

## PRODUCT BRIEF

### KEY FEATURES

- Protection for all endpoints: laptops, desktops, tablets, mobile devices, and servers
- Single agent and console for complete endpoint protection, detection, and response
- Flexible deployment: on-premises, cloud managed, and hybrid models
- Adaptive protection
- Incident prediction
- Active directory security
- Advanced application control
- AI-guided security management
- Targeted attack analytics
- Real-time threat visibility powered by the Symantec Global Intelligence Network (GIN)

# Symantec® Endpoint Security

## Automate, Customize, and Maximize Protection

### Introduction

Enterprises across the globe invest heavily in endpoint security solutions to protect their valuable assets. Despite the time and money spent, more breaches are happening today than ever before. But why?

Some security solutions deliver lower protection levels to minimize false positives. Add in configuration mistakes and weak settings and it's easy to see why endpoints are being compromised.

Strong prevention is non-negotiable as global cyber threats are more aggressive and damaging than ever. Because the detection and reaction window for modern attacks is growing smaller, it's critical to prevent attacks as early as possible. Investing in incident response is also critical for creating a hardened security posture to prevent future attacks.

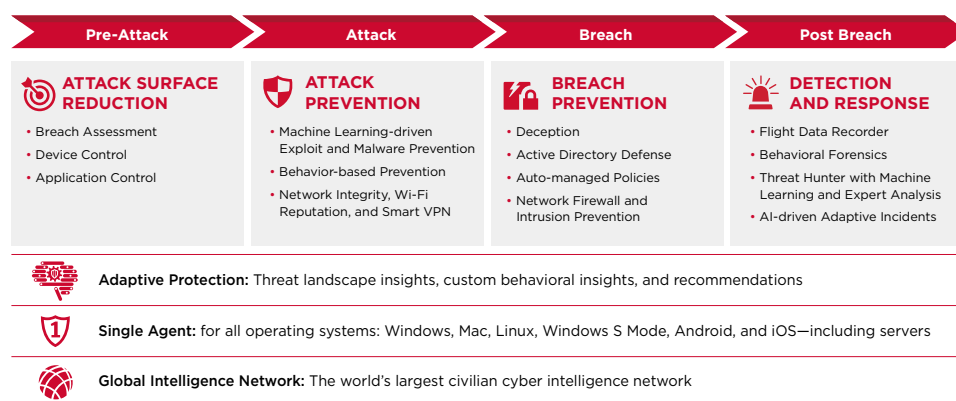
So what's the answer? The right endpoint security solution needs to maximize endpoint protection and balance detection effectiveness across all devices, operating systems, and the entire attack chain.

Symantec® Endpoint Security delivers customized protection for your organization, saving you time, money, and effort. With Symantec solutions, there's no reason to choose between the best security and the greatest simplicity. Now you can have both.

### Solution Overview

Symantec Endpoint Security delivers comprehensive, integrated endpoint security for modern enterprises. Delivered 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 levels. The unified cloud-based management console simplifies protecting, detecting, and responding to advanced threats and uses artificial intelligence (AI) to optimize security decisions.

Figure 1: Symantec Endpoint Security



## Unmatched Endpoint Safety for Your Organization

Symantec Endpoint Security provides a combination of endpoint security capabilities that enable you to reduce your overall risk, prevent attacks from reaching your endpoints, and neutralize any threats that do get in.

Symantec solutions reduce the attack surface and eliminate blind spots through Adaptive Protection, an innovative approach to help you shift left and focus on enhancing protection across the entire attack chain. Adaptive Protection automates security configuration to deliver customized protection for each organization with no manual effort. Proactive attack surface reduction and innovative attack prevention technologies provide the strongest defense against threats that rely on stealthy malware, credential theft, fileless, and living-off-the-land attack methods.

