



Network Access Control

Trend Micro Inc. 

 Simple enforcement now

A Trend Micro White Paper | October 2006



CONTENT

- I. THE THREATS INSIDE THE CORPORATE NETWORK..... 3
- II. THREE MAJOR CONCERNS FOR IT MANAGERS: COMPLIANCE, COMPLIANCE, COMPLIANCE.....3
- III. NETWORK ACCESS CONTROL: A NEW WEAPON IN THE SECURITY ARSENAL..... 4
- IV. CHALLENGES IN MOVING TO NAC..... 4
- V. FIVE KEY FACTORS IN CHOOSING THE RIGHT NAC SOLUTION.....5
- VI. TREND MICRO™ NETWORK VIRUSWALL™ ENFORCER.....7
- VII. WHY NETWORK VIRUSWALL ENFORCER?..... 8
- VIII. TREND MICRO™ ENTERPRISE PROTECTION STRATEGY..... 9
- IX. THE BOTTOM LINE: NAC NOW.....10

I. THE THREATS INSIDE THE CORPORATE NETWORK

It's ironic. Today's enterprises have been busy building security infrastructures to keep out an ever-increasing number of external threats, and with a great deal of success. But unfortunately, they have been blind-sided by threats that penetrate the network from the other direction—internal threats that arise from inside the corporation itself.

Security-savvy enterprises have devised elaborate and effective defenses to secure their perimeters, effectively intercepting virtually all of the “front door” threats. However, more and more often, companies that thought that they were well-protected are being penetrated by threats from so-called “friendly” devices inside the perimeter—an employee laptop, a computer used by a remote worker via a virtual private network (VPN) or a contractor temporarily working in the building and connecting directly to the corporate network. The proliferation of mobile devices, together with the need to extend network access to increasing numbers of suppliers, partners and customers, is bypassing and therefore undermining traditional perimeter-based defenses.

At the same time, attacks are becoming more dangerous to the enterprise. The motive of the hacker has shifted from disrupting enterprise operations to stealing assets that can be used for illicit financial gain, including customer credit card numbers, intellectual property and bank account information. There have even been instances in which an attacker penetrated the defenses, encrypted the enterprise's operational information—then blackmailed the company to pay for the decryption key to unlock the information so that operations could resume. With this as a goal, attackers are increasingly focusing their attacks by singling out individual companies. The more successful and high-profile the company, the more likely that it will be a target.

II. THREE MAJOR CONCERNS FOR IT MANAGERS: COMPLIANCE, COMPLIANCE, COMPLIANCE

In its 2006 survey of IT managers, the U.S. Federal Bureau of Investigation (FBI) found that regulatory compliance ranks as the second most critical issue facing IT managers over the next two years, behind only data protection.¹ Regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX) and, more recently, the PCI Data Security Standard, continue to dominate planning discussions in executive suites. And those executives are looking to IT managers to provide solutions.

Why IT? Because compliance is all about showing regulatory institutions that your enterprise is controlling access to information. Since the IT department owns the corporate information, it is the group that has the operational ability and responsibility for compliance. IT managers must factor compliance considerations into every modification or enhancement they make to the enterprise IT infrastructure, no matter how small or straightforward the change appears to be.

¹ 2006 CSI/FBI Computer Crime and Security Survey, by Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, published by Computer Security Institute.

III. NETWORK ACCESS CONTROL: A NEW WEAPON IN THE SECURITY ARSENAL

In light of these trends, many IT managers are looking to boost their security strategies with protection from the threats posed by mobile and remote workers, and to better comply with the growing number of regulations. Gaining greater control over any device that connects to the network with a reliable access control solution such as network access control (NAC) significantly boosts compliance efforts.

NAC secures the network from infected devices by screening them at the time they attempt to connect to the network. It enforces corporate security policies across the entire network, including LANs, wireless and VPN nodes. More than just a security tool, a comprehensive NAC implementation provides a mechanism to help IT administrators manage their networks more effectively, upgrading the enterprise's compliance profile and improving corporate governance. NAC addresses the root cause of internal security threats: noncompliant users.

