



Symantec™ Network Access Control

Comprehensive Network
Access Control

Symantec Network Access Control

Comprehensive Network Access Control

Contents

Executive summary	4
Maintaining a secure and managed state	5
The Symantec Network Access Control architecture	6
Symantec endpoint evaluation technologies: Flexible and comprehensive	8
Persistent agents	9
Dissolvable agents	10
Remote vulnerability scanning	12
Symantec Enforcers: Flexible enforcement options for eliminating IT and business disruptions	12
Gateway Enforcer	14
DHCP Enforcer	15
LAN Enforcer—802.1x	16
Symantec policy management: Comprehensive, integrated endpoint security management	18
Single management console	19
Unified agent	19
Eliminating network access control obstacles	19
End-to-end endpoint compliance	20

Executive summary

The managed state of an organization's individual endpoints plays a critical role in the overall security and availability of its IT infrastructure and related business operations. The new wave of sophisticated crimeware not only targets specific companies, but it also targets desktops and laptops as backdoor entryways into those enterprises' business operations and valuable resources. To safeguard themselves against these targeted threats, organizations must have a means to guarantee that each endpoint continually complies with corporate security and configuration management policies. Failure to guarantee endpoint policy compliance leaves organizations vulnerable to a wide array of threats, including the proliferation of malicious code throughout the enterprise, disruption of business-critical services, increased IT recovery and management costs, exposure of confidential information, damage to corporate brand, and regulatory fines due to non-compliance.

Symantec Network Access Control enables organizations to ensure the proper configuration and security state of user endpoints—including those of onsite employees, remote employees, guests, contractors, and temporary workers—before they are allowed to access resources on the corporate network. It discovers and evaluates endpoint compliance status, provisions the appropriate network access, and provides remediation capabilities to ensure that endpoint security policies and standards are met. Symantec Network Access Control is network OS-neutral and easily integrates with any network infrastructure, making its implementation more comprehensive, easier, faster, and more cost-effective than competing solutions.

By leveraging the endpoint compliance verification and enforcement capabilities of Symantec Network Access Control, organizations can enjoy:

- 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 near-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 firewall technologies are properly enabled

Maintaining a secure and managed state

IT administrators go to great lengths to ensure that newly deployed desktops and laptops are configured according to corporate policy, including all the applicable security updates, approved application sets, antivirus software, firewall settings, and other configuration settings. Unfortunately, as soon as those machines are put into production, administrators often lose control of the configuration of those endpoints. Users install new software, block patch updates, disable firewalls, or make other changes that put the device—and ultimately the entire IT infrastructure—at risk. Remote and mobile users create even greater exposure when they use their non-compliant laptops at Internet cafés, hotel rooms, or other non-secure locations where they are even more vulnerable to attack or infection.

Some organizations employ patch management or software distribution solutions that, on a predetermined schedule, can eventually change out-of-compliance computers back to their proper states, but once the computer has been infected and then connected to the network, those solutions do too little, too late. They also prove ineffectual against users with administrator privileges who think they are exempt from corporate policy and, as result, block attempts to roll back their computers to their proper state of configuration.

Network access control solutions enable organizations to prevent this behavior from affecting the corporate IT infrastructure. Before any computer can access the production network and its resources, that computer must be in total compliance with established corporate policy, such as proper version levels of security patches, antivirus software, and virus definitions.

However, in spite of their ability to prevent non-compliant endpoints from attaching to the corporate network, network access control solutions have not been embraced by some organizations for a variety of reasons, including the fact that many solutions:

- Fail to deliver effective enforcement and remediation
- Increase the number of management agents that must be installed on the endpoints
- Introduce too much complexity and too many disruptions to the IT infrastructure
- Lack the flexibility to meet organizations' unique needs, such as appropriately accommodating guest and temporary workers
- Fail to properly integrate with the overall endpoint security management infrastructure

Symantec Network Access Control addresses all of these concerns with an end-to-end solution that securely controls access to corporate networks, enforces endpoint security policy, and easily integrates with existing network infrastructures.

