Data Sheet: Endpoint Security

Symantec™ Network Access Control

Comprehensive Endpoint Enforcement

Overview

Symantec™ Network Access Control is a complete, end-to-end network access control solution that 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 can realize significant reductions in security incidents and increased levels of compliance with 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

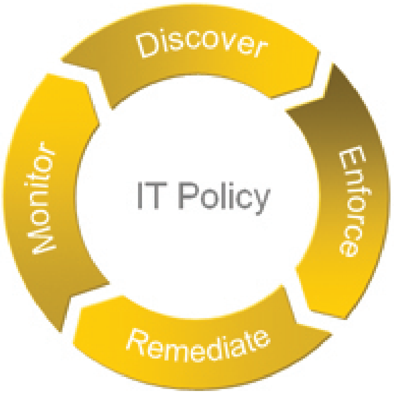
In today's computing environments, organizations and network administrators are challenged with providing access to corporate resources for a growing user population. This includes both onsite and remote employees, as well as guests, contractors, and other temporary workers. Never before has the burden 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 their systems, organizations must have the ability to verify the health and posture of endpoints, both prior to connecting to resources and on a continual basis after endpoints connect. Symantec Network Access Control helps ensure that 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 of crimeware
- 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
- Verification that endpoint security investments such as antivirus and client firewalls are properly enabled
- Seamless integration with Symantec™ Endpoint Protection

Key features



Symantec Network Access Control process

Symantec Network Access Control is a process—one that mandates coverage for all types of endpoints and all types of networks. It 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.

The process consists of four steps:

1. Discover and evaluate endpoints. This occurs as endpoints connect to the network and before they access resources. Through integration with the existing network infrastructure and the use of intelligent agent software, network administrators can be 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 the organization, are quarantined with limited or no access to the network.

3. Remediate noncompliant endpoints. Automatic remediation of noncompliant endpoints empowers administrators to quickly bring them into compliance and subsequently alter network access. Administrators can either fully automate the remediation process, resulting in a fully transparent process to the end user, or provide 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 composed 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 are charged with keeping the network secure and available. 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; therefore, administrators must have the flexibility to apply evaluation and connection controls consistently, 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 the Web application environment, organizations can be assured that end users and endpoints are in compliance at the point of contact to the corporate network.

Symantec Network Access Control architecture

The Symantec Network Access Control architecture includes three core components: policy management, endpoint evaluation, and network enforcement. All three components 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 Endpoint Protection Manager provides a Java™ technology–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 a 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, antispyware, 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. It checks antivirus, antispyware, and 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 offering the most flexible remediation and repair functionality of assessment options.
- **Dissolvable agents—**For noncorporate 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, uncredentialed 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

The evolution of each organization's network environment is unique, 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. Network-based enforcement options are available in the form of an appliance or plug-in.

Network-Based Enforcement

- **LAN Enforcer 802.1X** is an out-of-band 802.1X RADIUS proxy solution that works with all major switching
- **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 plug-in enables the rapid deployment of network access control without deploying additional devices to the network.
- **Gateway Enforcer** is an in-line enforcement device used at network choke points. It 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.
- **Microsoft® Network Access Protection (NAP) Enforcer** augments NAP's native capabilities by providing more comprehensive compliance-checking options and adds custom compliance checks. Organizations can deploy NAP quickly and easily through the unified architecture and simplified user interface provided by Symantec Network Access Control.

Host-Based 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.

- **Peer-to-Peer Enforcement** ensures that client-to-client communication can only occur between endpoints that are owned and managed by the organization and between endpoints that are compliant with defined endpoint security policies.

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 that they have comprehensive coverage and control irrespective of enforcement methodology.

Support services

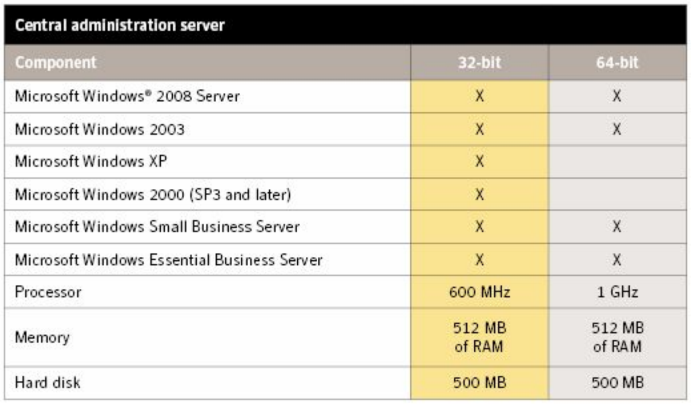
Symantec provides a range of consulting, technical education, and support services that can guide organizations through the migration, deployment, and management of Symantec Network Access Control and help them realize the full value of their investment. For organizations that want to outsource security monitoring and management, Symantec also offers Managed Security Services to deliver real-time security protection.

