

Symantec Endpoint Protection Feature Comparison

	SEP SBE	SEP Cloud	SEP Cloud	SEP 14.1	Description
Device Protection	Desktop, Laptop	Desktop, Laptop & Microsoft Surface Tablet	Desktop, Laptop, Tablet & Smartphone	Desktop, Laptop	
Meter	Per Device	Per Device	Per User	Per Device	
Max # of Devices	1	1	5	1	
Advanced Protection and Performance					
Advanced Machine Learning	✓	✓	✓	✓	Advanced Machine Learning (AML) on the endpoint for pre-execution detection of unknown and emerging threats.
File Reputation Analysis	✓	✓	✓	✓	Separates files with risky reputation from those that are safe, for faster and more accurate malware detection.
Memory Exploit Mitigation	✓	✓	✓	✓	Hardening to protect against zero-day exploits of vulnerabilities in common applications.
File based malware prevention	✓	✓	✓	✓	File signature based detection of known malware
Emulator	✓	✓	✓	✓	Static data scanning detects custom packed malware. Improves scan performance and effectiveness
Advanced Firewall	*	*	*	✓	Firewall policies and rules allow or block network traffic. SEP has an advanced firewall with granular controls. *SEP Cloud and SEP SBE provide simpler firewall controls
Behavior Monitoring and Blocking	✓	✓	✓	✓	Examines programs as they run, identifying and stopping malicious behavior
Intrusion Prevention	✓	✓	✓	✓	Scans network traffic for indications of or attempted intrusions, or attacks directed at browser vulnerabilities
Device Control	*	*	*	✓	Controls read and write access to specific device classes such as USB and other peripherals. *SEP Cloud and SEP SBE provide simple device control
Location Based Policy Control	*	*	*	✓	Configure policies based on the endpoint’s network location. *SEP Cloud has a simple model for Private vs. Public Firewall behavior and rules

Host Integrity				✓	Ensures that client computers are protected and compliant with your company's security policies and if not download and install patches and packages.
Application Rules	*			✓	Allow administrators to write rules to control file & registry access & sanctioned apps using blacklists & whitelists. * SEP SBE provides simple app rules
Custom Intrusion Prevention Signatures				✓	Create custom signatures that can detect attacks in the TCP/IP stack earlier than Symantec signatures.
Peer-to-Peer Authentication & Blocking				✓	Verify clients on local network pass host integrity checks before allowing network access such as local file sharing.
Intensive Protection				✓	Fine-tune security engines via easy-to-use sliders to deploy appropriate and specific protection for each endpoint and sets of endpoints
Deception				✓	Expose attackers with baits to reveal their intent, tactics, and targets. Use adversarial knowledge to update security policy and improve security posture
Application Isolation and Control				✓	Automatically discover and classify applications by risk score; Shield common applications from vulnerability exploits and isolate unknown applications to stop suspicious activity (SEP Hardening)
Device Management					
Password Protection & OS Device Controls	*	✓	✓	✓	Prevents unauthorized access to user devices by enforcing the password requirements you specify and enable extra security protection by controlling camera *SEP SBE offers device controls only
Lock & Wipe of mobile devices			✓		Ability to remotely lock or wipe a mobile device.
Wi-Fi & Email Access			✓		Configure email access on iOS/ android devices & Wi-Fi access on Mac/Android/ iOS devices
Platform Support					

Windows	✓	✓	✓	✓	Supports Windows 7/8/8.1/10. SEP 14 also supports Windows Embedded 8.1
Mac	*	✓	✓	✓	Mac OSX 10.9, 10.10, 10.11, 10.12, 10.13 * SEP SBE offers protection client only.
Linux				✓	For full list visit Supported Linux kernels for Symantec Endpoint Protection: <URL>
Android			✓		Mobile security and device management for Android devices running android 4.2+
iOS			✓		SEP Cloud supports device management for iOS 8+, Mobile Security for iOS coming soon
Windows Server	✓	*	*	✓	Windows Server 2008/2012/2016 *Requires SEP Cloud Server License
AWS Marketplace				✓	SEP14 on AWS offers SEP Manager hosted as a 64-bit AMI to manage AWS instances, on-premises SEP clients or hybrid and is offered as Paid and bring your own license
Integration with other Symantec Products					
Native Encryption Key Management			✓		Manage encryption of Windows/Mac/Android clients
IT Management: Visibility of devices into ITMS		✓	✓		ITMS customers can view SEP Cloud endpoints for end to end management of user systems and servers.
VIP Multi-factor Authentication		Coming Soon	Coming Soon		Enhanced security with administrator console by enabling two-factor authentication using VIP
Symantec Advanced Threat Protection Integration				✓	SEP is the single agent for SEP 14 and ATP. SEP customers can take advantage of ATP Endpoint Detection and Response (EDR)
Secure Web Gateway based Blacklisting				✓	Symantec Secure Web Gateway (SWG) sends blacklists based on network detection to be automatically blacklisted on SEP 14 endpoints
Orchestration, Usability, and Scale					

On-Premises Management Console		NA	NA	✓	SEP Manager is an on-premises management console and provides granular controls to manage SEP endpoints
Cloud based Management Console	✓	✓	✓	Coming soon	SEP Cloud provides a fully cloud-based console. SEP 14 will deliver hybrid cloud management with addition of a cloud-based server for advanced visibility and controls
Cross-Platform User-based Policies		✓	✓		Protect users on any device, anywhere with one step policy configuration
Reporting Capabilities	✓	✓	✓	✓	Canned Reports can be saved, scheduled, formatted and emailed
Local Update Distribution	✓			✓	SEP 14 supports Group Update Provider (GUP) to download and redistribute content locally. SEP Cloud updates are directly sent from Symantec to endpoints and a local update distribution is not required.
Custom Replication Schedule				✓	Run replication multiple times a day across multiple locations, improving effective reporting while preventing deadlocks on SEP Manager
REST APIs		✓	✓	✓	Enables integration and orchestration with third party tools like SIEM as well as integration with other Symantec products like ATP, Symantec secure Web Gateway (SWG)
Identity Provider Integration		✓	✓	✓	Supports integration with the following identity providers: Azure Active Directory (AD), Symantec VIP Access and Okta. It also supports AD Sync with Azure AD
Bulk User Import		✓	✓		Allows users to be imported/ updated in bulk using csv or xls templates
Contextual Exclusions		✓	✓		Allows creation of exclusions directly from events based on false positives
Custom Alert Rules	*	✓	✓		Allows creation of rules to correlate events and generate custom alert notifications * SEP SBE offers basic rule editor

Partner Management Console	✓	✓	✓		Web-based, unified, management portal for channel partners to add, view and manage customer accounts for Symantec products.
Partner Utilization APIs		✓	✓		APIs available for distributors to track product usage and adoption