

Symantec AntiVirus™ V5.2 for Network Attached Storage

Fast, scalable, and reliable scanning services to protect against viruses, malware and spyware.

Overview

Symantec AntiVirus for Network Attached Storage provides scalable, high-performance virus scanning and repair services to protect valuable data stored on network-attached storage devices. This solution provides increased scanning performance and improved detection capabilities for protection against multi-blended threats. Symantec AntiVirus for Network Attached Storage employs award-winning Symantec antivirus technologies using Symantec™ Scan Engine to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed-file formats. Virus definitions and engines are updated automatically with no interruption in virus scanning using Symantec LiveUpdate™. For even more frequent updates version 5.2 support Rapid Release. The solution easily accommodates growing traffic volumes with load-balancing across multiple servers running this software, providing highly scalable virus protection. Symantec AntiVirus for Network Attached Storage is certified for a long list of leading network-attached storage devices. The solution runs on Microsoft® Windows® 2000 Server and Windows Server 2003 (on x86 platforms), Sun™ Solaris™ 9/10 (on SPARC platforms), Red Hat® Enterprise Linux® Server 4.0/5.0 (on x86 platforms), and SuSE Enterprise Linux Server 9/10 (on x86 platforms).

What's New in 5.2

- Improved performance through changes to default tuning parameters
 - Rapid Release antivirus definition support
 - Resource consumption reporting including details on:
 - Running threads
 - Scan statistics
 - Number of processors in use by SAV for NAS
 - Log file size and available disk space
 - Support for Symantec Security Information Manager (SSIM)
 - Added support for Red Hat Enterprise Linux 5 and SuSE Enterprise Linux 10
-

Key benefits

- Provides high-performance scanning of files for viruses, malware, spyware, worms, and Trojan horses
- Easily integrates with third-party NAS devices via version 1.0 of the ICAP protocol
- 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 used
- Improved alerting allows event triggers to be sent via email or SNMP alerts when a predetermined number of events occur
- Central quarantine allows administrators to redirect

all irreparable, virus-infected files to a safe area on a centralized server

- Improved logging captures more event details
- User friendly Java™ based GUI to easily manage SAV for NAS. Includes a home page with valuable statistical and system information

Advantages of SAV for NAS

- Uses the same AV technology in ALL Symantec AV products (Norton, SAVCE, SEP)
- Only AV engine that has been the leader in the last 40 Virus Bulletin tests see next slide
- Scalable solution, can run many SAV for NAS servers in parallel and use round robin DNS to load balance
- One-to-one, one-to-many, many-to-one and many-to-many connections between application and scan engine
- Uses industry Standard ICAP protocol for communication
- Runs on Red Hat Linux, SuSE Linux, Windows 2000 and 2003 Server and Solaris SPARC
- Best performing server based AV in the industry
- Backed up by Symantec's worldwide Security Response organization
- Viruses research centers in every region of the world
- Lowest false positive rate of any major AV vendor
- Supports Rapid Release
- Virus definitions updated every 30 minutes

Supported NAS Devices

The following Network Attached Storage devices have been validated by their vendor to work with SAV 5.2 for NAS:

- BlueArc® Titan NAS Server (version 4.0 or later)
- EMC Celerra® Network Server (Celerra Antivirus Agent 3.6 or later)
- Hitachi® AMS/WMS with NAS Option (version 04-03 or later)
- Hitachi® High-performance NAS Platform™ (version 4.0 or later)
- Hitachi® USP/NSC NAS Blade (version 03-07 or later)
- Network Appliance™ (NetApp) Filer™ (Data ONTAP™ version 6.1.3R2 or later)
- Sun® StorageTek™ 5000 NAS Appliance (Sun NAS Firmware 4.20 or later)
- Sun® StorageTek™ 9990 NAS/9985 NAS (version 03-07 or later)
- Sun® StorageTek™ 7000 NAS version 2008.10

Check the SAV 5.2 for NAS web page on www.symantec.com for additional NAS devices that have been certified after the release of this datasheet.

-
- A software application or network device capable of making a TCP/IP connection over a network to the Symantec Scan Engine for each file (request) to be scanned
 - Operating system—one of the following:
 - Microsoft Windows 2000 Server with Service Pack 3

Data Sheet: Messaging Security Symantec AntiVirus™ V5.2 for Network Attached Storage

- Windows Server 2003 (x86 and x64)
- Solaris 9 or 10 (SPARC only)
- Red Hat Enterprise Linux 4/5 AS/ES (x86)
- SUSE Enterprise Linux 9/10 (x86)
- Minimum Hardware
 - 2.4 GHz Intel® Pentium® 4 or 1 GHz SPARC processor
 - 1 GB RAM
 - Minimum of 500 MB available hard disk space
 - NIC running TCP/IP with a static IP address
- Web-based administration requires
 - Java JRE 5 or later
 - Microsoft Internet Explorer® 6.0 (SP1) or later or
 - Firefox 1.5 or later

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 is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

Confidence in a connected world.

