



## Symantec AntiVirus™ for Caching

*Fast, scalable, and reliable virus protection for application files on caching devices*

### > The need for virus protection on caching devices

Rapid access to content is critical to the success of enterprises of all sizes. Content delivery can be accelerated and bottlenecks reduced by storing repetitive, bandwidth-consuming content closer to end users and centrally managing its flow via the use of caching devices. Because cached data consolidates enterprise traffic, it is an ideal point to check the traffic for viruses. While many organizations have deployed virus protection at the SMTP gateway to stop email-borne threats, the HTTP caching gateway is often overlooked. Casual employee Web surfing and downloads expose organizations to risk at the gateway even before these threats can affect desktops. At the same time, Web-based email opens a new virus propagation route that many organizations believe was closed through the deployment of SMTP gateway protection. Symantec AntiVirus for Caching provides a powerful and scalable solution to protect against the spread of viruses through caching devices.

### > Fast, scalable, and reliable virus protection

Symantec AntiVirus™ for Caching provides high-performance virus scanning and repair services for HTTP and FTP over HTTP traffic served through the caching device to ensure that infected files do not enter and spread throughout the network.

- ACCOMMODATES VOLUME VIRUS SCANNING – Symantec AntiVirus for Caching employs award-winning Symantec technologies – including Symantec AntiVirus Scan Engine – to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats.
- OPTIMIZED FOR SPEED AND RAPID DEPLOYMENT – To ensure highly scalable virus protection, the solution easily accommodates growing traffic volumes with automatic load balancing across multiple servers.
- VIRUS PROTECTION FOR WEB TRAFFIC – The solution utilizes Symantec antivirus technologies to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats.

### > Ease of management and flexible deployment

The solution includes features to ease management:

- REMOTE MANAGEMENT – Enables administrators to remotely manage virus protection, as well as configuration, logging, reporting, and alerting.
- OFFERS SEAMLESS INTEGRATION – The solution easily integrates with third-party software and hardware caching devices using the ICAP 1.0 protocol.
- CERTIFIED FOR LEADING CACHING DEVICES – Symantec AntiVirus for Caching is certified for Blue Coat ProxySG™, Network Appliance® NetCache, and Cisco's ACNS Content Engines.
- PROVIDES AUTOMATIC UPDATES – Virus definitions and engines are updated automatically using Symantec Live Update™ with no interruption in scanning.
- SUPPORTS HETEROGENEOUS NETWORK ENVIRONMENTS – The solution runs on Microsoft® Windows® 2000/2003 Server platforms, Sun® Solaris®, and Red Hat® Linux® server so it can be easily deployed in multi-vendor hardware environments.

### KEY POINTS

- > Provides scalable and reliable virus protection for traffic served through, or stored on, caching devices
- > Enables administrators to remotely manage virus protection, as well as configuration, logging, reporting, and alerting
- > Virus protection for both HTTP and FTP/HTTP traffic
- > Employs award-winning Symantec technologies – including Symantec AntiVirus Scan Engine – to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats
- > Support for version 1.0 of the Internet Content Adaptation Protocol (ICAP 1.0), an industry standard which allows the deployment of antivirus services at the gateway with minimal network latency
- > Virus definitions and engines are updated automatically using Symantec LiveUpdate™ with no interruption in virus scanning
- > Easily accommodates growing traffic volumes with automatic load balancing
- > Certified for leading caching solutions, including Blue Coat ProxySG™, Network Appliance® NetCache, and Cisco's ACNS Content Engines
- > Runs on Sun® Solaris®, Red Hat® Linux®, and Microsoft® Windows® 2000/2003 Server platforms
- > Backed by Symantec™ Security Response, the world's leading Internet security research and support organization

➤ **Backed by Symantec™ Security Response**

Backed by Symantec™ Security Response – the industry’s largest dedicated team of virus experts working 24 hours per day, 7 days per week – and Symantec’s proven response capabilities for tracking new virus outbreaks, identifying new virus threats and providing repairs, Symantec AntiVirus™ for Caching is an effective solution for detecting and eliminating viruses.

For more information about Symantec AntiVirus for Caching, visit  
<http://enterprisesecurity.symantec.com>

**VIRUS PROTECTION IS A KEY COMPONENT OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.**

**SYSTEM REQUIREMENTS**

SYMANTEC ANTIVIRUS FOR CACHING 4.3

ONE OR MORE OF THE FOLLOWING PRODUCTS ARE REQUIRED:

- Blue Coat ProxySG™
- Network Appliance® NetCache
- Cisco's ACNS Content Engines
- Required Symantec AntiVirus Scan Engine Connector

SYMANTEC ANTIVIRUS FOR CACHING 4.3 ON WINDOWS 2000/2003 SERVER PLATFORMS

- Windows Server 2003 or Windows 2000 Server or Advance Server with Service Pack 2 or later
- 500 MHz Pentium® III
- 256 MB RAM
- 25 MB hard disk space available
- 1 NIC running TCP/IP with a static IP address
- Web-based administration requires Microsoft Internet Explorer 6.0 or later
- LiveUpdate™ of virus definitions requires an Internet connection

SYMANTEC ANTIVIRUS FOR CACHING 4.3 ON SUN SOLARIS

- Solaris 7,8, or 9
- 400 MHz SPARC® CPU
- 256 MB RAM
- 35 MB hard disk space available
- 1 NIC running TCP/IP with a static IP address
- Web-based administration requires Microsoft Internet Explorer 6.0 or later
- LiveUpdate™ of virus definitions requires an Internet connection

SYMANTEC ANTIVIRUS FOR CACHING 4.3 ON RED HAT LINUX

- Red Hat Linux 7.3, 8.0, or 9.0
- 500 MHz Pentium® III
- 256 MB hard disk space available
- 25 MB hard disk space available
- 1 NIC running TCP/IP with a static IP address
- Web-based administration requires Microsoft Internet Explorer 6.0 or later
- LiveUpdate™ of virus definitions requires an Internet connection

**WORLD HEADQUARTERS**

**20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
408 517 8000  
800 721 3934**

**For Product Information  
In the U.S., call toll-free  
800 745 6054**

**[www.symantec.com](http://www.symantec.com)**

**Symantec has worldwide  
operations in 35 countries.  
For specific country  
offices and contact numbers  
please visit our Web site.**