IV. CHALLENGES IN MOVING TO NAC

As with any emerging technology, implementing NAC has its challenges and involves risk and uncertainty.

For starters, the marketplace is crowded, with product offerings from smaller, niche players as well as major security vendors such as Trend Micro. Infrastructure companies, for example Cisco² and Microsoft³, also see NAC as an area where they can add value—and gain market share in the security arena. With a variety of choices and little practical experience, IT managers may not know where to turn for a proven solution.

Some NAC solutions require substantial changes to the network architecture, driving up adoption costs significantly, lengthening the timeline and causing operational disruptions. Already busy network and security administrators may balk at the additional workload of installing, configuring and maintaining an NAC solution. With the universal mandate to minimize IT operational costs, any enterprise considering NAC must carefully evaluate—and seek to minimize—the administrative burden that its deployment represents.

"Enterprise customers are eager to deploy comprehensive NAC solutions," said Chris Christiansen, vice president at IDC, "Simple, easy-to-deploy NAC appliances already meet the most immediate IT requirement of securing the network against mobile and guest users."

² Cisco defines NAC as Network Admission Control.

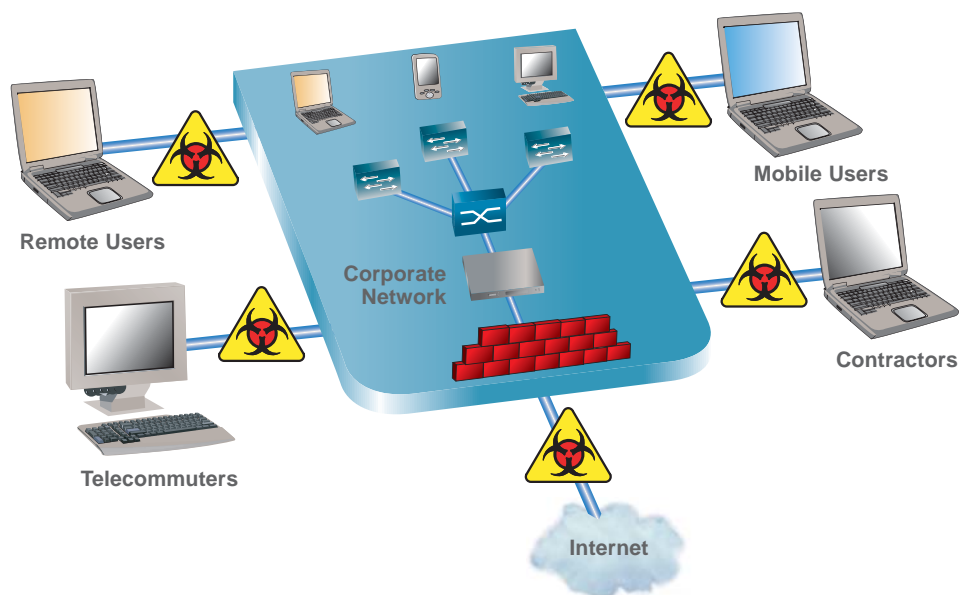
³ Microsoft refers to its solution in this space as Network Access Protection, a policy enforcement platform built into the Microsoft Windows Vista and Windows Server (Longhorn) operating systems.

V. FIVE KEY FACTORS IN CHOOSING THE RIGHT NAC SOLUTION

IT managers evaluating NAC solutions should consider these five factors in making their decisions.

➔ Agent-based versus agent-less solutions

Many solutions require that endpoint devices such as laptops have a preinstalled software agent before they can be screened for network access. With the growing number and diversity of mobile devices, this requirement is often impractical and needlessly restrictive, because it requires IT staff intervention to install and update agent-based software on every device that accesses or has the potential to access the network whether the user is an employee, contractor, visitor—or intruder.



