PRODUCT BRIEF

Symantec® Protection Engine

For Network Attached Storage 9.1

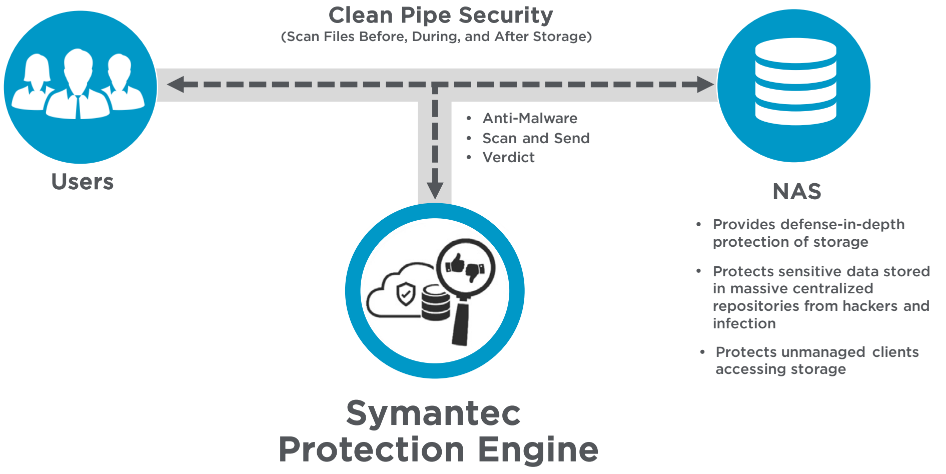
Scalable, High-performance Threat Detection Services

Symantec® Protection Engine (SPE) for Network Attached Storage 9.1 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 industry-leading Symantec malware protection with Symantec File Reputation Service technology and advanced machine learning to deliver fast, scalable, and reliable content scanning services. This product 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, Rocky Linux, and CentOS ensures that you can take advantage of market-leading malware detection wherever you need it (Windows-only for NetApp).

Many storage vendors certify their platforms with SPE for Network Attached Storage, including NetApp, Hitachi, Dell, and Nutanix, providing you with scalable and secure integration.


Clean Pipe Security
(Scan Files Before, During, and After Storage)
Users
Anti-Malware
Scan and Send
Verdict
NAS
Provides defense-in-depth protection of storage
Protects sensitive data stored in massive centralized repositories from hackers and infection
Protects unmanaged clients accessing storage
Symantec Protection Engine

AT A GLANCE

Reduced Risk Profile

- Protect network storage devices from hosting and distributing malware.
- Defend against *living off the land* attacks where threat actors could use unprotected storage to stage their malware.
- Track files globally and apply reputation intelligence to NAS.

Industry-leading Protection

- File reputation service powers fast, scalable, and reliable anti-malware scanning.
- Advanced machine learning provides strong protection with a low false-positive rate.
- Disarm feature that removes threats from *potentially malicious content* embedded in incoming documents.

Broad Application, Storage, and Platform Support

- Incorporate malware and threat detection technologies into NAS devices with broad device support from NAS vendors.
- High performance verdict engine is highly scalable to accommodate the most demanding NAS environments.
- Two license models (per-user and per-terabyte) provide deployment flexibility for sizing and architecture without additional licensing charges.
- Secure 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.

SPE for Network Attached Storage Enhancements

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 user interface 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

Increased Protection

- Symantec STARGate integration
- 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 and Productivity

- Support for large files > 2 GB

New Platform Support

- Containerized SPE with Helm Charts
- Windows 2022
- Rocky Linux 8.7
- Amazon Linux 2

Key Features

- Rich, easy-to-use centralized console for managing and monitoring all instances, either on-prem or in the cloud. The console provides scan statistics, system information, policy control, and quarantine management.
- Modern deployment option: SPE 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.
- Syslog support.
- Out-of-box support for NetApp filers.
- Detect both known and unknown malware using Symantec File Reputation Service technology.
- Mobile data scanning capabilities for APK files.
- AV Microdefs for smaller definition updates.
- Reconstructs Office 2003/2007+ and PDF documents after removing active embedded content (meaning Macro and JavaScript).
- Supports secure ICAP for the NAS devices that support it.
- 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 through ICAP or RPC (NetApp only)
- Delivers statistical and detailed activity reports that can be viewed in HTML or exported to CSV format
- Delivers consumption reporting to show how resources are being utilized
- Improved alerts allow event triggers to be sent through email or SNMP alerts when a predetermined number of events occur
- 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 NetApp deployment
- Backed up by the Symantec Security Response organization
- Supports Rapid Release virus definitions

System Requirements

Scanner Supported 64-bit Operating Systems

- Microsoft Windows 2022, 2019, and 2016
- Red Hat Enterprise Linux 8.x
- CentOS 7.x, 8.0
- Rocky Linux 8.7
- SUSE Linux Enterprise Server 15.3 (64 bit)
- Amazon Linux 2

SPE Console Supported Operating Systems

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

Supported Virtualization Systems

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

Minimum 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
- 100 Mb/s Ethernet link (1 Gb/s recommended)

Learn more about SPE, refer to techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/symantec-protection-engine/9-1-0.html.

BROADCOM®
connecting everything®

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

SPE-NAS-PB101 October 5, 2023