The Symantec Network Access Control architecture

The Symantec Network Access Control architecture comprises three key components:

- **Endpoint evaluation technologies** assess the state (checks if they are compliant or non-compliant with policy) of endpoints attempting to access the network
- **Enforcers** act as the gate/door that permits or denies access to the network
- **Policy management** creates, edits, and manages network access control rules or policies via a central management console

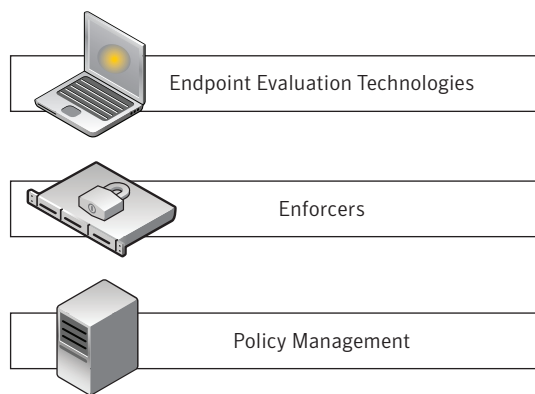


Figure 1. Symantec Network Access Control architecture

The enforcement evaluation technologies report to and receive their configuration policy information from the Symantec Endpoint Protection Manager, where policies are created, edited, and managed. If the Symantec enforcement evaluation technology determines that the endpoint is not in compliance with policy, it will tell the Symantec Enforcer to block the endpoint from accessing the network.

Based on policies set by the IT administrator (and based on the type of enforcement option deployed), the Symantec enforcement technologies are able to automatically bring non-compliant endpoints into compliance. This is accomplished by performing remediation tasks, such as calling upon a local patch manager to install the latest patches or leveraging other tools installed on the endpoint for other tasks.

Symantec Network Access Control: Comprehensive Network Access Control

Symantec Network Access Control validates and can enforce policy compliance for all types of endpoints on all types of networks. This validation and enforcement process begins prior to an endpoint's connection to the network and continues throughout the duration of the connection, with policy serving as the basis for all evaluations and actions. This network access control process executes the steps illustrated in Figure 2.

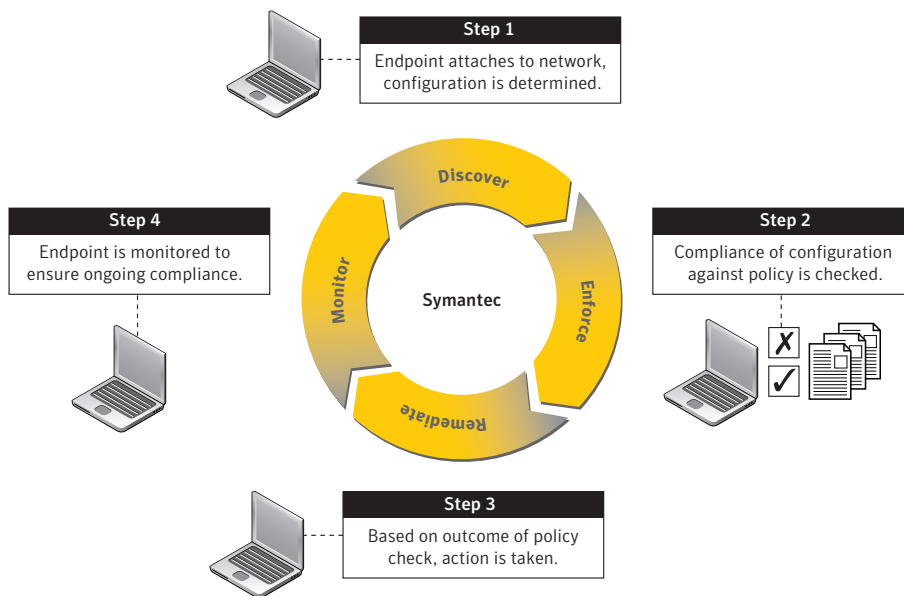


Figure 2. Network access control process

- 1. Discover and evaluate endpoints.** Discovers endpoints as they connect to the network, 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 an 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.

Symantec endpoint evaluation technologies: Flexible and comprehensive

Network access control can protect the network from malicious code and from unknown or unauthorized endpoints by verifying that endpoints connecting to the network are configured properly so that they will be protected from online attacks. Network access control typically involves checking for antivirus, antispymware, and installed patches. However, most organizations quickly expand well beyond these typical checks after the initial network access control deployment. Regardless of the goal, the process begins with evaluating the endpoint. Due to the diverse number of endpoints that connect to the network (e.g., "managed endpoints," or endpoints procured by the company, and "unmanaged endpoints," or endpoints not procured by the company, such as telecommuters using their home computers, contractors, temporary employees, and partners that might use their own laptops), Symantec Network Access Control offers three distinct endpoint evaluation technologies to determine endpoint compliance:

- Persistent agents
- Dissolvable agents
- Remote vulnerability scanning



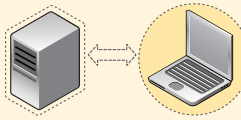
		Recommended Use	Evaluation Capabilities
	Persistent Agents	For managed endpoints	BEST
	Dissolvable Agents	For unmanaged endpoints	BETTER
	Remote Vulnerability Scanner	For unmanaged and unmanageable endpoints (e.g., UNIX devices, etc.)	GOOD

Figure 3. Endpoint evaluation technologies

Persistent agents

Corporate-owned and other managed systems use an administrator-installed agent to determine compliance status. The agent checks antivirus, antispysware, 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.

