

Endpoint Security for the Enterprise

Multilayered Defense for the Cloud Generation

FAMILY BROCHURE



The diagram illustrates the Symantec Endpoint Protection 14 architecture. It features a central cloud component labeled "SEP" containing "GIN", "Analytics", "Sandbox", and "Cloud Proxy". This central cloud is connected to three main data sources: "Headquarters Data Center", "Branch Office", and "Roaming Users". A "Security Stack" is shown between the data centers and the central cloud. The central cloud is also connected to various cloud services including "Dropbox", "Gmail", "LinkedIn", "Oracle", "Salesforce", "Office 365", "iCloud", and "GoToMyPC". At the bottom, a "Personal Devices" section shows icons for Windows, Mac, and Android devices, along with a "SEP Mobile" icon. The diagram uses icons for shields to represent security and cloud symbols for cloud services.

Today's workforce is increasingly nomadic. Employees use personal and company-owned devices—desktops, laptops, tablets, and smartphones with various operating systems—to access corporate resources over different networks from virtually anywhere. Roaming users and cloud-based applications have eroded the network perimeter where enterprises have traditionally focused their security controls.

Making matters worse, traditional security approaches cannot address an evolving threat landscape that includes ransomware, stealthy attacks that dwell in a customer's environment 191 days on average,¹ and malware targeting mobile devices. In fact, the mobile workforce is more vulnerable than ever before.

Symantec™ provides a complete endpoint solution powered by the world's largest civilian Global Intelligence Network (GIN). You can secure your enterprise and mobile workforce across traditional and modern OS devices used over any network and from any location. Multiple layers of endpoint security technologies provide you with industry-leading efficacy against emerging threats. Symantec endpoint security is part of our larger Integrated Cyber Defense platform, covering web and email security, threat analytics, security orchestration and automation, and more. The single agent architecture and hybrid management capabilities enable your organization to operate more efficiently and enjoy a lower total cost of ownership.



FAMILY BROCHURE | SYMANTEC ENDPOINT SECURITY FOR THE ENTERPRISE

As a SEP portfolio customer, you benefit from the following defense-in-depth capabilities:

- **Prevention**—Multilayer endpoint security goes beyond signature blocking to fuse signatureless technologies such as advanced machine learning, behavioral analysis, memory exploit mitigation, and OS emulation with time-tested ones including intrusion prevention, reputation analysis, and application and device control. All with the simplicity of a single agent.
- **Endpoint Detection and Response (EDR)**—Detect, isolate, and eliminate intrusions, and investigate incidents, all within one agent. Extend these capabilities to roaming users and to macOS and Linux devices.
- **Deception**—Deploy baits and decoys at scale to lure attackers into revealing their intent, tactics, and targets ... without their knowledge.
- **Hardening**—Auto-classify risk levels of all endpoint applications, then isolate suspicious apps to limit vulnerability exploits and protect trusted applications.

Symantec Endpoint Protection Mobile:

For complete mobile threat defense, extend superior threat visibility and layered defense to all your mobile devices—both managed and unmanaged—with Symantec Endpoint Protection Mobile:

- Block malware processes and installation of malicious apps
- Protect your devices from compromised Wi-Fi networks
- Reduce risk from zero-day attacks and other unpatched vulnerabilities

Symantec Endpoint Protection 14—Multilayer protection

SEP 14 defeats ransomware and other threats regardless of how they attack your endpoints. With SEP 14, you can:

- Stop ransomware with a combination of artificial intelligence techniques (including advanced machine learning and behavior analysis) and time-tested technologies, such as intrusion prevention. The number of new ransomware variants more than tripled to 101 in 2016, suggesting more attackers are jumping on the ransomware bandwagon.²

- Use signatureless technology to prevent attackers from exploiting vulnerabilities in popular software, including browsers and productivity tools.
- Gain greater visibility into suspicious files, and customize protection on the fly to suit different needs, by fine-tuning machine learning, behavior analysis, intrusion prevention, and more. Use the low-bandwidth mode to protect network-constrained environments without compromising efficacy.
- Orchestrate your response to address threats quickly. SEP 14 integrates with existing security infrastructure including web and email gateways, sandboxing, and more for a unified threat response.
- Enjoy less operational complexity and a lower total cost of operation by consolidating all endpoint security uses cases—such as prevention, detection and response, deception, endpoint hardening and threat analytics—on a single, lightweight SEP agent. The same agent paves the way for high performance, significantly reducing scan times and bandwidth requirements.

SEP 14 exceeds the high bar for security requirements, and it does so without compromising user productivity.

Symantec Endpoint Protection Cloud—Uncompromising security for limited IT budgets

Symantec Endpoint Protection Cloud (SEP Cloud) delivers security-as-a-service and is ideal for organizations with limited IT resources. It protects and manages PC, Mac, and mobile devices and servers from a single console, and comes with built-in default security settings and self-service device enrollment capabilities for quickly protecting your endpoints.

