

Symantec™ Network Access Control

Deployable, scalable, manageable network access control – today.

Overview

Symantec® Network Access Control is a complete end-to-end network access control solution which enables organizations to efficiently and securely control access to corporate networks through integration with existing network infrastructures. Regardless of how endpoints connect to the network, Symantec Network Access Control discovers and evaluates endpoint compliance status, provisions the appropriate network access, provides remediation capabilities if needed, and continually monitors endpoints for changes in compliance status. The result is a network environment where corporations realize significant reductions in security incidents and increased levels of compliance to corporate IT security policy.

Symantec Network Access Control makes deploying and managing network access control an achievable and cost-effective goal.

Authorizing endpoints, not just users

In today's computing environments organizations and network administrators are challenged with providing access to corporate resources for a growing user population. This includes both onsite and remote employees, as well as guests, contractors, and other temporary workers. Never before has the burden of maintaining the integrity of network environments been more challenging. It is no longer acceptable to provide unchecked access to the network. With the significant increase in the numbers and types of endpoints

accessing your systems, organizations must have the ability to verify the health and posture of endpoints, both prior to connecting to resources as well as on a continual basis after endpoints connect. Symantec Network Access Control ensures endpoints are in compliance with IT policy before they are allowed to connect to the corporate LAN, WAN, WLAN, or VPN.

Key benefits

Organizations deploying Symantec Network Access Control experience multiple measurable benefits.

These include:

- Reduced propagation of malicious code such as viruses, worms, spyware, and other forms crime-ware
- Lowered risk profile through increased control of unmanaged and managed endpoints accessing the corporate network
- Greater network availability and reduced disruption of services for end-users
- Verifiable organizational compliance information through real-time endpoint compliance data
- Minimized total cost of ownership as a result of an enterprise-class centralized management architecture

Key features



Network access control process

Network access control is a process - a process which mandates coverage for all types of endpoints and all types of networks. It is a process that begins prior to connection to the network and continues throughout the duration of the connection. As with all corporate processes, policy serves as the basis for evaluations and actions.

Four step network access control process:

1. Discover and evaluate endpoints

Discover endpoints as they connect to the network and prior to accessing resources. Through integration with existing network infrastructure and the usage of intelligent agent software, network administrators are assured that new devices connecting to the network are evaluated according to minimum IT policy requirements.

2. Provision network access

Full network access is granted only after systems are evaluated and determined to be in compliance with IT

policy. Systems not in compliance, or failing to meet the minimum security requirements for your organization, are quarantined with limited or no access to the network.

3. Remediate non-compliant endpoints

Automatic remediation of non-compliant endpoints empowers administrators to quickly bring endpoints into compliance and subsequently alter network access accordingly. Administrators can either fully automate the remediation process, resulting in a fully transparent process to the end-user, or provide remediation information to the user for manual remediation

4. Proactively monitor compliance

Adherence to policy is a full-time issue. As such, Symantec Network Access Control actively monitors, on an administrator-set interval, the compliance posture for all endpoints. If at any time the endpoint's compliance status changes, so will the network access privileges of the endpoint.

Pervasive endpoint coverage

Networks are comprised of new and legacy corporate systems, contractor systems, guest systems, public kiosks, business partners, and any number of other unknown systems. Administrators often have little or no control over the management of many of these endpoints, yet must ensure the security and availability of the network. Symantec Network Access Control makes it possible for organizations to apply the network access control process to devices — managed or unmanaged, legacy or new, known or unknown.

Deployable in any network

The typical corporate user connects to the network via multiple access methods; as a result, administrators must have the flexibility to consistently apply evaluation and connection controls regardless of the connection type. As one of the most mature network access control solutions on the market today, Symantec Network Access Control allows network administrators to actively enforce compliance through existing investments in network infrastructure with no required network equipment upgrades.

Whether using one of the Symantec Network Access Control Enforcers that integrate directly into the network — the host-only enforcement option requiring no network integration, or a dissolvable agent integrated into your web-application environment, organizations are assured end-users and endpoints are in compliance at the point of contact to the corporate network.

Network Access Control architecture

Because IT begins at the endpoint: The Symantec Network Access Control architecture includes three core components; policy management, endpoint evaluation, and network enforcement. All three component pieces work together as a single solution without relying upon external elements for functionality.

Centralized policy management and reporting

Paramount to the efficient operation of any solution is an enterprise-class management console. The Symantec Sygate™ Policy Manager provides a Java™-based console

to centrally create, deploy, manage, and report agent and Enforcer activity. Scalable to fit the most demanding environments in the world, the policy manager provides granular control to all administrative tasks in high-availability architecture.

Endpoint evaluation

Network access control protects the network from malicious code and from unknown or unauthorized endpoints, but it also verifies that endpoints connecting to the network are configured properly so they are protected from online attacks. Regardless of the goal, the process begins with evaluating the endpoint. While checking for antivirus, anti-spyware, and installed patches are several of the common minimum requirements for allowing network access, most organizations quickly expand well beyond these minimums after the initial network access control deployment.

Symantec Network Access Control offers three distinct endpoint evaluation technologies when determining endpoint compliance.

Persistent agents

Corporate-owned and other managed systems use an administrator-installed agent to determine compliance status. Check antivirus, anti-spyware, installed patches, as well as complex system status characteristics such as registry entries, running processes, and file attributes. Persistent agents provide the most in-depth, accurate, and reliable system compliance information, while also offering the most flexible remediation and repair functionality of assessment options.