Symantec believes that the key to successful network access control also begins by deploying a persistent agent-based solution. Due to the way desktop operating systems function, to effectively examine and remediate whether certain software is properly installed and running and if the endpoint computer is properly configured or in an acceptable state, a network access control solution must be able to examine the endpoint's process table and registry, and perhaps even modify certain entries. The best way to accomplish this is through an agent that has administrator privileges and that has been installed on the endpoint at the time of initial deployment. Solutions that are completely non-agent-based do not give the administrator sufficient permissions to adequately or accurately examine the endpoint for complete compliance. Also, non-agent-based solutions will very likely not have sufficient permissions to make the necessary modifications to the endpoints to bring them into compliance.

Symantec Network Access Control: Comprehensive Network Access Control

Symantec Network Access Control provides the option of a persistent and administrator-installed enforcement agent to determine the compliance status of endpoints. The agent can check for antivirus, antispyware, installed patches, and complex system status characteristics, including registry entries, running processes, and file attributes. This persistent agent option provides the most in-depth, accurate, and reliable system compliance information needed to ensure compliance with corporate policy.

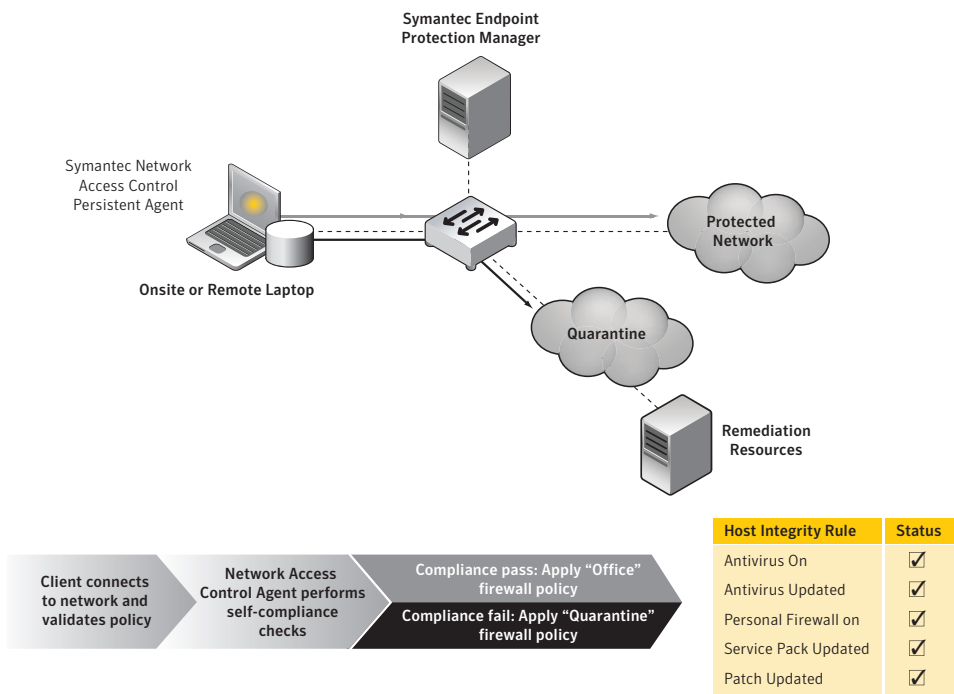


Figure 4. Persistent Agent

Dissolvable agents

One of the biggest challenges in the area of network access control is the proper handling of the admission of guest users onto the network. Productivity can be significantly and negatively impacted without an automated way to provision network access to temporary workers and guests. Time and money is wasted if contractors or temporary employees show up to work, but can't access the network for days or weeks due to manual provisioning of network access. Similarly, the same is true if automated network access control solutions unnecessarily block these users' access.

Symantec Network Access Control: Comprehensive Network Access Control

Effective network access control solutions must have the ability and flexibility to verify that a new or temporary endpoint does not pose a threat to the network, as well as determine what level of network access should be granted to the endpoint. The most accurate way to assess an endpoint is to install a full-time network access control agent onto the endpoint, but it's not usually in the best interest of the organization or the guest to deploy a full-time agent onto an endpoint that does not belong to the organization.