SEP with Hardening—Advanced application defense

The Hardening add-on provides advanced application defense, enabling your employees to use any application safely. Implement it in minutes via an intuitive cloud console. Hardening fully supports standard employee workflows so it doesn't impact productivity.

² Symantec Internet Security Threat Report Vol. 22

SEP Hardening:

- Isolates suspicious apps
- Shields trusted ones such as browsers—2.4 browser vulnerabilities were discovered per day in 2016³ and
- Combined with SEP 14, it delivers unprecedented protection against malware and suspicious applications—unlike application-isolation point products from other vendors.

SEP with Deception—Preemptive security, early warning, and attacker Surveillance

The Deception feature baits attackers into revealing their intent, tactics, and targets ... without letting them know they're being watched—giving you the early visibility you need to adapt your security posture. SEP Deception offers the most accurate and insightful detection as well as the fastest time to value—set the trap simply by flipping a switch and quickly scale the protection enterprisewide. Become a Symantec Managed Security Services customer and you'll also benefit from 24x7 real-time SEP Deception monitoring and response by a global team of experts.

We're the only security vendor with advanced deception technology integrated in our endpoint portfolio.

Symantec Risk Insight—Threat analytics dashboard

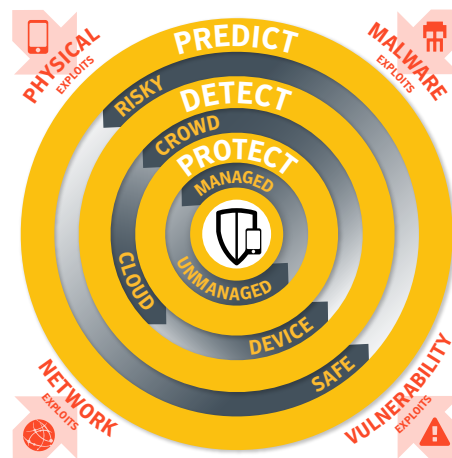
Symantec Risk Insight is a cloud-delivered threat analytics dashboard that displays your assessed security posture across your environment—customers, supply chain, and brand.

Risk Insight collects telemetry from local sources—including SEP and the Symantec Global Intelligence Network—providing visibility into granular industry and regional benchmarks and charting trends for key metrics such as malware analysis, targeted attacks, infection rate, mean time to remediate, and more. Cut costs and complexity by using cloud delivery and local telemetry—no hardware or new agents to install.

SEP Mobile—Protection from mobile cyber attacks

SEP Mobile is a complete mobile threat defense solution, extending your security outside the perimeter to protect all your mobile devices—BYOD and corporate-owned, across

Android, iOS, and Windows. It accurately predicts, detects, and effectively protects against every mobile threat vector. With its predictive, layered technology tapping massive, crowd-sourced threat intelligence, as well as device- and server-based analyses, SEP Mobile heads off identified malware, network threats, and vulnerability exploits while safeguarding user privacy and the user experience. All in one app.



SEP Mobile covers all the attack vectors the SANS Institute identifies as necessary for a complete mobile threat defense solution.⁴ It conquers each one with a layer of security and as well as crowd-sourced intelligence and analysis from a dedicated team of mobile threat experts. SEP Mobile defense layers include:

- **Physical defense**—Passcode lock prevents access to corporate information and remote wipe in case a device is lost or stolen.
- **Network defense**—Blocks malicious Wi-Fi networks by detecting and blocking malicious iOS profiles, identifies man-in-the-middle threats, stops SSL downgrading and content manipulation attacks.
- **Vulnerability defense**—Monitors devices for unpatched known vulnerabilities while security teams search for zero-day vulnerabilities in apps and operating systems.
- **Malware defense**—Uses real-time response and incremental app analysis with multiple approaches including code, structure, permissions, and behavior to detect mobile malware.

Mobile malware threats are increasing—Symantec observed 18.4 million mobile malware threats in 2016, an increase of 105 percent on 2015⁵—but with SEP Mobile you can mobilize without compromise.

^{3,5} Symantec Internet Security Threat Report Vol. 22

⁴ Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices.
© 2016 SANS™ Institute

Symantec Endpoint Detection and Response—Intruder rejection

Symantec Endpoint Detection and Response (EDR) solutions stop attacks from becoming breaches. Detect, isolate, and quickly eliminate intrusions across all your endpoints with artificial intelligence, automated incident generation, and unparalleled threat intelligence. EDR capabilities are integrated with SEP (as Advanced Threat Protection: Endpoint); Symantec EDR Cloud, delivers the same protections without requiring SEP.

