Symantec
A Division of Broadcom

Product Brief

Symantec Endpoint Security

Implementing Cohesive Endpoint Security Strategy Is More Important Than Ever

Introduction

Endpoints are a primary target for cyber attackers. As the consequences and resulting damage of successful attacks grow, many companies try to bolster their overall defense by adding multiple endpoint protection products. Unfortunately, this approach weakens an organization's security posture.

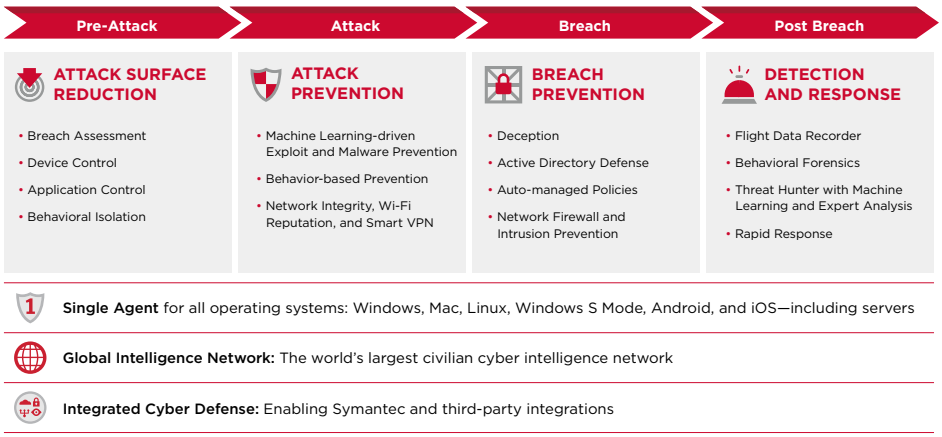
Ponemon Institute found that organizations install, on average, seven different endpoint agents to support IT management and security.[1] Each agent operates independently with its own console and set of rules and policies—all of which must be configured, rolled out, managed, and maintained. In addition to creating more IT overhead and costs, multiple products introduce defense gaps and errors, increasing the chances a threat is missed.

Prevention matters as global cyber threats are more aggressive than ever and can have a staggering impact on a business. In the time it takes you to read this product brief, an entire enterprise could be compromised. The NotPetya attack reportedly crippled one of the world's largest shipping companies in only 7 minutes[2], along with thousands of other organizations. It is critical to prevent attacks as early as possible as the detection and reaction window to a modern attack is very short. Investing in Incident Response is also critical for creating a hardened security posture to prevent future attacks. With Symantec, you can end the compromises. Why choose between the best security and the greatest simplicity when you can have both?

Key Features for Symantec Endpoint Security Complete

- Protection for all endpoints: laptops, desktops, tablets, mobile devices, and servers
- Single agent for attack surface reduction, attack prevention, breach prevention, and Endpoint Detection and Response (EDR)
- Single console with real-time threat visibility
- Flexible deployment: on-premises, cloud managed, and hybrid models
- Active Directory Security
- Behavioral Isolation and Application Control capabilities
- Artificial Intelligence (AI) guided security management
- Targeted Attack Analytics and Threat Hunter
- Global Intelligence Network (GIN), one of the largest in the world, delivers real-time threat information, threat analytics, content classification, and comprehensive threat blocking data
- Integration with third-party applications including Microsoft Graph, Open C2, and other Symantec solutions through Symantec ICDx

Figure 1: Symantec Endpoint Security Complete



1: The 2017 State of Endpoint Security Risk, Ponemon Institute LLC, November 2017.
2: *You're Just 7 Minutes Away from an Infinite Toxic Loop in Your Network*, Symantec Blog, April 2019.

