



Network Access Management: Stopping Intruders and Worms Before They Get on the Network

A Vernier Networks White Paper



Vernier Networks, Inc.
490 East Middlefield Road
Mountain View, California 94043

www.verniernetworks.com

The Security Shortcomings of Static Network Infrastructures

The onslaught of security attacks on enterprise networks seems unrelenting. In 2004, 78% of organizations surveyed by the Computer Security Institute (CSI) and the FBI detected virus attacks on their networks, and 39% detected penetrations of IT systems. Systematic control over network access remains elusive: 53% of organizations reported discovering that their computer systems were being used in unauthorized ways, and 37% detected users gaining unauthorized access to information.¹ A study by the Yankee Group found similar problems with network access and data security. Data theft is on the rise (reported by 13% of enterprises in 2003 and 15% in 2004), and the number of enterprises reporting problems with data disclosure nearly doubled (rising from 8% in 2003 to 14% in 2004).²

These numbers highlight some glaring shortcomings in the design, security, and management of today's enterprise networks.

First, **reactive security measures and lax management of end user devices are no match for the new forms of malware that are sweeping the Internet.** Worms and viruses now traverse the globe within minutes. When the Slammer worm struck in January, 2003, it doubled in size every 8.5 seconds and had reached 90% of vulnerable hosts worldwide—an estimated 75,000 machines—within 10 minutes. Fast-moving attacks like Slammer leave network administrators no time to set up traditional defenses, such as updating signature files in firewalls and running AV program updates. The rapid transmission of new attacks, as well as the laggardly updating of defense software, helps explain why even though 99% of enterprises report using anti-virus (AV) software, 78% of them are still suffering from virus and worm attacks. To assure business continuity in the face of such attacks, the network must be protected and partitioned ahead of time, so the scope of attacks is minimized and remediation can be accelerated. Once installed, AV software must be continually evaluated and updated.

¹ 2004 CSI/FBI Computer Crime and Security Survey.

² Yankee Group Research Note, September 8, 2004, http://www.yankeegroup.com/public/products/research_note.jsp?ID=11932.

Second, **the rapid transmission of malware combined with the busy everyday work of large, mobile user populations means that the security state of a network is always in flux.** A LAN that is secure at 9:00 AM might be in serious trouble by 9:03 AM after a sales representative, whose laptop became surreptitiously infected at an airport hot spot, logs in. A contractor might log in from the lobby at 10:00 AM, a conference room at 11:00 AM, and a software architect's office at 2:00 PM. Depending on the data assets and network resources at risk, it may be appropriate for the network to enforce different security policies at each of these locations and times. But few enterprises today have security controls that recognize the changes taking place on the network, such as the changing locations and security levels of users and the changing combination of applications that are in use. Static security controls, such as firewall ACLs and VLANs, are not granular enough and proactive enough to respond to threats that may suddenly appear and require immediate action, such as the quarantining of devices.

Third, **network security involves guarding data and controlling its access, not just scanning for malware attacks.** Even if enterprises have made progress installing AV software on nearly every user's PC, the data theft and data access statistics cited in the CSI/FBI and Yankee Group studies are powerful reminders that network security is about more than recognizing virus signatures. Access to information assets must be tightly controlled, particularly in industries such as financial services and health care, where industry regulators can impose fines and criminal penalties and where the well-being of an organization's customers is at stake.

Finally, **the cost of these security attacks is simply too high.** Worm and virus attacks cost businesses \$55 billion in 2003³, and this figure doesn't include costs from network security problems such as data theft, laptop theft, financial fraud, and fines resulting from violations of industry regulations such as HIPAA.

The current security model of deploying a rigid network for trusted users at fixed locations and then patching the network when attacks occur just isn't responsive enough or comprehensive enough for today's enterprise networks.

Recognizing the Problem with Static Network Infrastructures

The frequency, virulence, and variety of security attacks are forcing enterprises to re-evaluate their network infrastructures. Static network configurations, such as firewall ACLs and VLAN configurations, are proving inadequate in the face of viruses and worms that can sweep across a network in seconds and transform trusted machines into suspect, and possibly hostile, devices.

³ Trend Micro, cited in http://www.techtips101.com/TechTips/2004TechTips/TT_0403/TT040304-04.htm.

Administrators need to make the network infrastructure itself responsive when an attack occurs. As appropriate, they need to be able to enforce “guilty until proven innocent” security policies to screen large numbers of devices. To protect the network—as well as the mission-critical business operations that depend on the network—enterprises need to make security measures more precise, capable of responding to a threat from a specific device at a specific time, as well as more dynamic.