To address this issue, Symantec Network Access Control provides a temporary, dissolvable agent. This can be used for non-corporate devices or systems not currently managed by administrators. These 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. For example, when a guest endpoint tries to connect to the network, a network-based enforcement solution can recognize that it's not a known endpoint device and redirect it to a Web server where it can download the dissolvable, on-demand agent. The agent will perform the appropriate compliance checks, based on the policies that the administrator has defined for guests. If it's compliant, the endpoint can be granted access to the production network. When the network session ends, the agent will automatically remove itself from the endpoint.

In addition to using this redirection capability for temporary endpoints, redirection can also be used for endpoints belonging to new employees. In this case, when the endpoint is redirected to the Web server to download the agent, there might be an option for guests and another option for employees. If the user selects the employee option, a network-based enforcer can determine if the endpoint is an asset that belongs to the organization. If it is one of the organization's endpoints, then a full-time and persistent network access control agent can be deployed instead of the disposable agent.

By providing multiple options for verifying compliance with policies for endpoint status and configuration, Symantec Network Access Control ensures that the employees and guests that attempt to access an organization's network meet its minimum security standards and requirements.

Remote vulnerability scanning

Another complementary endpoint assessment method that companies can employ when they do not have the option to install a persistent agent is to utilize 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.

Depending on the different types of endpoints that connect to the network, companies may choose to use a mixture of these three endpoint evaluation technologies for complete coverage.

Symantec Enforcers: Flexible enforcement options for eliminating IT and business disruptions

Each organization's network environment is unique in how it has evolved over time, and as a result, no single enforcement method can 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 organizations to select the most appropriate enforcement method for different parts of their network without increasing operational complexity or cost.

The **network-based** enforcement methods from Symantec are available as appliance-delivered components, and include LAN, DHCP, and gateway methods, with the DHCP method also available as a software plug-in.

Symantec also offers a simple **host-based** enforcement method, known as self-enforcement. This method uses a Symantec desktop firewall to permit or deny access. The firewall is already included as part of the Symantec Endpoint Protection product offering.

The advantage of using self-enforcement is that it does not require the deployment of a network-based enforcement component to police access to the network. Rather, it uses the Symantec desktop firewall to police network access, providing the easiest and fastest enforcement deployment option. It's even easier to implement if the organization has already deployed the Symantec Endpoint Protection product.

However, the self-enforcement option only works for "managed" endpoints. It cannot address the problem of unmanaged endpoints, such as guests or temporary workers, connecting to the network. Symantec Network Access Control addresses the issues associated with unmanaged endpoints through dissolvable agents and remote vulnerability scanning.

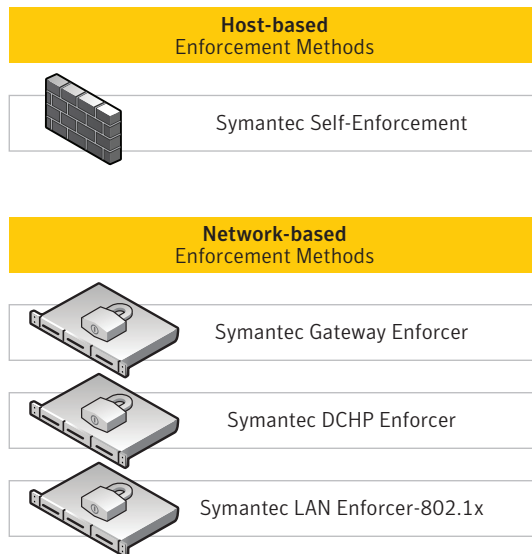


Figure 5. Classes of Symantec enforcement options

Many organizations hesitate to deploy network access control solutions because many offerings are inherently disruptive in design. Often they require expensive and time-intensive network infrastructure upgrades and changes. Many solutions are overly complex and too difficult to deploy. Some solutions require that endpoint agents be deployed simultaneously with upgrades being made to the network infrastructure. Problems encountered on either the agent or network enforcement side of the deployment result in a non-functioning solution that can be extremely difficult to troubleshoot and resolve, and that can also cause users to be inappropriately blocked from accessing the network.

Symantec helps eliminate these disruptions by providing a broad array of enforcement options that can be deployed using a simple, phased approach to deploying effective and comprehensive network access control. Network access control can easily be deployed with a Symantec host-based enforcement option. Deployments of this type require no infrastructure changes and no time-consuming deployment efforts. Organizations that are already using the Symantec Endpoint Protection solution already have the agent deployed, and simply need to enable network access control to take advantage of that capability. The host-based enforcement option is the fastest and easiest way to conduct network access control for a managed endpoint.

