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 easy to use security-as-a-service that protects and manages PC, Mac, mobile devices and servers from a single console, making it the ideal solution for organizations with limited IT security resources. SEP Cloud effectively stops today's ransomware, zero-day threats and other sophisticated attacks using advanced multi-layered technologies including advanced machine learning and behavior analysis. Utilizing SEP Cloud's, default security settings and user self-enrollment capabilities, this solution quickly protects your endpoints.

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.
- **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

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

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

Comprehensive mobile threat defense is built into SEP Cloud for iOS and Android devices to deliver superior protection against an extensive range of existing and unknown threats. SEP Cloud uses a layered approach to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits.

- **Malware Defense** provides proactive defense against zero-day malicious repackaged apps based on signatures, static/dynamic analysis, behavior, structure, permissions, source and real-time response.
- **Network Defense** delivers an effective shield against malicious Wi-Fi networks, and blocks man-in–the-middle, SSL downgrading, and content manipulation attacks with patented active honeypot technology.
- **Vulnerability Defense** monitors devices for unpatched known vulnerabilities, and uncovers zero-day vulnerabilities in apps and operating systems.
- **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** 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.
- **Email and Wi-Fi Policy** creation controls 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 (macOS, 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

- **An intuitive dashboard** provides a quick view of your 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.
- **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.
- **User self-enrollment** allows employees to enroll their corporate and personal devices in minutes using an online portal.
- **Automated agent updates** delivered from the SEP Cloud service ensures the newest information is downloaded to the device and is always up to date.
- **Device discovery** ensures all your devices are protected by continuously scanning your network for unprotected devices, and auto enrolling these devices with a single click.
- **Automate agent deployment** with Windows and macOS installation packages that can be pushed out using popular software distribution tools.
- **Built-in integration with Identity Providers** such as Azure AD, Okta, Oracle IDCS 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.
- **REST APIs** enable developers to integrate SEP Cloud with other security, reporting, information, and event technologies.
- **Partner management tools** provide resellers and managed service providers with an aggregated view of their SEP Cloud customers for monitoring and management of the service on their behalf. Symantec provides a partner-based cloud-management console (PMC), and integration with popular remote management and monitoring tools, including ConnectWise.

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. A per device subscription provides protection for a single PC, Mac or mobile 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			
Subscription Options	Per User (up to 5 devices)	Per Device	Per Server
Features			
Windows and macOS	●	●	Windows Server
Firewall & Intrusion Prevention	●	●	
Block Zero-Day Threats Contained in Memory	●	●	●
Antivirus Scanning	●	●	●
Virtual Machine Detection of Hidden Threats in Files & Executables	●	●	●
Pre-Execution Detection of Threats using Machine Learning	●	●	●
iOS and Android	●	●	
Malware Defense	●	●	
Network Defense	●	●	
App/OS Vulnerability Defense	●	●	
Mobile Device Management	●	●	
Add-Ons			
Device Encryption Management	●		

Symantec Consistently Named a Leader in Endpoint Protection
- Gartner Magic Quadrant leader for past 16 years
- Best endpoint protection award, AV-TEST, 2017
- Endpoint Security Vendor of the Year, Frost & Sullivan, 2017
- Leader Mobile Threat Management Security Market, IDC MarketScape, 2017

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

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.

✓Symantec™

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

19B185256_DS_SEP_CLOUD_EN