

Symantec™ Network Access Control

Enforce IT security policy through the enterprise network on managed and unmanaged endpoints

Overview

Symantec Network Access Control increases security, network availability, and regulatory compliance by enabling enterprises to enforce security settings and software running on the hosts connected to their enterprise networks. Symantec's Universal NAC solution does this on the industry's largest array of network equipment, access methods, and protocols, maximizing ROI by eliminating ties to specific vendors. Integrates seamlessly with Symantec Sygate™ Enterprise Protection and Symantec Sygate Policy Manager in a single management architecture.

Key benefits

- Increases network availability
 - Reduces malicious code propagation
 - Helps ensure regulatory compliance
 - Discovers endpoints and compliance with security policies
 - Remediates non-compliant endpoints
 - Continuously monitors the network
-

Features and technical specifications

Enforcement technologies

- Self-enforcement for when agents leave the network
- API-based integration with dialers and VPNs
- Gateway enforcement for in-line enforcement on any network

- On-Demand Agents for unmanaged devices connecting through SSL VPNs, Web-based applications, and wireless switches
- DHCP-based approach for LAN and Wireless over any infrastructure
- 802.1x standards-based approach for LAN and wireless networks
- Cisco® Network Admission Control integration

How it works

- Policy creation centrally managed through Symantec Policy Manager
- Host Integrity checks include compliance status via Symantec Enforcement Agent
- Network access control enforcement via Symantec Network Access Control Enforcers (appliance and/or software)
- Non-compliant device remediation brings non-compliant endpoints to compliance without user intervention

Example scenarios

- Salesperson connecting to a hotel network
- Guest accessing the Internet through the corporate wired or wireless LAN
- Infected out-of-date desktop computer on the corporate network



Data Sheet: Integrated Security Symantec Network Access Control

System requirements

Symantec Network Access Control

Symantec Network Access Control requirements

Symantec Sygate Policy Manager

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

Symantec Enforcer

- Symantec Network Access Control Enforcer 6100 Series

| | |
|------------------|----------------------------------------------------|
| Rack units | 1 |
| Dimensions | 1.68" x 17.60" x 21.5" |
| Processor | 1x2.8 Ghz Intel Pentium® 4 processor |
| Memory | 1 GB |
| Storage | 1 x 160 GB (SATA) |
| Network adaptors | 2 |
| Ethernet NIC | Intel Pro 1000MT Dual Port Gigabit network adapter |
| Platform | Pre-hardened Red Hat® Linux® operating system |

- Software only
 - Red Hat Linux ES 3 (Kernel 2.4.21-27EL)
 - Red Hat Linux ES 3 (Kernel 2.4.21-4EL)

Symantec Enforcement Agent

- Operating System:
 - 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

More information

Visit our Web site

<http://enterprisesecurity.symantec.com>

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

Call toll-free (800) 745 6054

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

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 Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