Symantec Network Access Control: Comprehensive Network Access Control

Organizations can implement, at their own pace, additional, network-based enforcement options offered by Symantec to supplement host-based enforcement options. Network-based enforcers are a necessary component to control unmanaged endpoints connecting to the network. These additional key network-based enforcement offerings include:

- **Gateway Enforcer**—In-line enforcement at network choke point
- **DHCP Enforcer**—DHCP-based approach for LAN and wireless networks over any infrastructure
- **LAN Enforcer—802.1x**—Out-of-band standards-based approach for LAN and wireless networks

Just like the network access control agent, the Symantec Enforcer offerings are network OS-neutral and can easily integrate with any network infrastructure. These solutions are security vendor-neutral, meaning they will work with other leading antivirus, firewall, and host intrusion prevention solutions. Since these solutions have no inherent network or infrastructure dependencies, organizations can take a phased approach to their implementation, deploying them at their own discretion and on their own timetable.

Additionally, to further simplify administration and compliance enforcement, the enforcers are all centrally managed through Symantec Endpoint Protection Manager as are the Symantec Network Access Control endpoint evaluation technologies.

Gateway Enforcer

Gateway Enforcer from Symantec is an in-line enforcement appliance deployed at network choke points, enabling it to control and block the flow of traffic from remote endpoints based on the endpoints' compliance with established corporate policy. 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, as well as remediation services to bring non-compliant endpoints back into compliance.

Typical deployment scenarios for Gateway Enforcer might be behind an IPSec VPN, WAN connections between a remote branch office and corporate headquarters, on wireless networks, on conference room networks, in front of critical servers, or in front of small data centers.

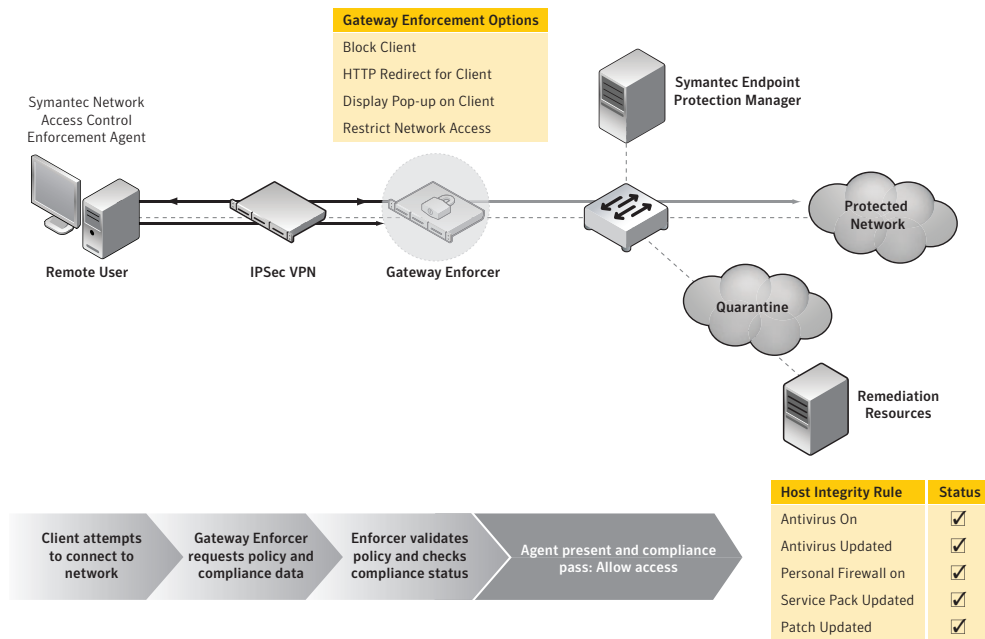


Figure 6. Gateway Enforcement

DHCP Enforcer

DHCP Enforcer from Symantec is deployed in-line between endpoints and an organization's existing DHCP service infrastructure. DHCP Enforcer issues a restrictive DHCP lease assignment if an endpoint is not running the network access control agent, is out-of-compliance, or its compliance status is unknown. This restrictive lease assignment is a non-routable or quarantined IP address that provides reduced access to the network.