Symantec Network Access Control Starter Edition product family		
	Symantec Network Access Control	Symantec Network Access Control Starter Edition
Central management		
Symantec Endpoint Protection Manager	X	X
Enforcement		
LAN 802.1X	X	
DHCP	X	
Gateway	X	X
Microsoft NAP	X	X
Self-enforcement	X	X
Peer-to-Peer	X	X
Endpoint evaluation		
Persistent agent	X	X
Dissolvable agent	X	X
Remote vulnerability scanning*	X	X
* = purchased separately		

Minimum system requirements

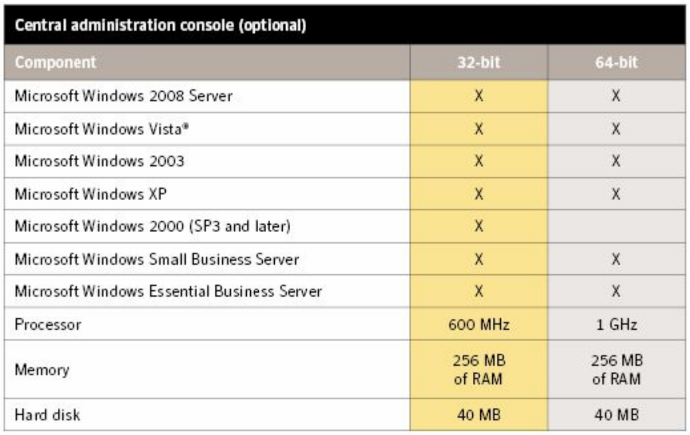
Platform support

Symantec Endpoint Protection Manager



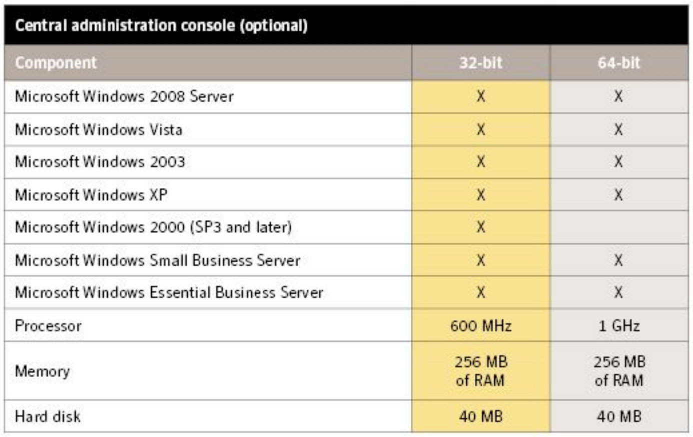
Central administration server		
Component	32-bit	64-bit
Microsoft Windows® 2008 Server	X	X
Microsoft Windows 2003	X	X
Microsoft Windows XP	X	
Microsoft Windows 2000 (SP3 and later)	X	
Microsoft Windows Small Business Server	X	X
Microsoft Windows Essential Business Server	X	X
Processor	600 MHz	1 GHz
Memory	512 MB of RAM	512 MB of RAM
Hard disk	500 MB	500 MB

Symantec Endpoint Protection Console



Central administration console (optional)		
Component	32-bit	64-bit
Microsoft Windows 2008 Server	X	X
Microsoft Windows Vista®	X	X
Microsoft Windows 2003	X	X
Microsoft Windows XP	X	X
Microsoft Windows 2000 (SP3 and later)	X	
Microsoft Windows Small Business Server	X	X
Microsoft Windows Essential Business Server	X	X
Processor	600 MHz	1 GHz
Memory	256 MB of RAM	256 MB of RAM
Hard disk	40 MB	40 MB

Symantec Network Access Control Client



Central administration console (optional)		
Component	32-bit	64-bit
Microsoft Windows 2008 Server	X	X
Microsoft Windows Vista	X	X
Microsoft Windows 2003	X	X
Microsoft Windows XP	X	X
Microsoft Windows 2000 (SP3 and later)	X	
Microsoft Windows Small Business Server	X	X
Microsoft Windows Essential Business Server	X	X
Processor	600 MHz	1 GHz
Memory	256 MB of RAM	256 MB of RAM
Hard disk	40 MB	40 MB

Symantec Network Access Control Enforcer 6100 Series Appliance

Rack units	1
Dimensions	1.68" x 17.60" x 21.5"

Microsoft DHCP Server Plug-in option installs directly on Microsoft DHCP servers, eliminating the need for an external DHCP appliance.

Symantec Network Access Control Scanner (optional)

- Microsoft Windows 2000 Server SP4
- Microsoft Windows 2003 Server SP1
- Microsoft Window 2000 Professional
- Intel® Pentium® 4 1.8 GHz minimum
- 1 GB of RAM minimum
- Internet Explorer® 5.5 or later

Visit Our Web Site

http://enterprise.symantec.com

Contact Us Today

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.

12/08 12836809-3