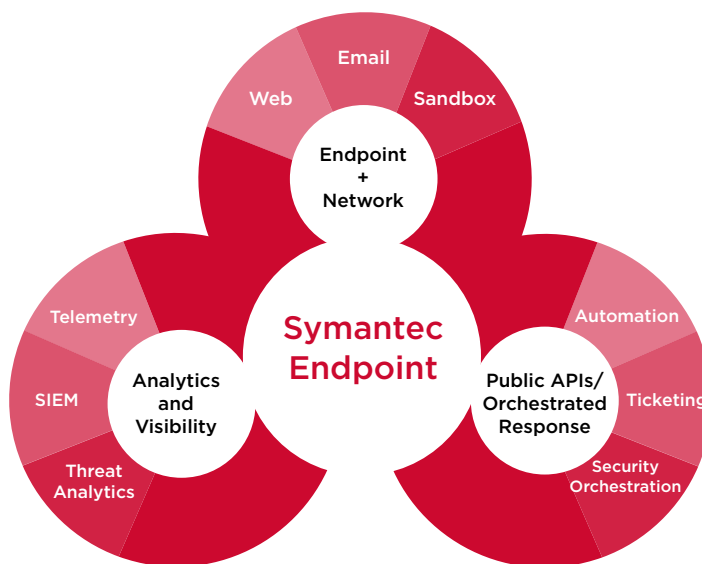
Symantec solutions also prevent full-blown breaches before exfiltration can occur. Sophisticated attack analytics, behavior forensics, automated investigation playbooks, and industry-first lateral movement and credential theft prevention provide precise attack detection and proactive threat hunting to contain attackers and resolve persistent threats in real time.

## Attack Surface Reduction

Symantec solutions enable you to proactively enhance your security posture with attack surface reduction capabilities that are customized to each environment and enforced using advanced policy controls. Leveraging technologies that continuously scan for vulnerabilities and misconfigurations across applications, Active Directory, and devices, the attack surface can be greatly reduced, eliminating the risk that many tactics and techniques pose to your endpoint estate.

- **Adaptive Protection** monitors your environment for applications and behaviors that are rarely or never used for legitimate business reasons and blocks or reduces access to those applications so they cannot be leveraged by an attacker to stage an attack or dwell in your environment.
- **Breach Assessment** continuously probes Active Directory for domain misconfigurations, vulnerabilities, and persistence using attack simulations to identify risks and allow for immediate mitigation and remediation recommendations.
- **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.

Figure 2: Symantec Endpoint Security



## Attack Prevention

Symantec multilayer attack prevention immediately and effectively protects against file-based and fileless attack vectors and methods. Using machine learning (ML) and AI alongside advanced device-based and cloud-based detection schemes, Symantec solutions 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 and signature-based methods to identify and mitigate malware. Pre-execution detection methods leverage advanced ML and sandboxing to detect malware hidden in custom packets. Behavioral monitoring and blocking of suspicious files mitigate new and evolving threats. Identify and mitigate malware with signature-based methods, including file and website reputation analysis and malware scanning.
- **Exploit Prevention** blocks memory-based zero-day exploits of popular software vulnerabilities.
- **Incident Prediction** matches the power of AI with analysis of 500,000+ real-world attack chains to predict an attacker's next four to five moves with up to 100% confidence.
- **Intensive Protection** optimizes protection against and visibility into suspicious files by fine tuning the degree of detection and blocking.
- **Network Connection Security** protects network connections and supports compliance through rogue Wi-Fi network identification, hot spot reputation technology, and a policy-driven VPN.

## Breach Prevention

The Symantec prevention approach contains attackers as early as possible, before they have an 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 systems and firewalls** block known network-based and browser-based malware attacks using rules and policies, and prevent 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 attackers, determine their intent and tactics, and delay their planned attacks.
- **Active Directory security** defends the primary attack surface against lateral movement and domain administrator credential theft by controlling the attacker's perception of an organization's Active Directory resources using unlimited obfuscation. With obfuscation, the attacker gives itself away by interacting with fake assets or attempting to use domain administrator credentials.
- **Auto-managed policies**, based on advanced AI and ML, uniquely combine indicators of compromise and historical anomalies to continuously adapt endpoint policy thresholds or rules and keep them up-to-date and aligned with the risk profile of your organization.
- **Incident prediction** automatically identifies the next steps that a specific attacker will likely take based on past attack patterns. It then applies mitigation policies to block those predicted actions, disrupting most attackers' progress before they can encrypt or exfiltrate data.