DHCP Enforcer can also communicate with the endpoint agent to initiate necessary remediation actions to bring the endpoint in compliance with policy. Once in compliance, the endpoint will initiate a DHCP release and renew request. Once DHCP Enforcer receives the renewal request and determines that the endpoint is in compliance, the endpoint will be granted a DHCP lease on the normal production network, allowing full access to the network.

Since DHCP Enforcer works as an in-line DHCP proxy, it is compatible with any existing DHCP infrastructure and can work in any existing network environment with no upgrades of hardware or software. As an alternative to a DHCP Enforcer appliance, Symantec offers a DHCP Enforcer plug-in that can be installed directly on Microsoft® DHCP servers. The Microsoft DHCP server implementation enables the Microsoft DHCP server to act as the enforcement point.

LAN Enforcer—802.1x

LAN Enforcer from Symantec is an out-of-band 802.1x RADIUS proxy solution that works with all major switching vendors supporting the 802.1x standard. Nearly all wired and wireless Ethernet switch makers support the IEEE 802.1x Admission Control Protocol. LAN Enforcer uses this link-level protocol to evaluate endpoint compliance, provide automatic problem remediation, and admit compliant endpoints onto the corporate network.

During enforcement, the Symantec agent on the endpoint uses 802.1x to transmit compliance information to the network switch, which relays it to LAN Enforcer. If the endpoint is not in compliance with policy, LAN Enforcer will place it in a quarantine network where the endpoint can be remediated without impacting any of the compliant endpoints. Once Symantec Network Access Control remediates the endpoint and brings it into compliance, the 802.1x protocol will attempt to re-authenticate the user and grant access to the network.

LAN Enforcer can participate with existing AAA identity-management architectures to authenticate users and endpoints, or it can act as an independent RADIUS solution for environments that only require endpoint compliance validation, also known as transparent mode. In transparent mode, the administrator simply configures the switch to use LAN Enforcer as the RADIUS server, allowing the appliance to authenticate endpoints based on compliance with defined policy. Running LAN Enforcer in transparent mode requires no additional infrastructure and is a simple way to implement a secure, VLAN-switching-based network access control solution.

Symantec Network Access Control: Comprehensive Network Access Control

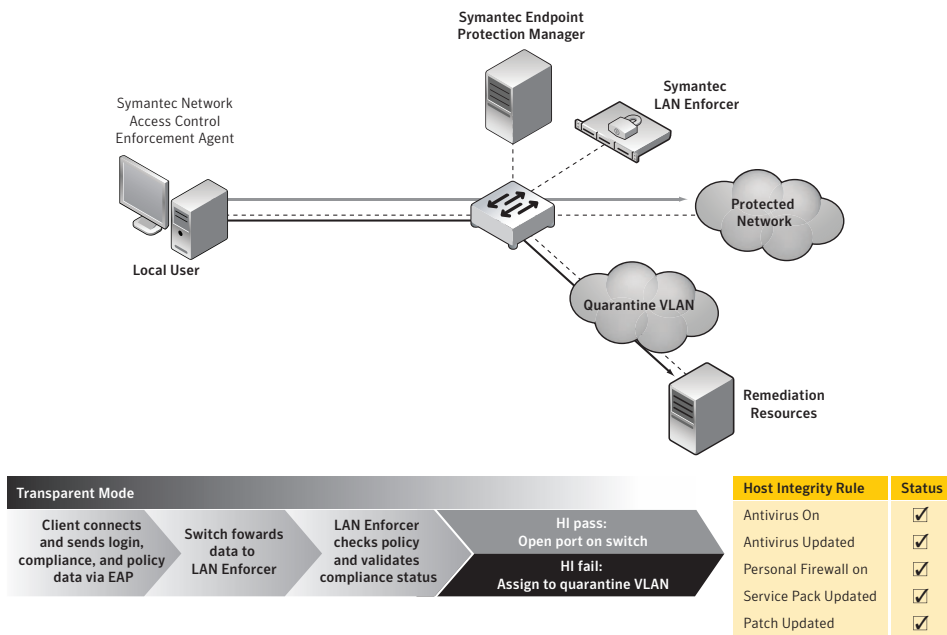


Figure 7. LAN (802.1x) Enforcement

Network access control industry framework support

Symantec Network Access Control can currently operate independently or in conjunction with Cisco® Network Admission Control. Also, it will soon work with other network access control industry frameworks, including Microsoft Network Access Protection and the Trusted Computing Group’s Trusted Network Connect standard. Both the Microsoft and Cisco technologies are architectural frameworks that focus on building protocols and interfaces that can be used by multiple vendors to provide complete network access control solutions. The Trusted Computing Group is a consortium of over 80 IT industry companies that have sponsored the Trusted Network Connect standard, which is similar in intent and architecture to the Microsoft and Cisco efforts, but is intended to operate on any type of network hardware infrastructure and any host operating system.

