PRODUCT BRIEF

Symantec® Protection Engine

For Cloud Services 9.2

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 higher trust of new content
- Tracks files globally and applies reputation intelligence to cloud services

Industry-Leading Protection

- File Reputation Service powers fast, scalable, and reliable antimalware 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
- Amazon S3 storage
- Google GCP storage

Innovative Security Services

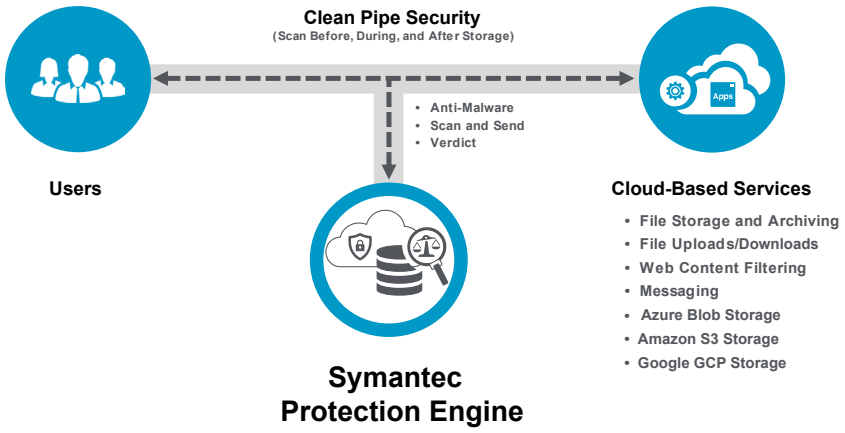
Symantec® Protection Engine (SPE) for Cloud Services 9.2 is a flexible and feature-rich client/server application that allows customers to incorporate malware and threat detection technologies into almost any application.

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.

The scanner itself runs on Windows or Linux. It can run in the cloud, in a data center, or in a Docker container. Protecting business applications and devices is simplified by the diverse methods of integration. In addition to native Internet Content Adaptation Protocol (ICAP) support, SPE for Cloud Services provides a full client software development kit (SDK) and API set. Finally, SPE ships a Helm-based container solution to protect cloud storage such as Azure Blobs.

Figure 1: SPE for Cloud Services



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 antimalware 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.
- In-tenant scanning for Microsoft Azure Blobs, Amazon S3 buckets, and Google GCP storage is built in. SPE scanners run as containers in a pod. As files are written or changed, the pod is notified and the file is scanned by the pool. Events are reported to the native cloud provider tools such as AppInsight. Kubernetes takes care of scaling the number of scanners up or down depending on load.
- Role-based access controls separate API functions for scanning tasks and administrative tasks.

Enhancements in SPE for Cloud Services

Flexible Management Options

- SPE management is simplified through a new central console. This modern Windows-based application provides the following functionality:
  - Easily manage SPE scanners and policies
  - Create groups for scanner pools with common policies
  - View status and statistics on a dashboard
  - Centralized view and management of scanner quarantine
  - Centralized reporting and license management
- On-premises GUI for one-to-one local management
- Command-line management for on-demand scalability with script-based configuration
- Greatly expanded REST API for scanner management and orchestration using third-party tools

Increased Usability and Productivity

- Support for files greater than 2 GB

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
  - Ability to use Disarm in log-only mode including more detail on the nature of the active content

New Platform Support

- Containerized Symantec Protection Engine with Helm Charts
- Windows 2022
- Red Hat Enterprise Linux 8.x
- Rocky Linux 8.7
- Amazon Linux 2

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.
- In-tenant scanning for cloud data stores, such as Azure Blobs, means that the data never leaves the customer's environment.

SYSTEM REQUIREMENTS

SPE Server: Supported 64-Bit Operating Systems

- Microsoft Windows Server 2016, 2019, and 2022
- Red Hat Enterprise Linux 7.x, 8.x, and 9.3
- Rocky Linux 8.7 and 9.3
- SUSE Linux Enterprise Server 15.3 (64 bit)
- CentOS 7.x
- Amazon Linux 2

SPE Console: Supported 64-Bit Operating Systems

- Microsoft Windows Server 2019 and 2022
- Microsoft Windows 10 and 11

Supported Virtualization Systems

- VMware® vSphere Hypervisor 5.5 or later
- Microsoft Hyper-V Server 2016 and 2019
- Kubernetes, OpenShift, and Docker

Minimum Hardware Configuration

- Intel or AMD server-grade single processor quad-core system or higher
- 16 GB RAM or higher (24 GB if using URL Insight)
- 40 GB hard disk space minimum (60 GB hard disk space if using URL filtering)
- One NIC with a static IP address running TCP/IP
- 100 Mb/s Ethernet link (1 Gb/s recommended)

Key Features

- Rich, easy-to-use centralized console for managing and monitoring all instances either on-premises or in the cloud. The console provides scan statistics, system information, policy control, and quarantine management.
- Modern deployment option: Symantec Protection Engine Docker with Helm, which supports Kubernetes and Red Hat OpenShift. The one-click Helm deployment simplifies the installation, scanning, and management experience and allows for elastic scaling.
- Enhanced REST services for SPE scanners: management and scanning.
- 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 including macros and JavaScript.
- Supports secure ICAP.
- Syslog support.
- REST API to fetch reports from all servers in CSV format. This can be imported to reporting software.
- Supports both date and time ranges for product content updates through LiveUpdate.

For information about this version of the application, see What's New in Symantec Protection Engine 9.2.0.

For the latest platform support matrix and system requirements, see System requirements.

To learn more about Symantec Protection Engine, see Symantec Protection Engine 9.2.0.

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

SPE-CS-PB104 March 13, 2025