

Symantec™ Sygate™ Enterprise Protection

Integrated endpoint protection and network access control (NAC) on a single agent

Overview

Symantec™ Sygate™ Enterprise Protection provides advanced endpoint protection and seamless integration with network access control in one management architecture. Protect managed endpoints against known and unknown attacks with desktop firewall, Host-based Intrusion Prevention, and Adaptive Protection. Secure networks against non-compliant endpoints via integration with Symantec™ Network Access Control (NAC), featuring broad integration support of network infrastructure. Eliminate unwelcome audit findings by enforcing Compliance on Contact™ with the enterprise network using the Endpoint Compliance option, Symantec Network Access Control, and Endpoint Discovery. Manage the integrated solution with Symantec's distributed Policy Management, offering real-time policy distribution, ease-of-use, and proven scalability.

Key benefits

- Helps prevent security incidents
 - Increases network availability
 - Helps ensure regulatory compliance
 - Helps rid the network of non-compliant endpoints with Symantec™ Network Access Control
 - Helps ensure Compliance on Contact™ across all entry points
 - Protects endpoints with host intrusion prevention
-

Features and technical specifications

How it works

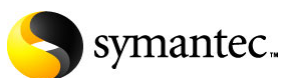
- Policy creation and deployment centrally managed

through Symantec™ Policy Manager

- Host integrity checks include compliance status via Symantec™ Protection Agent
 - Network Intrusion Prevention System blocks network-based attacks and allows authorized network traffic
 - Application protection blocks exploits and allows authorized executables
 - Operating system protection blocks exploits and allows authorized operations
 - Device control blocks transfer of data to unauthorized removable media devices and allows transfer of data to authorized devices
 - Network Access Control endpoint enforcement via Symantec Network Access Control Enforcers
 - Automatic remediation brings endpoints into compliance without user intervention
 - Buffer overflow protection prevents buffer overflow attacks before malicious code is executed
 - Adaptive Policies apply appropriate policies based upon network connection type and/or network location
-

Example Scenarios

- Targeted attack on a business-critical server
- Infected guest computer connecting to the corporate network
- Information theft through an iPod or USB key



System requirements

Symantec™ Sygate Enterprise Protection

Supported Platforms

Symantec Policy Manager

- Operating Systems: Windows® Server 2003 Standard or Enterprise
- Database:
 - Microsoft® SQL 2000 (SP3 or higher)
 - Integrated Database
- Web Server: Internet Information Services

Symantec Protection Agent

- Operating Systems:
 - Windows 2000 Professional
 - Windows 2000 Server
 - Windows 2000 Advanced Server
 - Windows 2000 Datacenter Server
 - Windows XP Home Edition or Professional
 - Windows Server 2003 Standard or Enterprise

Symantec Enforcers

- Operating System:
 - RedHat Linux ES 3 (Kernel 2.4.21-27EL)
 - RedHat Linux ES (Kernel 2.4.21-4EL)

More information

Visit our web site

<http://enterprisesecurity.symantec.com>

To speak with a Product Specialist in the US

Call toll-free (800) 745-6054

To speak with a Product Specialist outside the US

Symantec has operations in 40 countries. For specific country offices and contact numbers, visit our web site.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of 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

(408) 517-8000

(800) 721-3934

www.symantec.com

