Symantec Endpoint Security

Implementing a cohesive endpoint security strategy is more important than ever

Introduction

Endpoints are a primary target for cyber attackers. In 2018 new endpoint threats significantly increased[2], mobile malware variants surged[3], and attack frequency rose.[4] In response, 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 organizations install, on average, seven different endpoint agents to support IT management and security.[5] 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.

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 data sheet, an entire enterprise could be compromised. The NotPetya attack reportedly crippled one of the world's largest shipping companies in only 7 minutes[1], 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?

Solution overview

Symantec Endpoint Security delivers the most complete and integrated endpoint security platform on the planet. As an on-premises, hybrid, or cloud-based solution, the single-agent Symantec platform protects all your 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 3 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

[1] "7 minutes is all it took," Symantec Blog: https://www.symantec.com/blogs/expert-perspectives/youre-just-7-minutes-away-infinite-toxic-loop-your-network
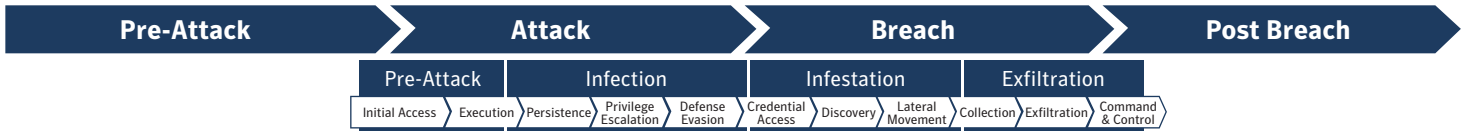[2] "The 2018 State of Endpoint Security," Ponemon Institute, October 2018.
[3] "Internet Security Threat Report – Volume 24," Symantec, 2019.
[4] "The 2018 State of Endpoint Security," Ponemon Institute, October 2018.
[5] "The 2017 State of Endpoint Security Risk," Ponemon Institute LLC, November 2017.

Symantec Endpoint Security Complete

Pre-Attack	Attack	Breach	Post Breach

	Pre-Attack	Infection	Infestation	Exfiltration	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control

Attack Surface Reduction
- Breach Assessment
- Vulnerability Remediation
- Device Control
- Application Control and Isolation

Attack Prevention
- Malware Prevention
- Exploit Protection
- Behavior based Prevention
- Secure Connection: Wi-Fi and Network Integrity and Smart VPN

Breach Prevention
- Deception
- Active Directory Defense
- Auto-managed Policies
- Network Firewall and Intrusion Prevention

Detection & Response
- Targeted Attack Analytics
- Behavioral Forensics
- Expert SOC Investigator
- Threat Hunting and Rapid Response

① **Single Agent:** Symantec Agent for Win, Win S Mode, macOS, Linux, Android, iOS

⤨ **Flexible Management:** Cloud, Hybrid and On-Premise Management Console

🌐 **Global Intelligence Network:** World's largest civilian intelligence network

👁 **Integrated Cyber Defense:** Symantec and Third Party Integrations

Service Options:
- Run it for us
- We Want Help
- We will Manage it ourselves

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.

- **Vulnerability Remediation**** enhances your security posture by providing visibility and intelligence into vulnerabilities and their associated risk. Discovered vulnerabilities are ranked by severity based on the CVSS (Common Vulnerability Scoring System) along with identification of the number of affected devices, to ensure the most critical threats are fixed first.
- **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.

- **App Isolation & App Control** allows only known good applications to run, shields known-good applications to prevent attackers from exploiting application vulnerabilities and isolates unknown apps to stop malicious behaviors such as privileged operations on files.

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 your endpoints maintain integrity and you avoid negative impacts.

- **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** enables fine-grained tuning of the level of detection and blocking separately to optimize protection and gain enhanced visibility into suspicious files.

- **Network Connection Security** identifies rogue Wi-Fi networks and utilizes hotspot reputation technology and delivers a policy-driven VPN to protect network connections and support compliance.

Breach prevention

Symantec's 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 (fake asset and credential creation). With obfuscation, the attacker gives themselves away while interacting with "fake assets" or attempting 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.

- **Targeted Attack Analytics** provides precise detections from time tested Targeted Attack Analytics used by Symantec's 3,000 researchers, based on global activity of the good and the bad, across all enterprises that comprise our telemetry set. Real-time incidents are generated—with a detailed analysis of the attacker, techniques, impacted machines, and remediation guidance.
- **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 – 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.
- **Expert SOC Investigator** is a 24x7 forensics investigation and threat hunting service that employs Symantec SOC analysts to actively detect stealthy attacks and expertly examine suspicious activity. These analysts use Symantec Endpoint Detection and Response (EDR) coupled with machine learning analytics and Symantec Global Intelligence Network correlation.