## Post-Breach Response and Remediation

Symantec solutions combine endpoint detection and response (EDR) capabilities with unmatched security operations center (SOC) analyst expertise to simplify endpoint investigation and response workflows and minimize attack impacts. Delivered through the same agent and console that protect both traditional and modern endpoints, the Symantec EDR capabilities precisely detect advanced attacks, provide real-time analytics, and enable you to pursue forensic investigations and remediation.

- **Behavior forensics** records and analyzes 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 incident responders during investigations.
- **Advanced threat hunting tools** search across recorded event metadata and identify point-in-time endpoint status. Incident responders also can hunt across the enterprise for IOCs by directly querying endpoints.

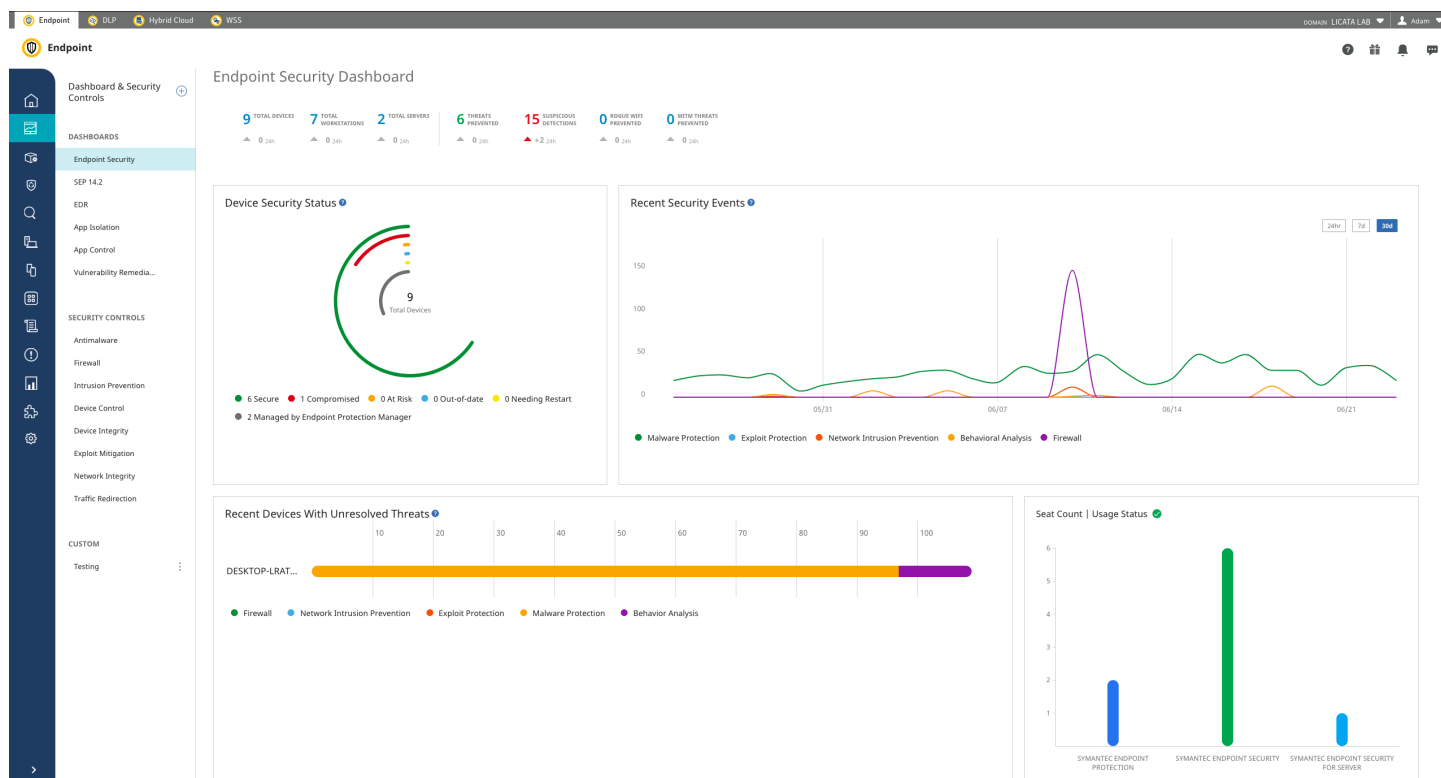
- **Integrated response** takes direct action on the endpoint to remediate by retrieving files, deleting files, isolating endpoints, and blocking access. Symantec Endpoint Security automatically submits suspicious files to a sandbox for complete malware analysis, including exposing VM-aware malware.
- **Threat hunting capabilities** identify high-fidelity incidents and uncover the tools, tactics, and procedures used by the adversaries that carried out the attack, ensuring that critical attacks are quickly identified and contextualized. Additionally, access to Symantec global security data augments your team's threat hunting efforts with insight into attacks that are seen in the wild.
- **Incident analytics** identifies potentially suspicious activities and automatically correlates associated events into an incident for investigation.
- **Adaptive incidents** highlight anomalous sources of suspicious behavior and summarizes those behaviors into a single incident that can be addressed through a simple adjustment to your Adaptive Protection policies.