Enterprise Version Key Features

- Protects laptops, desktops, mobile phones and tablets
- Single agent for endpoint security
- Single console with real-time threat visibility
- Flexible deployment: on-premises, cloud-managed and hybrid models
- Artificial Intelligence (AI) guided security management
- Global Intelligence Network, one of the largest, delivers real-time threat information
- Integration with third-party applications like Microsoft Graph, Open C2, and other Symantec solutions through Symantec Integrated Cyber Defense Exchange (ICDx)

Solution Overview

Symantec Endpoint Security Complete delivers the most comprehensive and integrated endpoint security platform on the planet. As an on-premises, hybrid, or cloud-based solution, the single-agent Symantec platform protects all traditional and mobile endpoints, providing interlocking defenses at the device, application, and network level, and uses artificial intelligence (AI) to optimize security decisions. A unified cloud-based management system simplifies protecting, detecting, and responding to all the advanced threats targeting your endpoints.

Unmatched Endpoint Safety for Your Organization

Symantec Endpoint Security provides your organization with the best security at the endpoint for both traditional and mobile devices across the three attack phases—Pre-Attack, Attack, and Post Attack—with an emphasis on prevention across the attack chain for rapid containment. Proactive attack surface reduction and innovative attack prevention technologies provide the strongest defense against the hardest-to-detect threats that rely on stealthy malware, credential theft, fileless, and "living off the land" attack methods. Symantec also prevents full-blown breaches before exfiltration can occur. Sophisticated attack analytics, behavior forensics, automated investigation playbooks, and industry-first lateral movement and credential theft prevention provide precise attack detections and proactive threat hunting to contain the attacker and resolve persistent threats in real time.

Attack Surface Reduction

Symantec delivers proactive endpoint defense with pre-attack surface reduction capabilities based on advanced policy controls and technologies that continuously scan for vulnerabilities and misconfigurations across applications, Active Directory, and devices. With attack surface reduction defenses in-place, many attacker tactics and techniques cannot be leveraged on your endpoint estate.

- **Breach Assessment** continuously probes Active Directory for domain misconfigurations, vulnerabilities, and persistence using attack simulations to identify risks allowing for immediate mitigation with prescriptive recommendations on remediation.
- **Device Control** specifies block or allow policies on different types of devices that attach to client computers, such as USB, infrared, and FireWire devices to reduce the risk of threats and exfiltration.
- **Application Control** assesses the risk of applications and their vulnerabilities and allows only known good applications to run.
- **Behavioral Isolation** limits unusual and risky behaviors of trusted applications with minimal operational impact.

Attack Prevention

Symantec multilayer attack prevention 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 endpoints maintain integrity and negative impacts are avoided.

- **Malware Prevention** combines pre-execution detection and blocking of new and evolving threats (advanced machine learning, sandboxing to detect malware hidden in custom packers, and suspicious file behavioral monitoring and blocking), and signature-based methods (file and website reputation analysis and malware scanning).
- **Exploit Prevention** blocks memory-based zero-day exploits of vulnerabilities in popular software.
- **Intensive Protection** separately enables fine-grained tuning of the level of detection and blocking to optimize protection and gain enhanced visibility into suspicious files.
- **Network Connection Security** identifies rogue Wi-Fi networks, utilizes hotspot reputation technology, and delivers a policy-driven VPN to protect network connections and support compliance.

Breach Prevention

The Symantec prevention approach entails containing attackers as early as possible—at the endpoint—before they have any opportunity to persist on the network. Various AI-driven deception and intrusion prevention technologies work together to thwart network persistence before and immediately following endpoint compromise—before a full-blown breach can occur.

- **Intrusion Prevention and Firewall** blocks known network and browser-based malware attacks using rules and policies and prevents command and control setup with automated domain IP address blacklisting.
- **Deception** uses lures and baits (fake files, credentials, network shares, cache entries, web requests, and endpoints) to expose, determine attacker intent and tactics, and delay attackers through early visibility.
- **Active Directory Security** defends the primary attack surface for lateral movement and domain admin credential theft by controlling the attacker's perception of an organization's Active Directory resources from the endpoint using unlimited obfuscation (meaning fake asset and credential creation). With obfuscation, the attacker gives themselves away while interacting with *fake* assets or attempting the use of domain admin credentials on Active Directory's perception.
- **Auto-managed Policies,** based on advanced AI and ML, uniquely combines indicators of compromise and historical anomalies to continuously adapt endpoint policy thresholds or rules and keep them up-to-date and aligned with the current risk profile of your organization.

