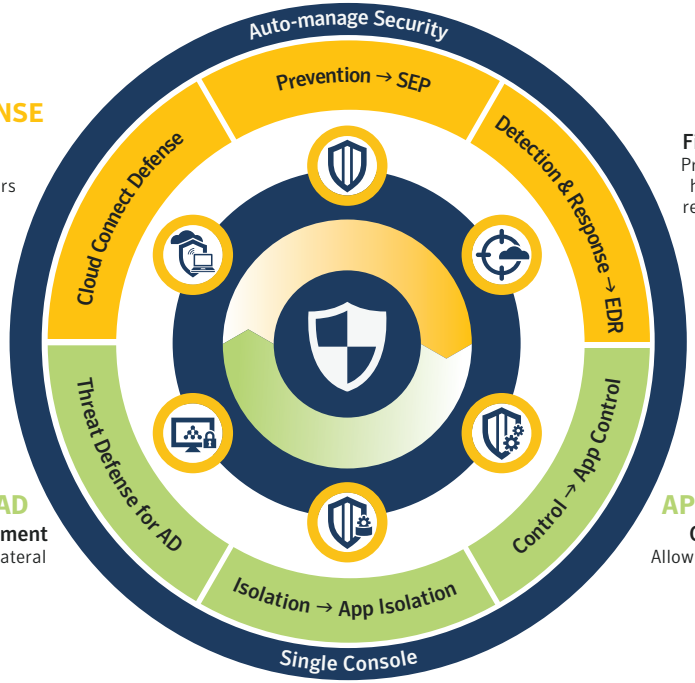
Enhance your security efficacy

Deploy multi-layer prevention technologies to help defend against advanced attack methods and vectors for traditional endpoints

SEP MOBILE

Defend your mobile devices

Mobile threat defense with comprehensive detection of risky and unwanted applications, networks and behavior



CLOUD CONNECT DEFENSE

Ensure network integrity

Proactive validation of network integrity for cloud-connected users everywhere

SYMANTEC EDR

Find the unfindable & remove it

Precise detection and proactive threat hunting to fully expose, contain and resolve persistent threats in real-time

THREAT DEFENSE FOR AD

Detect and prevent lateral movement

Disrupt reconnaissance and prevent lateral movement in Active Directory

APPLICATION CONTROL

Control your applications

Allow only trusted and safe applications to run in your environment

APPLICATION ISOLATION

Protect the good and jail the bad

Achieve complete visibility into apps running while defending known good and isolate suspicious apps

New Symantec Endpoint Security suites

Symantec has created unique endpoint security suites to match the level of endpoint defense to your security maturity and needs.

	Symantec Endpoint Protection	Symantec Endpoint Protection w/ Detection & Response	Symantec Advanced Endpoint Defense Suite (AED)	Symantec Complete Endpoint Defense Suite (CED)
Security Maturity	Prevention	Prevention + Detection + Response	Prevention + Hardening	Prevention + Hardening + Detection + Response
Security Need	"Need protection against sophisticated threats and attack vectors"	"Need protection and response capabilities to address evasive threats"	"Need a combination of advanced protection to defend against more advanced threats"	"Need prevention, hardening and precise detection with proactive threat hunting to fully expose and resolve the most advanced threats"
Endpoint Protection 14.x (On-Premises)	●	●	●	●
Endpoint Protection 15 (Cloud Delivered)	●	●	●	●
Endpoint Protection Manager (On-Prem | Hybrid)	●	●	●	●
Cyber Defense Manager (Cloud Delivered)	●	●	●	●
Endpoint Detection and Response		●		●
Endpoint Application Control			●	●
Endpoint Application Isolation			●	●
Endpoint Threat Defense for Active Directory			●	●
Endpoint Cloud Connect Defense				●

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, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Take the next step

For more information, please visit https://www.symantec.com/products/endpoint.

Symantec™

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

19C208104_SB_Endpoint_Security_EN