

Symantec™ Protection Engine for Network Attached Storage 7.8

Protect mission critical storage with fast, scalable, and on-demand threat detection and content control

Data Sheet: Secure File Sharing

Overview

Symantec™ Protection Engine for Network Attached Storage 7.8 provides scalable, high-performance threat detection services to protect valuable data stored on network attached storage (NAS) devices. This solution provides increased scanning performance and improved detection capabilities for protection against multi-blended threats. Protection Engine includes Symantec's industry-leading malware protection, including Symantec Insight™ technology, for fast, scalable, and reliable content scanning services, helping organizations protect their data and storage systems against the ever-growing malware threat landscape. Malware definitions and engines are updated automatically with no interruption in malware scanning using Symantec LiveUpdate™ or can be distributed centrally to multiple deployments utilizing the included Symantec LiveUpdate™ Administrator application.

Platform support spanning Linux, Windows®, Red Hat, and CentOS ensures that customers can take advantage of the market-leading malware detection wherever they need it.

Many of the market-leading storage vendors certify their platforms with Protection Engine for Network Attached Storage, including NetApp™, EMC® and Sun® (Oracle™) allowing customers to be sure of scalable and secure integration.

What's New in Protection Engine for Network Attached Storage 7.8

- 64-bit flexible threat detection engine that provides scalable, high-performance threat detection services to protect valuable data stored on network attached storage devices.
- Advanced Insight Reputation capability available along with Android Applications Reputation.
- Off-board AV scanning for NetApp C-mode architecture (compatibility with NetApp ONTAP v8.2.1 and later)

Features and benefits

Features

- 64-bit engine for content and URL scanning
- Detect known and unknown malware
- Mobile data scanning capabilities for APK files
- Powered by Symantec Insight technology
- AV Microdefs for smaller definition updates

Benefits

- Protect applications and storage from hosting and distributing malware.
- Provides high-performance scanning of files for viruses, malware, spyware, worms, and Trojan horses
- 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 of Protection Engine for Network Attached Storage

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

Supported NAS Devices

Supported NAS platform vendors include:

EMC

Hitachi®

NetApp

IBM

For the latest information about specific platform validation or certification please contact the storage vendor and/or refer to the information at <http://www.symantec.com/docs/HOWTO83461>

System requirements

Supported operating systems

64-bit OS

- Windows® 2012 R2 (English and Japanese)
- Windows® 2012 (English and Japanese)
- Windows® 2008 (English and Japanese)
- Windows® 2008 R2 (English and Japanese)
- Red Hat® Enterprise Linux 7.x
- Red Hat® Enterprise Linux 6.x
- Red Hat® Enterprise Linux 5.x
- SUSE® Linux Enterprise Server 11 and 12
- CentOS 7.x

Supported Virtualization systems

- VMware® vSphere Hypervisor™ v5.5 or later
- Windows® 2012 R2 Hyper-V
- Windows® 2012 Hyper-V
- Windows® 2008 R2 Hyper-V

All supported operating systems (Windows and Linux) are supported in above Hypervisors.

Minimum hardware configuration

- Intel or AMD Server Grade Single Processor Quad Core systems
- 8 GB random-access memory (RAM)
- 40 GB hard disk space available (60 GB of hard disk space if using URL Filtering)
- 1 NIC with static IP address running TCP/IP
- 100 Mbps Ethernet link

Recommended hardware configuration

- At least Intel or AMD Server Grade Dual Processor Quad Core systems or higher
 - At least 16GB random-access memory (RAM)
 - At least 40 GB hard disk space available (60 GB of hard disk space if using URL filtering)
 - 1 NIC with static IP address running TCP/IP
 - At least 1 Gbps Ethernet link
-

More Information

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free +1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is a global leader in security solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

+1 (800) 721 3934

www.symantec.com