Post Breach Response and Remediation

Symantec combines endpoint detection and response (EDR) technologies and unmatched security operations center (SOC) analyst expertise, giving you the tools necessary to quickly close out endpoint incidents and minimize attack impacts. Integrated EDR capabilities, in a single-agent architecture that covers both traditional and modern endpoints, precisely detect advanced attacks, provide real-time analytics, and enable you to actively hunt threats and pursue forensic investigations and remediation.

- **Behavior Forensics** provides the ability to record and analyze endpoint behavior to identify Advanced Attack Techniques that may be using legitimate applications for malicious purposes. This data is enriched with the MITRE ATT&CK framework to help guide incidents responders during investigations.
- **Advanced Threat Hunting** tools are provided in Symantec EDR including built-in playbooks that encapsulate the best practices of skilled threat hunters and anomalous behavior detection. Incident responders can hunt across the enterprise for IOCs to include directly querying the endpoint.
- **Integrated Response** takes direct action on the endpoint to remediate by retrieving files, deleting files, isolating endpoints, and blacklisting. Symantec EDR supports automatic submission of identified suspicious files to sandboxing for complete malware analysis including exposing malware that is VM-aware.

Post Breach Response and Remediation (cont.)

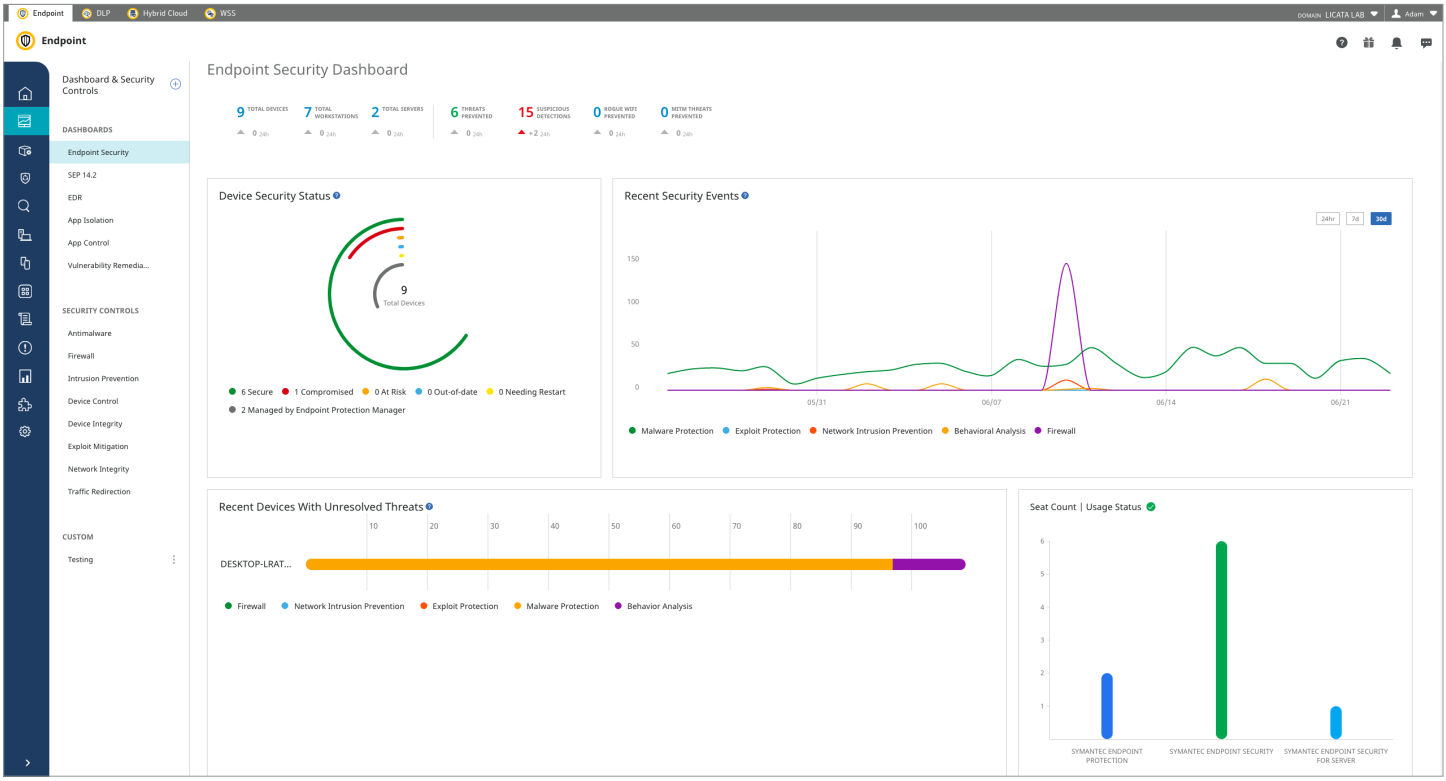
- **Threat Hunter** hunts for high-fidelity incidents and combines the power of advanced machine learning and expert SOC analysts to discover the tools, tactics, and procedures used by adversaries. It ensures that critical attacks are quickly identified with the relevant context. In addition, it delivers intuitive access to Symantec's global security data to augment your team's threat-hunting efforts.
- **Rapid Response** minimizes the time to remediate threats and respond to attackers in real time. Built-in tools and playbooks contain threats by isolating attackers and provide interactive access to endpoints.