All of these different frameworks typically require software or hardware from several different vendors in order to build a complete solution, often resulting in multiple layers of complexity to deploy. However, Symantec Network Access Control does not require the existence of any of these industry framework technologies to provide end-to-end effective and comprehensive network access control. Still, Symantec Network Access Control will support, enhance, and seamlessly operate alongside these industry frameworks, allowing enterprises to deploy the technologies that they feel best fits their needs.

Symantec policy management: Comprehensive, integrated endpoint security management

As organizations have had to deal with growing user populations that include onsite employees, remote employees, short-term employees, guests, contractors, and other temporary workers, they have become increasingly susceptible to a vast array of threats trying to enter the network. Security concerns include viruses, spyware, zero-day attacks, and unknown exploits, all of which try to find their way onto the business network through openings created by endpoint devices that are not compliant with established corporate security policies.

Symantec believes that true endpoint security requires the seamless coupling of endpoint protection technologies with endpoint compliance technologies. Symantec enables organizations to take a more holistic approach to endpoint security to address this threat through its tight integration of Symantec Endpoint Protection (endpoint protection) and Symantec Network Access Control (endpoint compliance). These offerings seamlessly interoperate to provide a comprehensive and unified multilayered endpoint protection solution that enables IT administrators to successfully strike the balance between network access, end-user productivity, and security, while simplifying endpoint security administration.

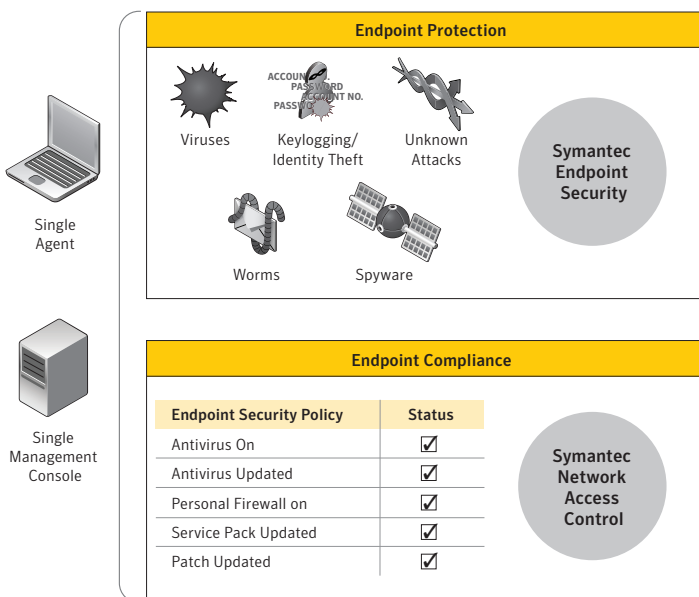


Figure 8. Endpoint Security = the seamless combination of Endpoint Protection and Endpoint Compliance

Symantec Network Access Control: Comprehensive Network Access Control

Single management console

Key to this holistic management approach is the ability provided by the Symantec Endpoint Protection Manager to centrally create, deploy, manage, and report on all endpoint security activities. From a single management console, administrators can set policies that control all aspects of the integrated Symantec Network Access Control components, such as the Symantec evaluation technologies and Symantec Enforcers in addition to the Symantec Endpoint Protection policies. The policy manager's enterprise-class centralized management architecture can scale to meet the most demanding environments, provide granular control to all administrative tasks, while simplifying and unifying all endpoint security management efforts to reduce total cost of ownership.

Unified agent

For organizations that have already deployed the Symantec Endpoint Protection product, the network access control persistent agent functionality is already present on the agent. In other words, it is not necessary to deploy an additional agent to implement network access control. The network access control capability integrated into the Symantec Endpoint Protection agent can be easily enabled through the purchase of a license. The consolidation of all these security capabilities into a single agent reduces complexity and system resources and requires no change to the client when adding network access control. Additionally this single, unified agent is managed via the Symantec Endpoint Protection Manager.

Eliminating network access control obstacles

Symantec helps eliminate the obstacles to leveraging the benefits of network access control by delivering a comprehensive and integrated endpoint security solution that:

- Delivers effective policy compliance enforcement and remediation
- Reduces the number of security management agents that must be installed to a single agent
- Simplifies IT complexity while eliminating disruptions to the business and IT infrastructure
- Provides the flexibility to address organizations' unique network access control implementation needs, including appropriately accommodating guest and temporary workers
- Seamlessly integrates with an organization's overall endpoint security management infrastructure

Symantec Network Access Control: Comprehensive Network Access Control

To further help organizations leverage the benefits of Symantec Network Access Control, Symantec provides a range of consulting, technical education, and support services to guide them through its deployment and management, enabling businesses to realize the full value of their investment.