Dissolvable agents

For non-corporate devices or systems not currently managed by administrators, Java™-based agents are delivered on-demand and without administrative privileges to evaluate endpoint compliance posture. At the end of the session, these agents automatically remove themselves from the system.

Remote vulnerability scanning

Remote vulnerability scanning provides compliance information to the Symantec Network Access Control enforcement infrastructure based upon remote unauthenticated vulnerability scan results from the Symantec Network Access Control Scanner. Remote scanning extends the information gathering functionality to systems for which there is no agent-based technology currently available.

Enforcement

Each organization's network environment is unique in how it has evolved over time, and as a result, no single enforcement method has the ability to effectively control access to all points on the network. Network access control solutions must be flexible enough to easily integrate multiple enforcement methods into the existing environment without increasing management and maintenance overhead. Symantec Network Access Control allows you to select the most appropriate enforcement method for different parts of your network without increasing operational complexity or cost. Each of the network-based enforcement methods is available as software-only or appliance delivered components.

LAN Enforcer – 802.1X

LAN Enforcer is an out-of-band 802.1X RADIUS proxy solution that works with all major switching vendors supporting the 802.1X standard. The LAN Enforcer can participate with an existing AAA identity-management architecture authenticating users and endpoints, or act as an independent RADIUS for environments only requiring endpoint compliance validation. The LAN Enforcer provisions switch port access dependant upon authentication results for connected endpoints.

DHCP Enforcer

DHCP Enforcer is deployed in-line between endpoints and the existing DHCP service infrastructure and acts as a DHCP proxy. Restrictive DHCP lease assignments are given to all enforced endpoints until policy compliance is verified, at which time a new DHCP lease is assigned to the endpoint. Integration of the DHCP Enforcer with Microsoft DHCP Server enables the rapid deployment of network access control without deploying additional devices to the network.

Gateway Enforcer

Gateway Enforcer is an in-line enforcement device used at network choke points which controls the flow of traffic through the device based upon policy compliance of remote endpoints. Whether the choke point is at perimeter network connection points, such as WAN links or VPNs, or on internal segments accessing critical business systems, Gateway Enforcer efficiently provides controlled access to resources and remediation services.

Datasheet: Endpoint Security

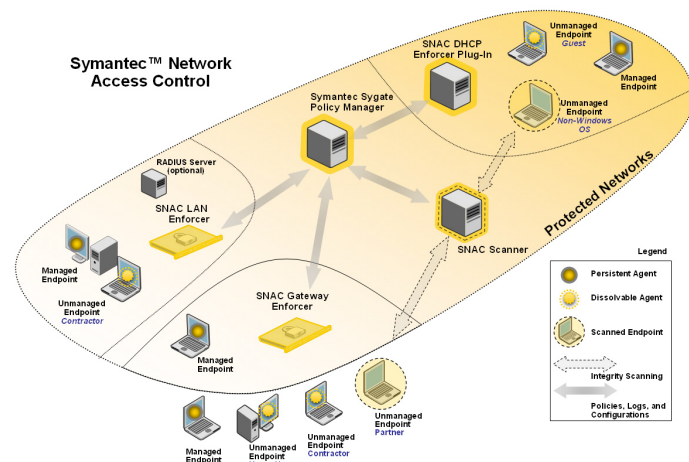
Symantec™ Network Access Control

Self-enforcement

Self-Enforcement leverages the host-based firewall capabilities within the Symantec™ Protection Agent to adjust local agent policies according to endpoint compliance status. This allows administrators to control access to any network, on or off the corporate network, for devices such as laptops that routinely move between multiple networks.

Cisco Network Admission Control and Microsoft Network Access Protection

While Symantec Network Access Control provides end-to-end control functionality without requiring external solutions, it also integrates with and enhances other network access control technologies. Security administrators can be assured they have comprehensive coverage and control irrespective of enforcement methodology.



Symantec Network Access Control

Platform support

Symantec Sygate™ Policy Manager

Operating System:

- Windows® Server 2003 Standard or Enterprise

Database:

- Microsoft® SQL 2000 (SP3 or higher)
- Integrated Database

Web Server: Microsoft® Internet Information Services

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
- Apple OS X 10.4+

Symantec Network Access Control Scanner

Operating System:

- Windows 2000 Server SP4
- Windows 2000 Professional SP4
- Windows 2003 Server SP1
- Windows XP Professional SP2

Minimum processor Pentium 4 1.8 GHz

1GB of RAM minimum

1GB free hard disk space

Internet Explorer 5.5 or later Windows 2000

Professional



Symantec Network Access Control Enforcer 6100 Series

Base Appliance Option (Gateway, LAN & DHCP)

- 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 Gbit network adapter
- Platform Pre-hardened Linux® operating system

Fail Open Appliance Option (Gateway, LAN & DHCP)

- 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
- Quad port 10/100/1000 copper network interface card with bypass
- Platform Pre-hardened Linux® operating system

Software-only Delivery Option

(Gateway, LAN & DHCP)

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

Microsoft DHCP Server Plug-in Option

Installs directly on Microsoft DHCP servers, eliminating the need for an external DHCP Enforcer device.

– Operating System:

- Windows® Server 2000
- Windows 2003 Standard or Enterprise
- Microsoft DHCP Server

More endpoint information

Visit our endpoint Web site page at:

<http://www.symantec.com/endpoint>

Datasheet: Endpoint Security Symantec™ Network Access Control

More information

Visit our web site

<http://enterprise.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