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 technologies. Manage everything from a single cloud-based management system (Integrated Cyber Defense Manager), 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.

- **AI-guided security management** more accurately updates 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** help achieve optimal performance by eliminating routine tasks and making better decisions.
- **Autonomous security management** continuously learns from administrator and user behaviors to improve threat assessments, tune responses, and strengthen your overall security posture.

Figure 2: Endpoint User Interface



Reduce Complexity with Broad Symantec Portfolio and Third-Party Integrations

Symantec Endpoint Security is a foundational solution that facilitates integration so that IT security teams can detect threats anywhere in their network and address these threats with an orchestrated response. Symantec Endpoint Security works alongside other Symantec solutions and with third-party products via dedicated apps and published APIs to strengthen your security posture. No other vendor provides an integrated solution that orchestrates a response at the endpoint (blacklists and remediation) triggered by the detection of a threat at the web and email security gateways. Specific integrations include:

- **Symantec Web Security Service:** Redirects web traffic from roaming Symantec Endpoint Security users to Symantec Web Security Service and Symantec CASB using a PAC file.
- **Symantec Web Gateway:** Programmable REST APIs make integration possible with on-prem network security infrastructure.
- **Symantec Validation and ID Protection:** Multifactor authentication including PIV/CAC smart cards to Symantec Endpoint Security on-prem and cloud-based management consoles.
- **Symantec Content Analysis:** Utilizes dynamic on-prem sandboxing and additional threat engines for further analysis of suspicious files sent from Symantec Endpoint Security.
- **Symantec Data Loss Prevention:** Prevents data exfiltration of sensitive information by providing real-time threat intelligence of suspicious applications to DLP.