In most enterprises, and at sites such as universities and hospitals, the sheer number of devices to be screened and cleaned demands an automated solution. IT departments lack the budgets to add staff for manually inspecting and cleaning devices. Deploying a system that automatically determines the security status of a device and guides end users through the remediation of threats is the only practical solution for keeping networks active and end users productive once an attack occurs.

But today’s infrastructures were designed for static configurations and lack the dynamic, moment-by-moment policy controls that effective network security demands.

Moving to a Dynamic Security Infrastructure

How can enterprises create a dynamic security infrastructure? By complementing their existing infrastructure with new capabilities for:

- **Screening users and devices**, so that before users are granted access to the network, their credentials are verified and their devices are scanned for infections and compliance with configuration requirements and security policies; suspect or infected devices should be quarantined rather than granted access to the network
- **Restricting users to their authorized resources**, so that the scope of malware attacks is minimized and the risks of data theft and data disclosure are greatly reduced
- **Inspecting traffic continually for threats and potential policy violations**, recognizing that traffic generated from devices and the actions of users change continually and therefore require continual scrutiny
- **Enforcing security policies automatically**, so that threats are contained, remediation is prompt, and business continuity is optimized.

A dynamic infrastructure that performed these functions would greatly accelerate the detection and remediation of attacks. Such a dynamic infrastructure would make large networks and large user communities manageable for IT and security teams because basic screening and corrective action would be handled through automated procedures, rather than manual tasks.

Obviously, no enterprise today can afford the expense and the risk of wholly replacing its network infrastructure with a new infrastructure of dynamic switches, routers, and servers. Instead, these functions must be added to existing infrastructures in a manageable and affordable way.

How do enterprises go about transforming their networks to become dynamic and more secure?

Industry Initiatives for Network Access Management

Several industry initiatives are under way for creating a solution for screening devices and building a system for enforcing granular security policies. The three most significant initiatives in this area of network access management (NAM) are:

- Cisco's Network Admission Control (NAC) initiative
- Microsoft's Network Access Protection (NAP) architecture
- The Trusted Computing Group's Trusted Network Connect (TNC)

Cisco's NAC Initiative

Cisco's Network Admission Control initiative is Cisco's effort to develop an access management solution that would prevent non-compliant devices from gaining access to the network. The NAC solution calls for two software programs, the Cisco Security Agent and the Cisco Trust Agent, to be installed on each end user device. The Cisco Trust Agent would collect information about the state of the device, including its operating system level and AV signature status. Whenever the device attempts to access the enterprise network, the Trust Agent would pass this information to a policy server, such as a Cisco Secure Access Control Server, which would evaluate the state of the device and determine the appropriate access policy to apply. Compliant devices would be granted access to the network. Non-compliant devices could be granted restricted access or denied access altogether. The NAC initiative builds on the capabilities of Cisco's network infrastructure products in order to provide a level of access control missing from most enterprise networks.

Microsoft's NAP Initiative

Microsoft's Network Access Protection (NAP) platform is a proposed set of security compliance components designed to work with the upcoming "Longhorn" release of the Microsoft Windows Server. NAP enables administrators to screen end user devices for compliance with security policies and to isolate non-compliant devices on a more secure network segment, which Microsoft calls a restricted network. The NAP platform includes an API that developers and administrators can use for integrating NAP into their network infrastructure, creating custom solutions for managing network access, isolating non-compliant devices, and enforcing security policies. NAP itself does not include components for verifying or correcting the state of end user devices. Rather, Microsoft envisions NAP working with system health agents (SHA) and system health validators (SHV) that will be included in future versions of the Microsoft System Management Server (SMS).

Microsoft clearly states that the scope of NAP is limited to the screening of devices when they first connect a network. If a user with valid authentication credentials and a policy-compliant device connects to the network and later uploads viruses or other malware or in some other way jeopardizes the network's health, NAP will be unable to detect or thwart the attack. By combining NAP's screening services with a clientless network access management that monitors and protects the network after users log in, enterprises can significantly improve the security of their networks.

The Trusted Computing Group's TNC Initiative

The Trusted Computing Group (TCG) is an industry alliance that includes prominent networking and security technology vendors such as Juniper Networks, Network Associates, Symantec, and Trend Micro. This group originally came together to develop Trusted Computing Modules, special-purpose integrated circuits that would be installed on PC motherboards and provide tamper-proof authentication and state information about end user devices involved in business transactions. The widespread use of such motherboards is still years away.

While this work is under way, the TCG launched a second, parallel effort called Trusted Computing Network Connect (TNC). The purpose of TNC is to define an open software architecture that network administrators could use to enforce security policies for endpoint host connections across multi-vendor networks. Like Microsoft's NAP solution, the TNC architecture would enable administrators to ensure that any endpoint that connects to the network is properly screened for compliance with security policies. Devices with non-compliant security features and operating system levels could be quarantined or denied access altogether.

