Symantec™ Protection Engine for Network Attached Storage 7.0

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 7.0 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 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.

With platform support spanning Linux, Windows®, and Solaris® 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®, Sun®(Oracle™) allowing customers to be sure of a scalable and secure integration

What's New in 7.0

- The next generation malware detection engine enables Protection Engine to detect unknown, recent, and new threats through dynamic categorization and advanced heuristics
- Enhanced performance and scalability
- Provides flexible and powerful control over files that cannot be accurately scanned. For example, encrypted files or malformed containers

- Integration with Active Directory® for single-sign on

Key benefits

- Provides high-performance scanning of files for viruses, malware, spyrware, 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

Supported NAS Devices

Supported NAS platform vendors include:

BlueArc®

EMC

Hitachi ®

NetApp

Sun

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/TECH147442

System requirements

Supported operating systems

32-bit OS

- Windows® 2008 (English and Japanese)
- Windows Server® 2003 R2 (English and Japanese)
- Windows® 2003 (English and Japanese)
- Red Hat® Enterprise Linux 5.x
- Red Hat® Enterprise Linux 6.x
- SUSE® Linux Enterprise Server 11

64-bit OS

- Windows® 2012 (English)
- Windows® 2008 (English and Japanese)
- Windows® 2008 R2 (English and Japanese)
- Windows Server® 2003 R2 (English and Japanese)
- Windows® 2003 (English and Japanese)
- Solaris (SPARC) 10 and 11
- Red Hat® Enterprise Linux 6.x
- Red Hat® Enterprise Linux 5.x
- SUSE® Linux Enterprise Server 11

All the supported operating systems (Windows and Linux) are supported under

- VMware® vSphere Hypervisor™ v4.1 or later

Supported browsers

- Mozilla Firefox® 10 or later
- Microsoft® Internet Explorer® 8 (SP1) or later

Minimum hardware configuration

- Intel or AMD Server Grade Single Processor Quad Core systems or higher (Windows or Linux) or UltraSPARC (Solaris)
- Java™ Runtime Environment 6 or 7
- 4 GB random-access memory (RAM)
- 5 GB hard disk space available (10 GB of hard disk space if using URL Filtering)
- 1 NIC with static IP address running TCP/IP
- 100 Mbps Ethernet link (1 Gbps recommended)

Confidence in a connected world. ✓Symantec.

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 the global leader in security, backup, and availability 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

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.   20007094-2 07/12

Confidence in a connected world. ✓Symantec.