Figure 3: Symantec Endpoint Security

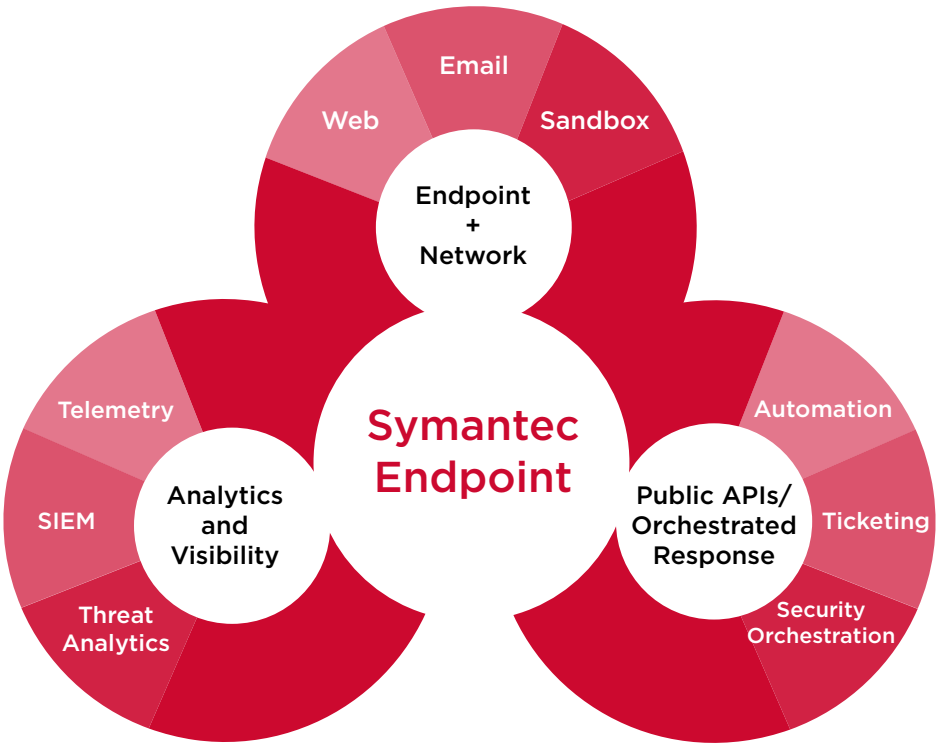


Figure 4: License Options

Features

	SEP	SES ENTERPRISE	SES COMPLETE
	Industry standard in Endpoint Protection. 5 years running as #1 Protection and now also #1 Performance by AV Test.	Extends SEP to all OSs and all devices including mobile. Offers cloud management.	Adds advanced protection, EDR, threat hunting, and other technologies for complete protection.
MANAGEMENT OPTIONS	On-Premises	On-Premises, Cloud, Hybrid	
AGENTS REQUIRED	SINGLE SYMANTEC AGENT		
DEVICE COVERAGE Corporate Owned, BYOD, UYOD	Laptop, Desktop, Server	Mobile, Tablet, Laptop, Desktop, Server	
OS COVERAGE	Windows, macOS, Linux	Windows (including S Mode and Arm), macOS, iOS, Linux, Android	

Protection Technologies

	SEP	SES ENTERPRISE	SES COMPLETE
ATTACK PREVENTION			
INDUSTRY BEST ATTACK PREVENTION	✓	✓	✓
MOBILE THREAT DEFENSE		✓	✓
SECURE NETWORK CONNECTION		✓	✓
ATTACK SURFACE REDUCTION			
BREACH ASSESSMENT			✓
BEHAVIORAL ISOLATION			✓
APPLICATION CONTROL			✓
DEVICE CONTROL	✓	✓	✓
BREACH PREVENTION ...			
INTRUSION PREVENTION	✓	✓	✓
FIREWALL	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
... BREACH PREVENTION			
DECEPTION	✓	✓	✓
ACTIVE DIRECTORY SECURITY			✓
RESPONSE AND REMEDIATION			
ENDPOINT DETECTION AND RESPONSE			✓
TARGETED ATTACK CLOUD ANALYTICS			✓
BEHAVIORAL FORENSICS			✓
THREAT HUNTER			✓
RAPID RESPONSE			✓
IT OPERATIONS			
DISCOVER & DEPLOY	✓	✓	✓
HOST INTEGRITY CHECKS	✓	✓	✓

Symantec™
A Division of Broadcom

For product information, visit our website at: go.broadcom.com/ses

SED-EPS-PB101 June 25, 2020