The TCG is still developing the specification for TNC. Broad implementation of the specification is likely to be years away.

The Quandary Facing Enterprises Today

As promising as these initiatives seem, they all have their limitations.

Cisco's NAC solution requires client devices to be running a Cisco software agent, which increases the cost and complexity of deployment. NAC is designed to work with Cisco switches and will likely be difficult to implement on networks with equipment from other vendors.

The Microsoft initiative is tied to Microsoft's "Longhorn" release, currently scheduled for 2006. The initial release will be limited to servers running "Longhorn" and client devices running Windows XP. NAP requires the use of another Microsoft product, the Microsoft SMS, and is not designed to monitor the health of end user devices or the network after users connect.

Finally, the TNC initiative remains a work in progress. The team developing the TNC specification is still deciding which authentication protocols to support. Even once the specification is drafted and ratified, widespread industry adoption will take time.

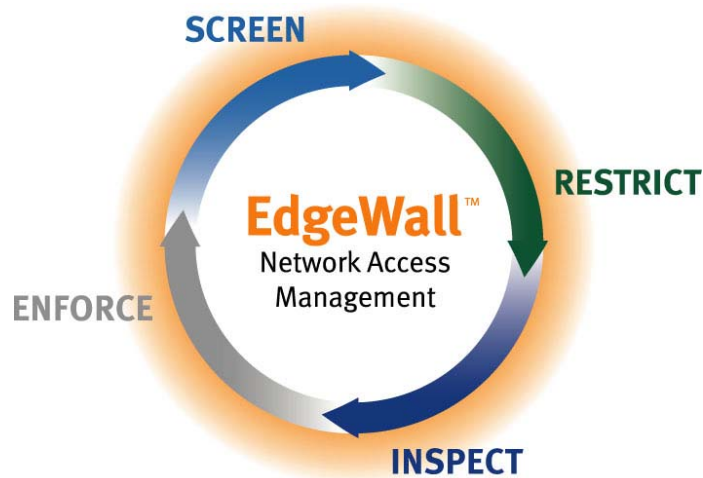
Real-world implementations of these initiatives are still years away. How can enterprises create dynamic network infrastructures and effective access management controls today?

A clientless, network-based solution for network access management (NAM) would overcome some of the limitations of these initiatives. Clientless security does not require IT departments to configure those devices with a particular vendor's client software ahead of time nor to limit policy enforcement only to those devices that the IT department can configure. A comprehensive NAM solution would work with any device attempting to access the network, and it would continually inspect devices for policy violations, regardless of how long they have been logged in. Such a solution could incorporate features and APIs from the initiatives such as Microsoft NAP when those initiatives become ready for widespread commercial use. In the meantime, the solution would provide protection against worms, viruses, and illicit data access—protection that enterprises desperately need today.

The Vernier EdgeWall Network Access Management Appliance

Vernier Networks, a network security solution provider, has created a solution for dynamically enforcing security policies and access management controls on enterprise networks.

The Vernier EdgeWall Network Access Management (NAM) appliance is a real-world solution for Network Access Management that enterprises can deploy today to make their network infrastructures more dynamic and secure. As its name implies, the EdgeWall appliance sits at the edge of the network, serving as a secure boundary and control point between end users and the network. Based on open standards, the EdgeWall appliance integrates with the network infrastructures and authentication systems enterprises already have in place. The EdgeWall solution complements these infrastructures with NAM features that enforce network security policies on every device at every moment, providing continuous, comprehensive security for enterprise networks.



The Vernier EdgeWall NAM solution performs four key access management functions for enterprise networks:

- **Screening:** The Vernier EdgeWall appliance screens users to assure that they are authenticated and devices to assure that they are clean of viruses and worms. Through the EdgeWall appliance's automated screening process, an enterprise can ensure that only users whose computers are in compliance with security policies can gain access to the network. The EdgeWall authentication service integrates with whatever combination of authentication systems an enterprise has already deployed.