What companies need is an agent-less solution that does not require preinstalled software agents, automates the entire NAC flow, and enforces policies on all devices, regardless of who is attempting network access. Unlike agent-based solutions, agent-less solutions can assess the health of all devices attempting to connect to the network, including those of guests, contractors, partners, vendors and customers. They ensure consistent policy enforcement across-the-board for all devices, at the time of connection, without the hassle associated with installing, maintaining, and updating software agents.

NETWORK ACCESS CONTROL

➔ Comprehensive policy enforcement

A good NAC solution should be able to enforce a range of policies, including keeping antivirus signatures up-to-date, maintaining the latest patches of operating systems, scanning for malware, and system registries. Any device that does not comply must be quickly and effectively blocked from accessing the network until it is compliant or cleaned up.

➔ Flexible quarantine and automatic remediation

When devices are noncompliant with security policies, they must be quarantined. However, every network is unique, so the NAC solution must be flexible enough to enforce a quarantine that fits into a range of network architectures. To minimize lost user productivity and IT burden, the NAC solution should complement the quarantine with powerful automatic remediation capabilities.

➔ Ease of management—plug and protect

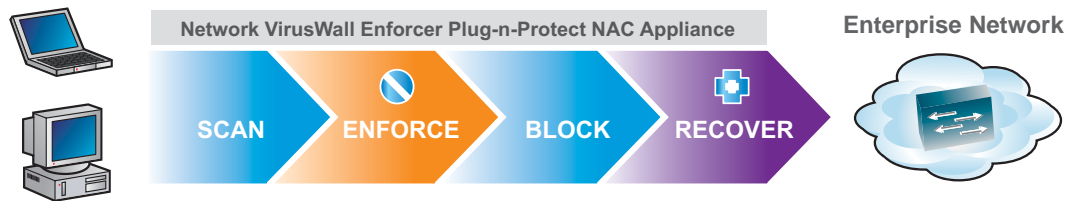
The NAC solution should require little or no configuration prior to deployment; that is, it should be plug-and-protect. At the same time, it must allow for easy policy updates. The NAC solution should include the ability to be centrally managed and integrate with the enterprise's existing security management console.

➔ Migration path

With the rapid pace of the developing NAC market, IT administrators must consider future-proofing. They need the flexibility to deploy a solution today, then safeguard that protection as they migrate to other solutions as they become available.

VI. TREND MICRO™ NETWORK VIRUSWALL™ ENFORCER BEATS THE INSIDER THREAT

Trend Micro has tracked the development of the NAC market and listened carefully to the needs of its users as described in the previous section. Its response is Trend Micro Network VirusWall Enforcer, a simple, integrated, second-generation NAC appliance designed to offer immediate network access control to protect the network against the fastest growing source of infection—the mobile and remote workforce.



Trend Micro Network VirusWall Enforcer:

- Scans devices when they attempt to connect to the network
- Enforces corporate security policies
- Quarantines devices if they do not comply with corporate policies
- Performs automatic agent-less remediation on quarantined devices

VII. WHY NETWORK VIRUSWALL ENFORCER?

Here's why many security and IT administrators consider Network VirusWall Enforcer the top NAC choice available today:

➔ **Network VirusWall Enforcer reduces risk**

Network VirusWall Enforcer builds on the success of Trend Micro Network VirusWall, a mature and proven product with thousands of satisfied users. By turning to a second-generation product, enterprises benefit from the experience of others, and reduce the risks usually associated with deploying a new technology.

➔ **Network VirusWall Enforcer ensures consistent policy enforcement**

Because it uses an agent-less approach, Network VirusWall Enforcer can enforce policies effectively for any device attempting to connect to the network. By removing the requirement of a preinstalled agent, enterprises can provide access to partners, consultants, suppliers and others who might otherwise be excluded.

➔ **Network VirusWall Enforcer minimizes drain on IT resources**

Remediation can consume a significant amount of IT time per machine. Thanks to the automatic remediation features of Network VirusWall Enforcer, IT staff doesn't have to get involved, freeing time for more strategic activities.

➔ **Network VirusWall Enforcer can be centrally managed in any environment**

Network VirusWall Enforcer includes a built-in Web console for managing simple deployments. For more complex environments, Network VirusWall can be managed using Trend Micro Control Manager™, a centralized management console that simplifies enterprise-wide security coordination, administration, and management.

