Symantec™

Symantec™ Endpoint Protection Cloud

Protecting users and their devices is critical for organizations of all sizes. For businesses with limited IT staff, endpoint protection and control over all your users' devices (desktops, laptops, tablets & smartphones) can be daunting. The need to address advanced threats with limited resources requires a solution that simplifies endpoint protection and device management.

Advanced Endpoint Security Made Easy

Symantec Endpoint Protection Cloud (SEP Cloud) is an endpoint security service offering easy to use advanced threat protection for PC, Mac, and mobile clients and servers, plus mobile device management for endpoint compliance and data protection. SEP Cloud is based on the same advanced multi-layered scanning technologies powering Symantec Endpoint Protection for its enterprise customers to thwart advanced threats such as zero-day attacks and ransomware. Using a single console, this cloud-based service provides quick setup and policy configuration with just a few simple steps. Combining multi-layered protection with intuitive cloud-based management makes Symantec Endpoint Protection Cloud the ideal solution for organizations that lack IT security resources and expertise.

Intelligent Protection for Emerging Threats

A powerful combination of detection technologies stop advanced threats and rapidly-mutating malware regardless of how they attack your endpoint – all in a high-performance, lightweight agent.

- **Advanced machine learning** blocks new and emerging threats using trillions of samples of good and bad files in the Symantec Global Intelligence Network to power machine-learning results.
- **Behavior monitoring** determines file risk by monitoring nearly 1,400 file behaviors while they execute in real time to block malicious files.
- **Memory exploit mitigation** neutralizes zero-day exploits in popular software that has not been patched by the vendor using signatureless technology that works regardless of flaw, bug, or vulnerability.
- **High-speed emulation** technology detects malware hidden by polymorphic custom packers. A static data scanner runs each file in milliseconds, in a lightweight virtual machine, to force threats to reveal themselves, improving both detection rates and performance.

Stop Targeted Attacks and Zero-Day Threats with Layered Protection

PATENTED REAL-TIME CLOUD LOOKUP FOR ALL SCANNED FILES							
Advanced Machine Learning	Behavior Monitoring	Memory Exploit Mitigation	Emulator	Firewall and Intrusion Prevention	File Reputation	Antivirus	Device Control
Pre-execution detection of new and evolving threats	Monitors and blocks files that exhibit suspicious behaviors	Blocks zero-day exploits against vulnerabilities in popular software	Virtual machine detects malware hidden using custom packers	Blocks malware before it spreads to your machine and controls traffic	Determines safety of files and websites using the wisdom of the community	Scans and eradicates malware that arrives on a system	Blocks infections from USB storage devices, helps prevent data theft

- **Network firewall and intrusion prevention** technology analyzes incoming and outgoing traffic and blocks threats while they travel through the network before reaching endpoints. Rules-based firewall and browser protection defend against web-based attacks. With strong network protection, you can detect most threats before they reach endpoints.
- **File reputation analysis** identifies whether a file is good or bad and assigns a reputation score by inspecting key attributes such file download frequency, download date, and download location—all before the file arrives at the endpoint.
- **Antivirus protection** uses signatures and advanced file heuristics to analyze and eradicate malware on endpoints including viruses, worms, Trojans, spyware, bots, adware, and rootkits. Cloud-based file lookups during file scans provide the latest information and protect against outbreaks and new and emerging malware.

Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Easy to Use Cloud-Based Set-up and Management

SEP Cloud's highly intuitive cloud management allows you to secure and manage a wide variety of devices in the cloud

including: PCs, laptops, mobile phones, tablets and servers with broad OS support (Mac, Windows, iOS and Android). Setup takes just 5 minutes using the default security policy configurations.

Ready to Protect Users in Under 5 Minutes

Intuitive Policy Setting	Fast Action Dashboard	Always Up To Date
Create polices based on employees or groups that are seamlessly applied to all their devices.	Find and remediate infected devices in 3 clicks and easily bring devices into compliance based on status and distribution.	Stay ahead of threats with always-on security that is automatically updated.
Always Available Cloud-Based Architecture		
Cloud-based management console, user portal, real-time dashboard, and advanced endpoint protection		

- **One-click policy configuration** enables cross OS platform policy creation that protects users on any device. The policy is created just once, and that policy configuration translates to any device or operating system, greatly simplifying policy deployment and management.
- **Employee self-enrollment** allows employees to enroll their corporate and personal devices in minutes using an online portal.
- **Built-in integration with Identity Providers** such as Azure AD, Okta and VIP Access Manager makes it easy to synch users with SEP Cloud. For non-Azure Active Directory organizations, bulk upload of users via an Excel or .CSV file is available.
- **An intuitive dashboard** provides a quick view of an entire organization's devices, their status and distribution with the ability to run reports and take action quickly to **remediate devices, and keep them secure and in compliance.**
- **Automated agent updates** delivered from the SEP Cloud service ensures the newest information is downloaded to the device and is always up to date.
- **Pre-configured templates and reports** that can be scheduled or downloaded on-demand meet business reporting needs.
- **Powerful customizable rule engine** with pre-configured alert rules provide actionable intelligence and notification on demand.

Flexible Subscription Options to Meet Your Business Needs

SEP Cloud offers flexible per user or per device subscription options with affordable monthly or annual terms. With a per user subscription you can support multiple devices (PC, Mac or Mobile) on a per user basis for a flat fee and avoid budget surprises. The per device subscription provides protection for a single PC or Mac device that is used by one or multiple users. With SEP Cloud, your endpoint protection service is always up to date with the latest features enabled, and includes 24x7 technical support. The feature comparison table below details features included with each subscription option:

SYMANTEC ENDPOINT PROTECTION CLOUD			
Device Protection	Desktop, Laptop, Smartphone & Tablet	Desktop, Laptop & Microsoft Surface Tablet	Server
Features			
Network & Browser Exploit Prevention	●	●	
Advanced Machine Learning	●	●	●
File Reputation Analysis	●	●	●
Behavior Monitoring & Blocking	●	●	
Memory Exploit Mitigation	●	●	●
Emulator	●	●	●
File-based Malware Prevention	●	●	●
Advanced Firewall	●	●	
Granular Device Controls	●	●	
Mobile Device Management	●		
Mobile Security	●		
Wi-Fi & Email Access	●		
Subscription Options			
Per Device Subscription		●	
Per User (up to 5 devices)	●		
Server-based Subscription			●
Encryption Add-on	●		

Symantec Consistently Named a Leader in Endpoint Protection

- 18 months with 100 percent protection for zero-day attacks, AV-TEST
- Gartner Magic Quadrant leader for past 15 years
- Five-star rating and recommendation, SC Magazine, August 2016
- Overall highest endpoint security score, PassMark Software, Enterprise Endpoint Security, Performance Benchmarks, February 2017

For more information or to start a free trial, visit symantec.com/products/endpoint-protection-cloud

Symantec.

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

SYMC_DS_Endpoint_Protection_Cloud_EN_v1a