THE TOLLY GROUP

No. 207252 October 2007

Mirage Networks®, Inc.

Mirage Endpoint Control™ NAC Solution

Evaluation of Network Access Control for Real-World Endpoints and Applications

Test Summary

Premise: Network Access Control (NAC) has become a foundational security element in organizations across industries. NAC solutions should be more than "just another security layer" — but should provide tools to ensure policy compliance and behavioral control over not just the managed network assets, but also the "unmanaged, unknown, or rogue" endpoints and applications attempting to access the network.

Mirage networks, Inc. commissioned The Tolly Group to validate the chief capabilities of the company's Endpoint Control network access control (NAC) solution.

Tolly Group engineers examined the Mirage Endpoint Control NAC solution (consisting of the Endpoint Control 145 Advanced Compliance Server, the Endpoint Control 245 sensor appliance and the Mirage Operations Console (MOC) management applications) for its ability to detect and restrict network access of both managed and rogue devices and applications that fail to comply with IT security and behavioral policies.

Engineers tested high-risk applications like Peer-to-Peer (P2P) file-sharing services, Instant Messaging (IM) services, unknown or rogue devices like mobile communication devices, game consoles, personal routers and servers, that have the potential to introduce risk inside an organization's trusted network.

Tests were conducted in September 2007.

Test Highlights

- Protects customer networks from infected, out of policy, and unknown endpoints
- Detects, tracks and/or stops unauthorized applications such as instant messaging and peer-to-peer file sharing
- Requires registration of unknown/rogue devices such as gaming consoles, personal routers, and servers before granting network access
- Protects wireless networks from unauthorized mobile units such as iPhones and Windows Mobile devices

Features/Functions of Mirage Endpoint Control Validated by The Tolly Group

Compliance and Monitoring	Requires authentication and host posture check for Windows, Linux and Macintosh devices, restricting access when devices are not compliant	✓
	Monitors behavior of all devices on the network, restricting access when policies are broken	✓
P2P File Sharing Control	Detects and alerts on P2P packets	✓
	Stops flow of P2P traffic	✓
	Revokes network access to offending endstations	✓
Instant Messaging Checks	Detects IM traffic from AOL, GoogleTalk and MSN Messenger	✓
	Stops flow of IM traffic	✓
	Blocks network access of offending endpoint	✓
Rogue Device Registration	Detects unregistered gaming consoles such as Xbox and PlayStation	✓
	Allows devices to register for network access	✓
WLAN Access Control	Detects and blocks unauthorized Apple iPhones and Windows Mobile devices from accessing wireless LANs	✓

Source: The Tolly Group, September 2007

Figure 1

Executive Summary

Mirage Networks' Endpoint Control appliance proved that it offers the ability to allow authorized network access while policing network applications such as P2P and IM, rogue devices such as gaming consoles, personal routers and other devices exhibiting threatening or high-risk behavior, sending alerts and/or restricting network access when appropriate.

The agentless NAC solution from Mirage Networks was designed to provide network access control for real-world applications.

A Tolly Group evaluation shows that Mirage provides security that granularly controls or revokes network access of devices and applications that are unknown, out of policy, threat-infected, or are in violation of acceptable network access behavior for such a device or application.

The Tolly Group validated that the Mirage solution effectively deals with high-risk applications such as P2P and IM, and can identify and isolate rogue devices such as gaming consoles which may seem like nuisance devices, but have operating systems that can be infected, propagate threats and consume bandwidth.

Engineers also validated the ability to isolate mobile communication devices like Apple iPhones and Windows Mobile devices from joining wireless networks where they have been linked to broadcast storms with Cisco Wireless LAN controllers, causing a denial of service.

Mirage Networks Endpoint Control
Network Access Control Feature Evaluation

Endpoint Configuration Compliance Enforcement

Operating Sytem	OS patch detection	Anti-virus detection	Anti-spyware detection	Personal firewall detection
Windows XP Pro SP2	✓	✓	✓	✓
Windows Vista Ultimate	✓	✓	✓	✓
Macintosh OS X 10.4.5	✓	✓	✓	✓
Ubuntu 6.06	N/A	✓	N/A	✓

This list does not represent all operating systems supported by Mirage. This list was chosen as a representative sample of common endpoint operating systems.