Sophisticated attackers are increasingly using ‘living off the land’ tactics. One key indicator of this trend is the surge in PowerShell threats: A recent Symantec study found that 94.5 percent of PowerShell scripts were malicious⁶. Symantec EDR solutions give you the tools to expose, contain, and resolve breaches resulting from advanced attacks.

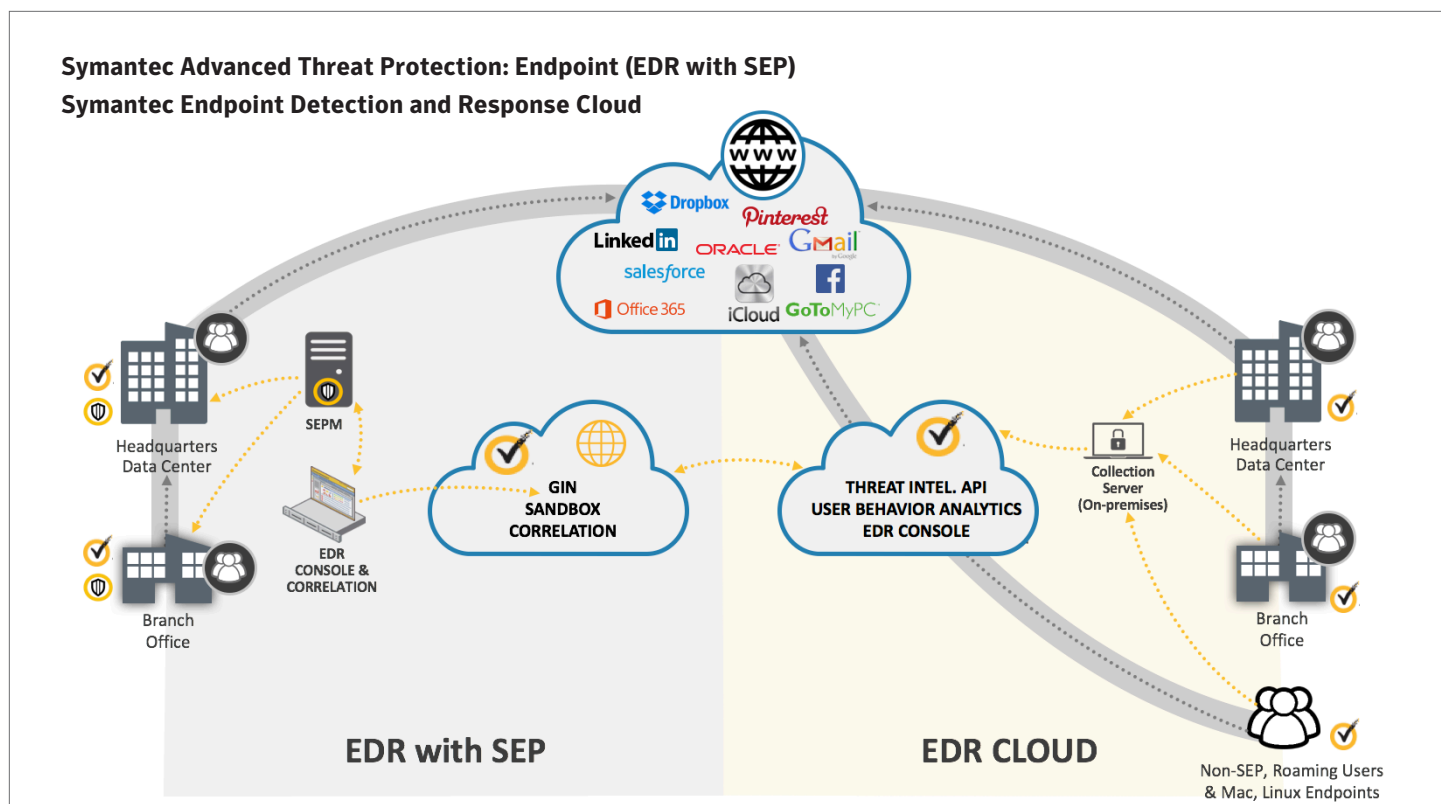
Symantec ATP: Endpoint—EDR for SEP; No new agent required

Symantec Advanced Threat Protection: Endpoint is the SEP-integrated EDR solution that can be ready to use within an

hour. It exposes advanced attacks with precision machine learning, behavioral analytics (to detect fileless attacks such as memory-based and malicious PowerShell execution), and threat intelligence—minimizing false positives to help your security team stay productive. Quickly search, identify, and contain all impacted endpoints while investigating threats using on-premises and cloud-based sandboxing. Gain full endpoint visibility and real-time querying ability thanks to the continuous recording of system activity.

Symantec EDR Cloud—For roaming Users, macOS and Linux devices

Symantec EDR Cloud is a unique service you can implement in minutes to deliver in-depth threat visibility and breach response across your entire enterprise. EDR Cloud enhances investigator productivity and significantly lowers costs by bringing your organization the baked-in skills and best practices—extensive rules, user behavior analytics, and more—of the most experienced security analysts. No SEP required.



