Symantec
A Division of Broadcom

Product Brief

Symantec Protection Engine
For Cloud Services 8.2

At A Glance

Reduced Risk Profile

- Provides an API, SDK, and sample code to allow integration of an on-demand verdict engine wherever malware prevention is needed.
- Common use cases include: web portals, data in transit, third-party applications, gateways between infrastructures, and more.
- Provides an additional layer of defense resulting in a higher trust of new content.
- Track files globally and apply reputation intelligence to cloud services.

Industry-leading Protection

- File reputation service powers fast, scalable, and reliable anti-malware scanning.
- Proprietary, patented rich URL categorization and filtering blocks malicious websites and content.
- Advanced Machine Learning provides strong protection with a low false-positive rate.
- Disarm feature that removes threats from Potentially Malicious Content (PMC) embedded in incoming documents

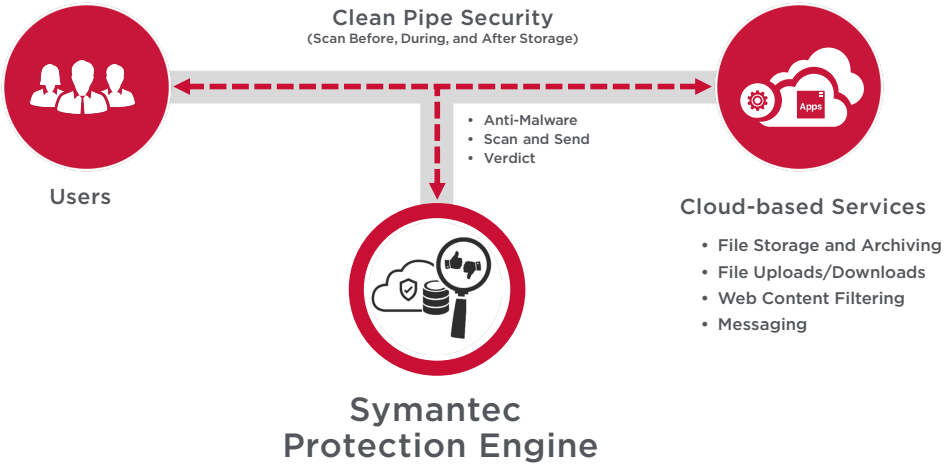
Innovative Security Services

Symantec™ Protection Engine (SPE) for Cloud Services 8.2 is a flexible and feature-rich client/server application that allows customers to incorporate malware and threat detection technologies into almost any application. SPE for Cloud Services provides access to innovative security that helps to ensure the safety of incoming content to your environment. Symantec file reputation service puts files in context, using their age, frequency, location, and other factors to expose threats that would otherwise be missed.

Advanced Machine Learning tunes the solution according to scanning behavior. SPE for Cloud Services includes proprietary Symantec URL categorization technology and industry-leading malware protection for fast, scalable, and reliable scanning services that help protect data and storage systems against the ever-growing malware threat landscape.

Alongside native Internet Content Adaptation Protocol (ICAP) support, SPE for Cloud Services provides a full client software development kit (SDK) that enables customers to fully embed malware protection in business-critical applications, services, and devices.

Platform support spanning Microsoft Windows, Red Hat Enterprise Linux, and CentOS ensures market-leading malware detection wherever it is needed.



At A Glance (cont.)

Broad Application, Storage, and Platform Support

- Protect a broad array of third-party applications with APIs for embeddable threat detection and content and anti-malware control.
- Incorporate malware and threat detection technologies into almost any business-critical application, service, or device with the full client software development kit (SDK) and native Internet Content Adaptation Protocol (ICAP) support.
- Two license models (per-user and per-transaction) provide deployment flexibility for sizing and architecture without additional licensing charges.
- The explosion of cloud services and related storage provides many business opportunities, but it can also increase enterprise risk. Important business data, tools, and utilities residing on storage devices need malware protection, even if backed up or archived.

Enhancements in SPE for Cloud Services

Flexible Management Options

- New Symantec hosted Cloud Console manages all SPE instances in a single console, included at no additional charge.
- On-premises Graphical User Interface (GUI) for one-to-one local management.
- Command-line management for on-demand scalability with script based configuration.

Increased Protection

- Symantec STARGate integration
- New Disarm feature:
  - Removes DDE, JavaScript, Macros, and Embedded Files from Office and PDF documents
  - Original file is quarantined for later retrieval as needed

Increased Usability/Productivity

- Support for files > 2 GB

New Platform Support

- Open JRE
- Windows 2019
- RHEL/CentOS 8.0, 8.1 and 8.2 8.0

Key Features

- Rich, easy-to-use centralized console for managing and monitoring all instances
- Advanced Machine Learning capability
- Detect both known and unknown malware using Symantec file reputation service technology
- Innovative URL filtering technology
- Flexible 64-bit threat detection engine allows almost any application running over different operating systems to examine files and URLs for threats
- Mobile data scanning capabilities for APK files
- Console provides scan statistics, system information, policy control, and user management
- Reconstructs Office 2003/2007+ and PDF documents after removing active embedded content (meaning Macro, JavaScript)
- Supports secure ICAP
- Syslog support
- Specify both time and time ranges in LiveUpdate Triggers

Benefits

- Simple integration with third-party applications
- Embeddable, industry-leading malware detection technologies
- Integrated rich URL categorization and filtering
- Protect applications and storage from hosting and distributing malware

System Requirements

Supported 64-bit Operating Systems

- Microsoft Windows 2019, 2016, 2012 R2, 2012
- Red Hat Enterprise Linux 7.x, 8.x
- CentOS 7.x, 8.x

Supported Virtualization Systems

- VMware vSphere Hypervisor 5.5 or later
- Microsoft Hyper-V Server 2019, 2016 2012 R2, 2012

Minimum Hardware Configuration

- Intel or AMD server-grade single processor quad-core system or higher
- 8 GB RAM or higher
- 40 GB hard disk space minimum available (60 GB hard disk space if using URL filtering)
- One NIC with static IP address running TCP/IP
- 100 Mb/s Ethernet link (1 Gb/s recommended)

For the latest Platform Support Matrix and documentation, see knowledge.broadcom.com/external/article?legacyId=INFO5084

To learn more about Symantec Protection Engine, see broadcom.com/products/cyber-security/endpoint/hybrid-cloud/protection-engine

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SPE-CS-PB100 October 28, 2020