Take control of data in use on endpoints

With Symantec Endpoint DLP integration with Symantec Endpoint Security, you can stop malicious or inadvertent mishandling or theft of sensitive data in real-time, regardless of whether endpoints are on or off your network, while providing broad data loss coverage across applications, devices and platforms.

- **100% cloud-based management:** Investigate and remediate security incidents from the same cloud-based management console used by Symantec Endpoint Security (Integrated Cyber Defense Manager) for simplified management and data policy control.

- **Threat-aware data protection:** Combat data theft by malicious and low-reputation applications with unparalleled threat awareness informed by Symantec Endpoint Security App Control capabilities that stop untrusted apps and processes from accessing and exfiltrating sensitive data.
- **Common agent packaging and device management:** Secure your managed endpoints in one seamless motion with single agent package deployment for DLP and endpoint security.

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.
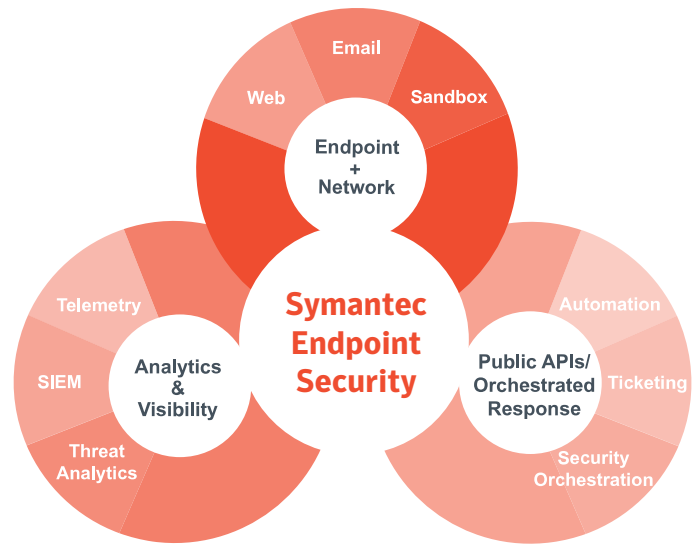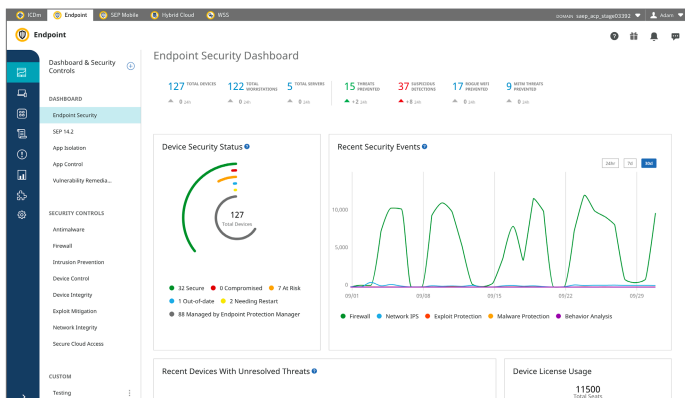
Reduce complexity with broad Symantec portfolio and third-party integrations

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.

License Options

		Symantec Endpoint Security Enterprise	Symantec Endpoint Security Complete
Management	SaaS / Pure Cloud	●	●
	On-Premise Management	●	●
	Hybrid	●	●
Operating Systems	Workstation (Windows/Mac)	●	●
	Mobile (iOS/Android)	●	●
	Server (Windows/Linux)		●
Attack Prevention	Malware Prevention	●	●
	Exploit Prevention	●	●
	Intensive Protection	●	●
	Network Connection Security**	●	●
Attack Surface Reduction	Breach Assessment		●
	Vulnerability Remediation*		Add-On
	Application Isolation and Control*		●
	Device Control	●	●
Breach Prevention	Intrusion Prevention	●	●
	Firewall	●	●
	Deception*	●	●
	Active Directory Security*†		●
	Auto-Managed Policies		●
Response and Remediation*†	Targeted Attack Analytics		●
	Behavioral Forensics		●
	Threat Hunting & Rapid Response		●
Threat Hunting	Threat Hunting Center		Add-On
Managed Services	Threat Hunting Service		Add-On

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

 *Supported on Windows workstations only
**Supported on Win 10, Win 10 in S Mode, iOS and Android devices only
† On Prem Management only

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.

Symantec.

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

20B284113_DS_SES_SOLUTION_EN