➔ **Network VirusWall Enforcer is easy to deploy**

The appliance's inline design requires no network re-architecting and can be deployed as a turnkey installation. Network VirusWall Enforcer is a complete NAC solution, requiring no additional hardware or software.

➔ **Network VirusWall Enforcer protects network performance.**

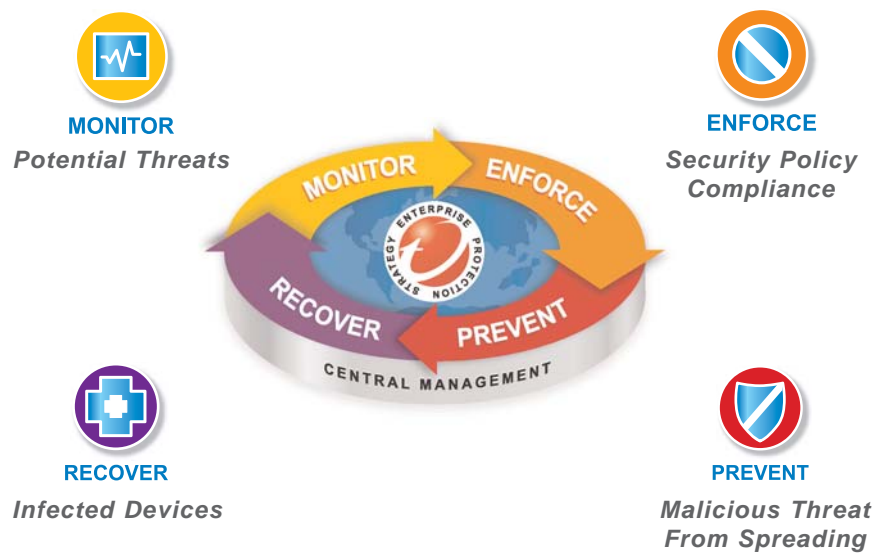
Network VirusWall Enforcer includes zero-minute protection against bots and worms that can infect the network during the scanning phase. It isolates infected network segments for cleanup to minimize damage, stop the spread of malware, and avoid network outages.

➔ **Network VirusWall Enforcer includes a migration path to Cisco NAC**

To help enterprises better adapt to future needs, Trend Micro has designed Network VirusWall Enforcer as part of a comprehensive NAC strategy. Enterprises can deploy Network VirusWall Enforcer today to address immediate needs, then migrate to a more comprehensive solution in the future. For investment protection, Trend Micro also plans to offer a software upgrade for out-of-band operation. By enabling a mixed inline/out-of-band solution, Trend Micro allows enterprises to customize their NAC deployments.

VIII. TREND MICRO™ ENTERPRISE PROTECTION STRATEGY

Network VirusWall Enforcer is part of the Trend Micro Enterprise Protection Strategy (EPS). This comprehensive security framework provides a unique approach to threat management for the porous enterprise infrastructure. Enterprise Protection Strategy combines multiple layers of products and services for comprehensive, intelligent protection against known and unknown threats. Tightly integrated and centrally managed security enables seamless collaboration among individual products that helps reduce overall threat exposure while reducing administration costs.



IX. THE BOTTOM LINE: NAC NOW

It's no longer sufficient to protect the enterprise network at the perimeter or to count on IT to outfit every laptop and remote PC with the latest security software and patches. As an additional—and vital—component of the enterprise security infrastructure, NAC addresses the root cause of many threats: unprotected user devices connecting to the network.

The Trend Micro NAC solution, Network VirusWall Enforcer is built on a proven security framework, offering enterprises the following advantages:

- Reduced risk
- Consistent policy enforcement
- Minimal drain on IT resources
- Centralized management
- Easy deployment
- Optional migration path to Cisco NAC

For more information on Network VirusWall Enforcer and Trend Micro Enterprise Protection Strategy, please visit <http://EndpointSecurity.trendmicro.com>.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com