⁶ Symantec Internet Security Threat Report Vol. 22

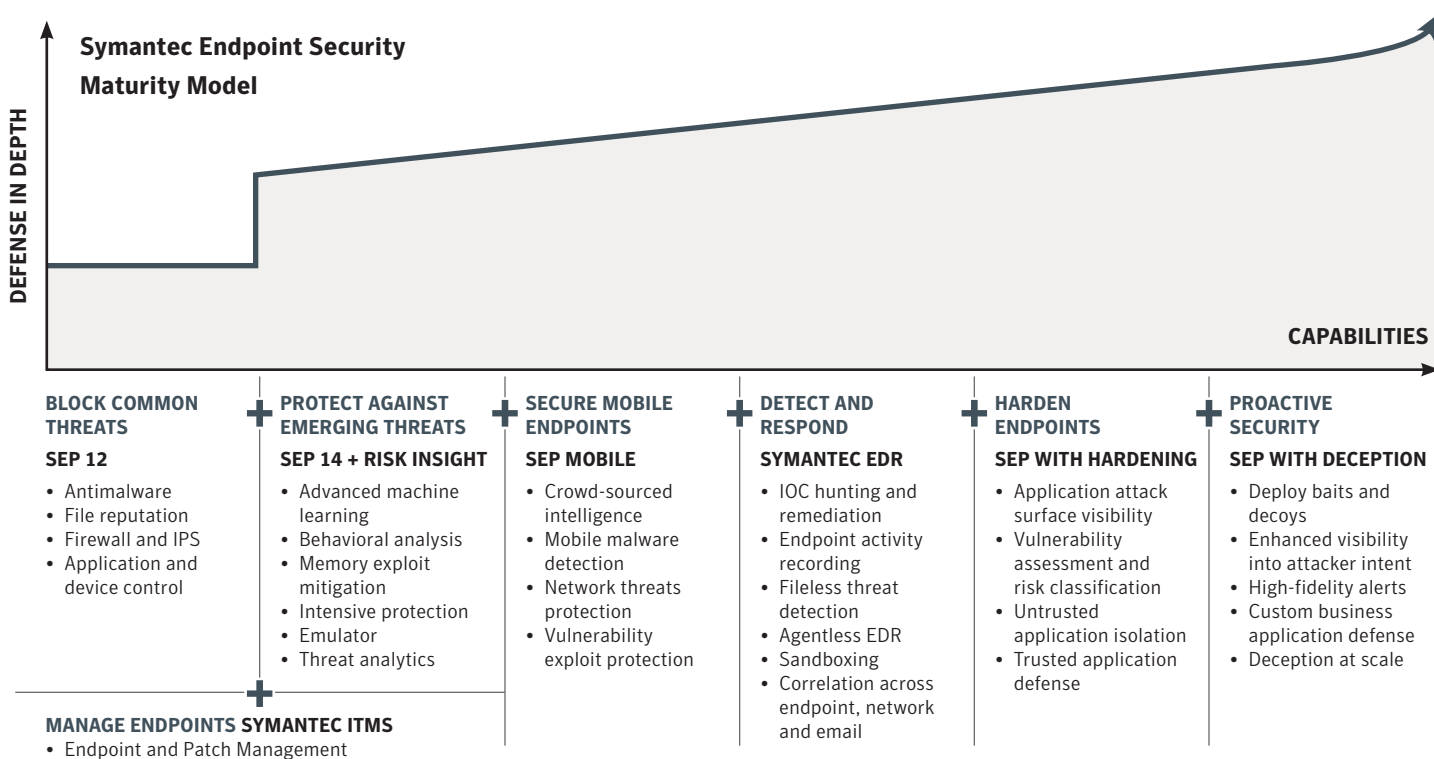
Symantec IT Management Suite—Endpoint patching and management

Symantec Endpoint Management gives you the visibility to securely and efficiently manage all your endpoints: Configure and deploy new devices and apps, manage software licenses, and remediate vulnerabilities by, for example, patching Microsoft products and 50 other leading applications. Works across Windows, Mac, Linux, Unix, and virtual environments. Policy-based management streamlines and automates existing processes, making them repeatable across hundreds or thousands of systems; it also provides detailed reporting

to uncover cost savings and increase productivity. Endpoint Management can also monitor the health of the SEP agent, adding a layer of SEP visibility and protection.

SEP Maturity Model—Defense-in-Depth framework

The Symantec Endpoint Protection maturity model is your framework for defense in depth across modern and traditional endpoints. With Symantec's integrated, scalable, multilayer approach to endpoint protection, your organization will thwart threats and retain the ability to flexibly step up protection as needed—cost-effectively and from a single agent.



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](#).



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