## Easily Secure Your Dynamic Endpoint Environment

A single-agent endpoint security stack reduces your footprint while integrating and coordinating the best available prevention, detection, and response technologies. Managing everything from a single cloud-based management system minimizes the time, resources, and effort required to configure, deploy, manage, and maintain your security posture. Everything you need is accessible with a click or two, making administrators more productive and speeding response times to quickly close out security events.

- **Automate** policy tuning to adapt your security to your unique environment.
- **Simplify** workflows to increase performance, efficiency and productivity.
- **Optimize** performance by eliminating routine manual tasks via context-aware recommendations.
- **Improve** threat assessments, tune responses, and strengthen your overall security posture with autonomous security management that continuously learns from administrator and user behaviors.

Figure 3: Symantec Endpoint Security User Interface



## Reduce Complexity with the Symantec Portfolio and Third-Party Integrations

As a foundational solution, 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 detects threats anywhere in your network and orchestrates a response at the endpoint triggered by the detection of a threat at the web and email security gateways.

Specific integrations include the following:

### Symantec Cloud SWG

Redirect web traffic from roaming Symantec Endpoint Security users to Symantec Cloud SWG and Symantec CASB using full-tunnel redirection or a PAC file.

### Symantec Validation and ID Protection

Multifactor authentication including PIV/CAC smart cards to Symantec Endpoint Security on-premises.

### Symantec Content Analysis

















Utilize dynamic on-premises or cloud sandboxing and additional threat engines for further analysis of suspicious files sent from Symantec Endpoint Security.

### Symantec Data Loss Prevention



















Prevent data exfiltration of sensitive information by providing real-time threat intelligence of suspicious applications to DLP.

Figure 4: License Options

## Features

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

## Protection Technologies

	SEP	SES ENTERPRISE	SES COMPLETE
<b>ATTACK PREVENTION</b>			
 INDUSTRY-BEST ATTACK PREVENTION	✓	✓	✓
 MOBILE THREAT DEFENSE	●	✓	✓
 SECURE NETWORK CONNECTION	●	✓	✓
<b>ATTACK SURFACE REDUCTION</b>			
 BREACH ASSESSMENT	●	●	✓
 APPLICATION CONTROL	●	●	✓
 ADAPTIVE PROTECTION	✓	●	✓
 DEVICE CONTROL	✓	✓	✓
<b>BREACH PREVENTION</b>			
 INTRUSION PREVENTION	✓	✓	✓
 FIREWALL	✓	✓	✓
 DECEPTION	✓	✓	✓
<b>BREACH PREVENTION</b>			
 ACTIVE DIRECTORY SECURITY	●	●	✓
<b>RESPONSE AND REMEDIATION</b>			
 ENDPOINT DETECTION AND RESPONSE	●	●	✓
 TARGETED ATTACK CLOUD ANALYTICS	●	●	✓
 ADAPTIVE INCIDENTS	●	●	✓
 BEHAVIORAL FORENSICS	●	●	✓
 THREAT HUNTER	●	●	✓
 THREAT INTELLIGENCE	●	●	✓
 RAPID RESPONSE	●	●	✓
<b>IT OPERATIONS</b>			
 DISCOVER & DEPLOY	✓	✓	✓
 HOST INTEGRITY CHECKS	✓	✓	✓