Organizations depend on their networks to be reliable and available at all times in order to communicate with customers and partners, execute business transactions, and provide customer support. To provide these services on an ongoing basis, they must enable people to access the network from a variety of entry points such as VPNs, intranets, and extranets using a growing number of endpoints, including laptops, desktops, and mobile devices. And in our 24x7 business environment, network downtime can cost millions of dollars in lost revenue and productivity. That’s why it is essential for organizations to protect their network assets and mission-critical applications from hackers, worms, viruses, and more—a task that becomes ever more difficult in today’s always-on, always-connected business environment.

---

**Cisco Network Admission Control**

**Now Powered by Symantec Security Technologies**

1. Non-compliant endpoint attempts connection
2. Connection allowed
3. Infection spreads; endpoints exposed
Maximum network security: It starts at the endpoint.

To address challenges created by the growing variety of endpoints and to maximize the overall network security, infrastructure device manufacturers and security providers are developing interoperable solutions that enforce security policy compliance at every point of entry to the network. If an endpoint attempts to connect to a network and does not comply with the security policy, it will be denied access. One such solution is Network Admission Control (NAC), a collaboration between Symantec and Cisco Systems®, and based on Symantec’s leading endpoint security technologies: Symantec Client Security and Symantec AntiVirus Corporate Edition.

Combining Symantec’s industry-leading security technologies and Cisco® infrastructure expertise delivers a comprehensive solution that fortifies security policy enforcement and allows administrators to permit, deny, quarantine or fix non-compliant devices before granting network access.

The solution allows the network administrator to set policies on what to do if a non-compliant endpoint attempts to access the network. Actions may be based on the degree of non-compliance, location, etc.

**Step A** Non-compliant desktop is denied access to the network.

**Step B** Non-compliant desktop is allowed access to the network but issue is logged.

**Step C** Non-compliant desktop is redirected to servers in order to download software or content updates to regain compliance. Once remediated, this system can be granted access to the network.
How the Symantec and Cisco NAC works.

The integrated solution is comprised of five essential components:


2. **Communications Agent.** Symantec endpoint security solutions interact with the Cisco Trust Agent, a software tool that collects security state information and communicates it to the network access device.

3. **Network Access Device.** Every device seeking access to the network contacts a router, switch, VPN concentrator, firewall, or other such access device. These devices request security credentials through Symantec endpoint security solutions and relay the information to policy servers.

4. **Policy Server.** The Cisco Secure Access Control Server evaluates endpoint security credentials and determines the appropriate policy: permit, deny, quarantine or restrict access.

Maximum business benefits: Interoperability.

The Symantec and Cisco collaboration allows organizations to proactively minimize network downtime and protect network availability and integrity from external and internal threats. By enabling interoperable security policy enforcement and access management at network endpoints, NAC gives organizations the power to:

- Reduce IT costs and total cost of ownership
- Maintain the productivity of IT personnel, enabling them to focus on higher-value initiatives
- Minimize risk by helping to ensure that all systems, plus its proven ability to meet the challenge of blended threats by using coordinated security technologies, make Symantec ideally suited for collaborating on NAC.

Protection from the worldwide leader in information security.

As the leader in information security, Symantec has an exceptionally strong track record of integrating leading-edge security software technologies. The company’s expertise in identifying known and unknown threats and vulnerabilities in endpoint systems, plus its proven ability to meet the challenge of blended threats by using coordinated security technologies, make Symantec ideally suited for collaborating on NAC.

An integrated solution from the biggest names in the business.

Unlike standalone security products, the integrated NAC solution provides completely integrated and ubiquitous admission control coverage, along with central management options that increase flexibility without compromising protection. As industry leaders, Symantec and Cisco are working to help mutual customers proactively mitigate risks by identifying, preventing, and adapting to new and emerging security threats.

For more information about the Symantec and Cisco NAC, visit www.cisco.com/go/nac.