DATA SHEET

Symantec Protection Engine (SPE) for Network Attached Storage 8.0

At A Glance

Reduced Risk Profile
- Prevent storage services from hosting and distributing malware.
- Track files globally and apply reputation intelligence to network attached storage (NAS).

Industry-leading Protection
- Symantec's file reputation service powers fast, scalable, and reliable anti-malware scanning.
- Advanced machine learning provides strong protection with a low false-positive rate.

Broad Application, Storage, and Platform Support
- Incorporate malware and threat detection technologies into NAS devices with a NetApp®-defined interface over remote procedure calls, native Internet Content Adaptation Protocol (ICAP) support, and partner integrations.

Securing storage is a critical aspect of keeping your enterprise safe. Important business data, tools, and utilities residing on storage devices need malware protection, even if backed up or archived.

Scalable, High-performance Threat Detection Services

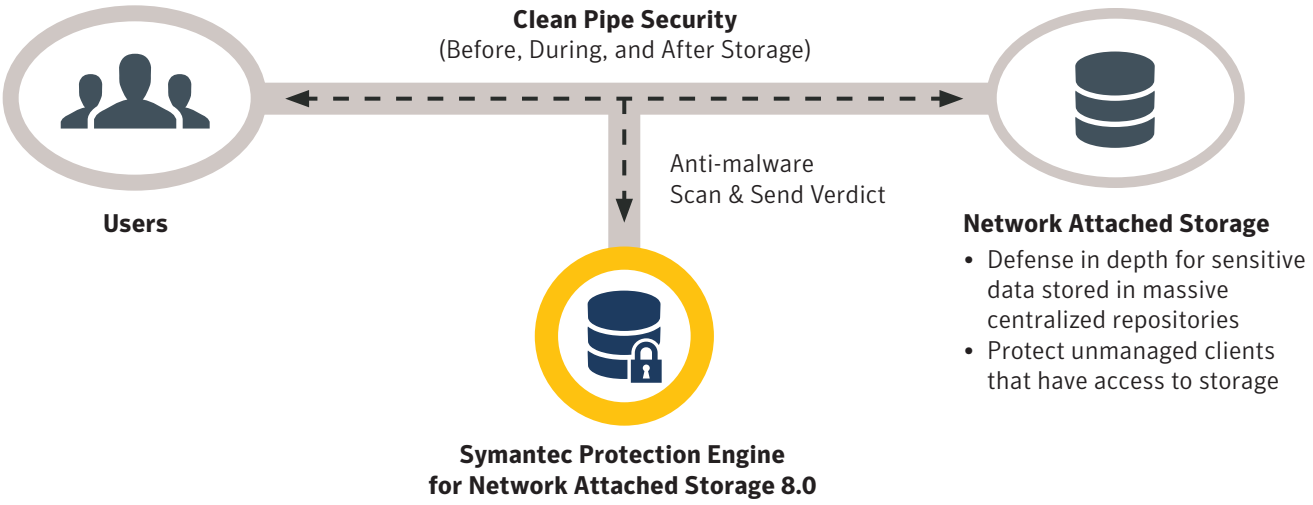
Symantec™ Protection Engine for Network Attached Storage 8.0 provides scalable, high-performance threat detection services to protect valuable data stored on network attached storage (NAS) devices. This product improves scanning performance and detection capabilities to protect against multi-blended threats. SPE includes Symantec's industry-leading malware protection with File Reputation technology, and Advanced Machine Learning to deliver fast, scalable, and reliable content scanning services. This helps organizations protect their data and storage systems against the ever-growing malware threat landscape.

Symantec LiveUpdate™ automatically updates malware definitions and engines without interrupting scanning. You can also centrally distribute definitions to multiple deployments with the included Symantec LiveUpdate Administrator application.

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.

Many storage vendors certify their platforms with Protection Engine for Network Attached Storage, including NetApp, EMC®, and Sun™ (Oracle®), providing you with scalable and secure integration.

Reduce organizational risk with fast, scalable threat detection and anti-malware for network attached storage



What's New in SPE for Network Attached Storage 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

New Platform Support

- Oracle Java JRE 10

Syslog Support

- Supports new logging destination on Linux

Advanced Machine-learning Integration

- Scans and eradicates malware based on more than 150 static file attributes
- Works with file reputation technology to provide strong protection with a low false-positive rate

Platforms

- Supports Windows® 2016, Red Hat® Enterprise Linux® 6.8, and CentOS® 7.2

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
- Out-of-box support for NetApp filers
- Detect both known and unknown malware
- Powered by Symantec file reputation service technology
- Mobile data scanning capabilities for APK files
- AV Microdefs for smaller definition updates
- Supports secure ICAP
- Specify both time and time ranges in LiveUpdate Triggers

Benefits

- Protect applications and storage from hosting and distributing malware
- High-performance scanning of files for viruses, malware, spyware, worms, and Trojans
- Easily integrates with third-party NAS devices via ICAP
- Delivers statistical and detailed activity reports that can be viewed in HTML or exported to CSV format
- Delivers consumption reporting to illustrate how resources are being utilized

- Improved alerts allow event triggers to be sent via email or SNMP alerts when a predetermined number of events occur
- Central quarantine allows administrators to safely move potential threats to a safe area on a centralized server
- Improved logging captures and displays more event details

Advantages

- Leverages the next generation of Symantec threat detection technology
- Scalable solution with the ability to run multiple SPE for NAS servers in parallel and utilize most popular load-balancing solutions
- Support for multiple operating systems and mixed mode deployment
- Backed up by the Symantec Security Response organization
- R&D centers in every region of the world
- Supports Rapid Release virus definitions

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

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.

Symantec

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

19B188212_DS_SPE-8_NAS_EN