DATA SHEET

Symantec Protection Engine (SPE) for Cloud Services 8.0

At A Glance

Reduced Risk Profile

- Prevent cloud-based applications and storage services from hosting and distributing malware.
- Ensure safe web browsing and information sharing for employees.
- Track files globally and apply reputation intelligence to cloud services.

Industry-leading Protection

- Symantec's 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.

Broad Application, Storage, and Platform Support

- Protect a broad array of third-party applications and storage services 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.

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.

Innovative Security Services

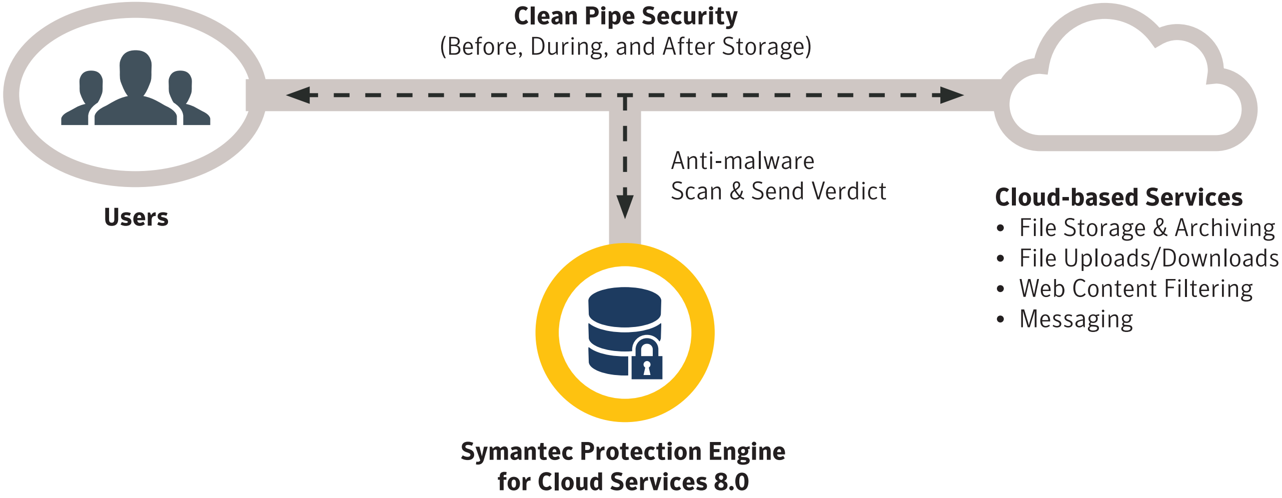
Symantec™ Protection Engine for Cloud Services 8.0 is a flexible and feature-rich client/server application that allows customers to incorporate malware and threat detection technologies into almost any application. SPE for Cloud Services provides access to innovative security that helps to ensure the safety of your information on the web. Symantec's 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. Protection Engine for Cloud Services includes Symantec's proprietary URL categorization technology and industry-leading malware protection for fast, scalable, and reliable scanning services that help you protect your data and storage systems against the ever-growing malware threat landscape.

Alongside native Internet Content Adaptation Protocol (ICAP) support, Protection Engine 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 that you can take advantage of market-leading malware detection wherever you need it.

Reduce organizational risk with fast, scalable threat detection and anti-malware for cloud-based applications and services



Clean Pipe Security
(Before, During, and After Storage)

Users

Anti-malware
Scan & Send Verdict

Cloud-based Services

- File Storage & Archiving
- File Uploads/Downloads
- Web Content Filtering
- Messaging

**Symantec Protection Engine
for Cloud Services 8.0**

What's New in SPE for Cloud Services 8.0

Centralized Management and Monitoring Console

- Manage all SPE instances in a single console
- New Cloud Console free to use for SPE customers
- Console shared with Cloud Workload Protection (CWP) and CWP for Storage

Secure ICAPSupport

- Configure encrypted communication between SPE Scanners and Client Application over Secure ICAP protocol

New Platform Support

- Oracle Java JRE 10

Key Features

- Rich, easy-to-use centralized console for managing and monitoring all instances
- On-premises Graphical User Interface (GUI) for one-to-one management
- Advanced Machine Learning capability
- Syslog support
- Detect both known and unknown malware
- Powered by Symantec file reputation service 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
- Central quarantine controls access to detected malware or files that cannot be identified or scanned
- Console provides scan statistics, system information, policy control, and user management
- URL filtering technology powered by Symantec RuleSpace™
- Supports secure ICAP
- 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 2016, 2012 R2, 2012, 2008 R2, 2008 (English and Japanese)
- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 6.8 and later
- CentOS 7.x

Supported Virtualization Systems

- VMware vSphere® Hypervisor 5.5 or later
- Microsoft Hyper-V® Server 2012 R2, 2012, 2008 R2

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 Mbps Ethernet link (1 Gbps recommended)

Recommended Hardware Configuration

- Intel or AMD server-grade single processor quad-core system or higher
- 16 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
- At least 1 Gbps Ethernet link

For latest Platform Support Matrix and Documentation, refer to: https://www.symantec.com/docs/INFO5084

Supported NAS platforms include:

- EMC
- NetApp
- Hitachi
- IBM®

For the latest information about specific platform validation or certification, contact the storage vendor or refer to the Symantec support matrix for partner devices.

Learn more about Symantec Protection Engine

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.