Symantec Enterprise Support Services have three levels of protection designed to meet the needs of the small business as well as the large enterprise. Symantec Education has a portfolio of training courses designed to get users up to speed quickly. Symantec Consulting Service provides assistance with solution design, deployment planning, installation package creation, and testing through either its Residency Services, where Symantec Consultants work side-by-side with customers' IT staff, or Operational Services, where the entire endpoint security function can be outsourced to Symantec—the security experts.

End-to-end endpoint compliance

In today's highly sophisticated and dangerous threat landscape, IT administrators must protect themselves not only from organized attacks against their specific company, but also from targeted attacks that leverage desktops and laptops as backdoor entryways into those enterprises' business operations and valuable resources. To maintain the integrity of the corporate IT infrastructure and its endpoints, organizations can no longer allow unchecked access to the network. With the significant increase in the numbers and types of endpoints accessing the network, organizations must be able 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 is an end-to-end solution that securely controls access to corporate networks, enforces endpoint security policy, and easily integrates 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 automated remediation capabilities, and continually monitors endpoints for changes in compliance status. The result is a network environment where corporations realize significant reductions in security incidents, increased levels of compliance to corporate IT security policy, and confidence that endpoint security mechanisms are properly enabled.

Symantec Network Access Control: Comprehensive Network Access Control

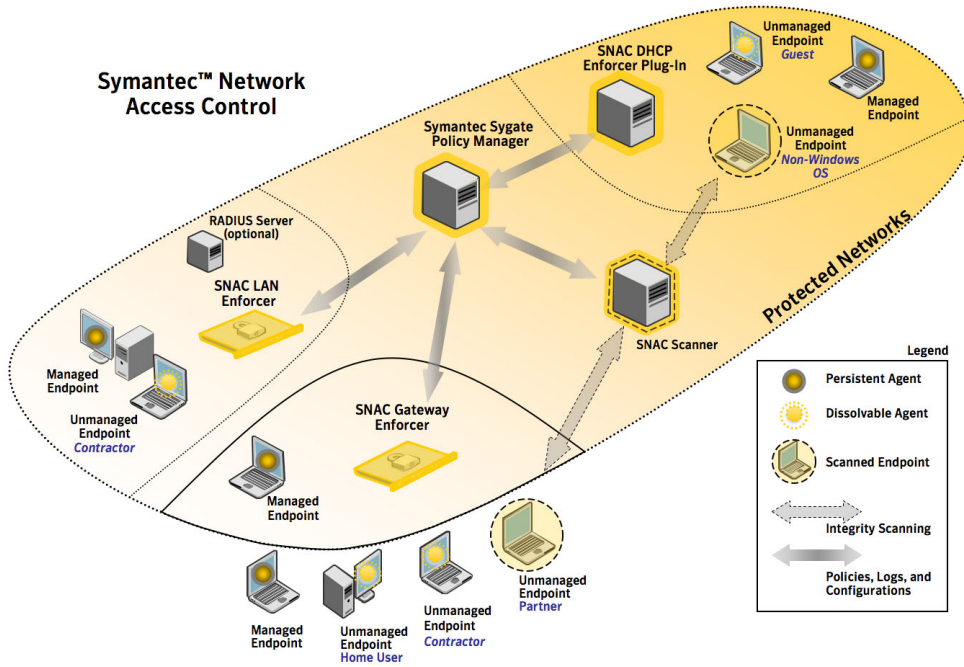


Figure 9. Symantec Network Access Control architecture

With its array of multiple agent assessment technologies and multiple enforcement options, along with being OS- and network vendor-neutral, Symantec Network Access Control is the most flexible and interoperable network access control solution on the market. This high level of flexibility and interoperability also allows organizations to easily and quickly deploy the combination of network access control assessment and enforcement options the way they need to and when they need to. To further aid in deployment, as well as to help speed the return on an organization's investment, Symantec also provides a range of consulting, technical education, and support services.

Symantec is a global leader in infrastructure software, as well as endpoint security, enabling businesses and consumers to have confidence in a connected world. Symantec helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. Java is a trademark or registered trademark of Sun Microsystems, Inc., in the U.S. or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
05/07 12516470