- **Restricting:** The Vernier EdgeWall appliance restricts each user's network access to only those resources that the user is authorized to use. Guest users can be granted access to public resources, such as the Internet, but not internal resources, such as databases and business applications. Network administrators can restrict each city employee's access to those resources appropriate for the employee's job.
- **Inspecting:** The Vernier EdgeWall appliance continuously inspects traffic from client devices to defend against viruses and worms and unauthorized sessions. The system recognizes attack patterns and blocks attacks from spreading to the rest of the network. Infected nodes are immediately identified, quarantined, and blocked from attacking the network or infecting others. The Vernier EdgeWall appliance takes protective action automatically and requires minimal policy changes or human intervention.
- **Enforcing:** The Vernier EdgeWall appliance enforces security policies to assure user and device compliance. Using the Vernier EdgeWall solution, an IT team can define access policies that meet the needs of various user groups while minimizing the risk of intrusion. For example, the Vernier solution can be configured to prevent laptops from communicating directly with a network router, eliminating the risk of these devices launching a Denial of Service (DoS) attack on the router. The Vernier appliance's fine-grained policy controls enable an IT department to automatically enforce user- and location-specific security policies, such as requiring users at remote locations to log in through a VPN or users in conference rooms to re-authenticate every hour.

The EdgeWall solution offers important benefits for securing and managing enterprise networks:

- The EdgeWall appliance works with all standards-based devices, including PCs, Macintoshes, and PDAs. Administrators can be sure that any device attempting to access the network is screened for compliance and carefully monitored.
- The EdgeWall appliance requires no special software or hardware to be installed on end user devices, reducing the cost of deployment and eliminating the need for administrators to spend long hours on installation and configuration work. The Vernier solution builds security into the network itself.
- The EdgeWall appliance integrates transparently with the switching fabric so that security never compromises network performance.
- The EdgeWall appliance is highly scalable. The EdgeWall solution was designed to accommodate all sizes of networks, from department LANs to multi-campus enterprise networks. IT departments can install EdgeWall appliances in wiring closets and in data centers to provide comprehensive security across campuses. A central Vernier Control Server coordinates policies across all the appliances and enables the appliances to detect security threats such as duplicate MAC addresses.

- The EdgeWall appliance works with both wired and wireless networks and in local and remote offices, providing enterprises with a single solution that fits all their networking needs.
- The EdgeWall appliance is available today. Unlike industry initiatives such as NAC and TNC, Vernier's EdgeWall solution is already installed at Fortune 500 companies and leading hospitals and universities. As new technologies such as NAP and TNC become available, EdgeWall will integrate with them, providing enterprises with best-of-breed security solutions.

With security threats like viruses and worms continuing to pummel networks, and with data theft and illicit data access on the rise, the Vernier EdgeWall solution provides a powerful NAM solution that enterprises can begin taking advantage of immediately.

Conclusion: Securing Business Continuity

Before the rise of the Internet, mobile computing, and the extended enterprise, organizations could secure their networks with static security controls at the perimeter. Once configured, end user devices rarely moved or came into contact with malware. Illicit data access, without the aid of an intranet, was difficult—an undertaking possible only for the most determined and technically proficient malicious user. In this controlled environment, a network that was secure at 9:00 AM on Monday morning would almost certainly be secure at 5:00 PM on Friday night.

Recent innovations in business models and in technology have done away with this tranquil, orderly world of static security. Now all aspects of a business run on the network. Business transactions traverse public and private networks in the blink of an eye. Users are mobile; they routinely carry their computers outside the protected confines of the office. Intranets and outsourcing are making illicit data access easier and more common. Security attacks are increasingly devious, dangerous, and frequent. The static security measures erected a decade ago are caving in under an onslaught of viruses and worms. Perimeter defenses cannot protect businesses whose supply chains and partner networks demand continuous connectivity.

To counter these challenges, IT organizations must transform the network infrastructure itself. Building on their investments in firewalls and routers, IT organizations must introduce new granular and dynamic security controls that respond instantly to threats arising from devices, users, and network connections. Network Access Management (NAM) solutions promise to provide the fine-grained, dynamic security enterprises need in order to achieve this transformation.

The Vernier EdgeWall appliance is a NAM solution that businesses can deploy today to secure their networks and to protect their business operations. By screening users and devices, restricting data access, continuously inspecting traffic, and enforcing security policies around the clock, the Vernier EdgeWall solution secures the networks and the business continuity of today's extended—and vulnerable—enterprise.

About Vernier Networks, Inc.

Vernier's EdgeWall is a network access management (NAM) appliance that is deployed at the network edge and provides comprehensive NAM to defend against intrusions and attacks on the network by screening users and devices, restricting access, inspecting traffic for worms and viruses, and enforcing access policy. Complementary to firewalls, which are deployed at the perimeter of the network to protect the corporate network from intrusions from the Internet, EdgeWall NAM appliances are deployed at the network edge to protect the network from intrusions from endpoints without disrupting network performance.

Vernier Networks products are distributed directly and by a network of strategic OEMs and Value Added Resellers and deployed by over 300 customers, worldwide. The company is headquartered in Mountain View, CA and has sales offices in Europe and Japan.

For more information, visit the Vernier Networks Web site at: www.verniernetworks.com or contact a Vernier representative at info@verniernetworks.com