Behavioral Policy Enforcement

Threat Category	Alerts (E-mail, SNMP, Syslog)	Block threat only	Block endpoint
Network scans	✓	✓	✓
Port scans	✓	✓	✓
Mass mailers	✓	✓	✓
Unauthorized Web servers	✓	✓	✓
Unauthorized FTP servers	✓	✓	✓
Unauthorized SMTP Servers	✓	✓	✓
Unauthorized gateways	✓	✓	✓
Instant messaging threats	✓	✓	✓
Contact dark IP addresses	✓	✓	✓
Unauthorized IP telephony	✓	✓	✓
Protocol violations	✓	✓	✓

This list does not represent every threat detected by Mirage. This list was chosen as a representative sample of common threat behaviors.

Unauthorized Application Control

Application	Alerts (E-mail, SNMP, Syslog)	Block application only	Block endpoint
BitTorrent 5.0	✓	✓	✓
Limewire 4.14	✓	✓	✓
Azureus 3.0	✓	✓	✓
Kazaa 3.2	✓	✓	✓
Xnap 2.5	✓	✓	✓
BitComet 0.93	✓	✓	✓
Yahoo! Instant Messenger 8.1	✓	✓	✓
MSN Instant Messenger 6.2	✓	✓	✓
AOL Instant Messenger 6.1	✓	✓	✓
Trillian 3.1	✓	✓	✓

This list does not represent every application detected by Mirage. This list was chosen as a representative sample of common, high-risk applications.

Rogue Device Control

Device	Alerts (E-mail, SNMP, Syslog)	Require authentication/registration	Block endpoint
Sony PlayStation 3	✓	✓	✓
Microsoft XBOX	✓	✓	✓
Linksys Wireless Router (WRT54GS v.5)	✓	✓	✓
HP iPAQ rx1950 (Windows Mobile 5.1.1702)	✓	✓	✓
Apple iPhone	✓	✓	✓

This list does not represent every device detected by Mirage. This list was chosen as a representative sample of common, high-risk devices.

Source: The Tolly Group, September 2007

Figure 2

Results & Analysis

Endpoint Authorization and Compliance

Tests demonstrated Endpoint Control's ability to restrict access to unknown endpoints until they meet policy compliance requirements with respect to the configuration of the endpoint. Tests show that the Mirage solution restricted access of endpoints running a variety of popular operating systems like Windows

XP, Windows Vista, Ubuntu Linux and Macintosh OS X, until each client demonstrated compliance with a configurable security policy by entering authentication credentials and completing a system scan that validates the presence of anti-virus and anti-spyware applications and personal firewalls.

When configured to do so, Mirage’s NAC solution also generated alerts via E-mail, SNMP or Syslog, while partially or completely limiting the network access of non-compliant endpoints. See Figure 2.

Behavioral Policy Enforcement

Mirage’s Endpoint Control also enforced behavioral policies for endpoints and applications accessing the network.

Behavioral policies were set in the Mirage Operations Console (MOC) to detect and protect against threatening and risky behavior like network scans, port scanning, unauthorized web/FTP/SMTP servers, mass mailers, unauthorized routers and more. These risky behaviors were launched from a laptop running Windows XP Professional SP2. See Figure 2.

Upon detection of policy violation, the Mirage solution was configured to generate an alert using Email, SNMP, Syslog etc. When configured to do so, the Endpoint Control solution partially or completely limited the network access of the non-compliant endpoint.

Unauthorized Application Control

Tests examined how the Mirage solution handles unauthorized application traffic on the network.

The MOC was configured with policies to detect and take appropriate action against unauthorized application traffic like those from P2P file-sharing and Instant Messaging (IM) applications.

Examples of P2P applications tested include BitTorrent, Azureus, Kazaa, LimeWire, Xnap and BitComet, and the IM applications tested include Yahoo Messenger, AOL Instant Messenger, MSN Messenger, and Trillian. These applications were launched from a laptop running Microsoft Windows XP Professional SP2.

Upon launch of traffic from these applications, engineers observed that the policy violation was logged in the MOC, and an SNMP, Syslog or E-mail alert was sent to chosen recipients.

When configured to do so, upon detection, the Mirage solution partially, or completely, limited the network access of the non-compliant endpoint.

Under the limited access scenario, only designated “in-policy” was allowed instead of blocking the endpoint entirely.

Rogue Device Detection and Restriction

Engineers validated that the Mirage NAC solution detected rogue or unregistered devices like Microsoft Xbox and Sony PlayStation 3 gaming consoles, personal wireless routers and servers, and blocked their network access until the devices were registered either through a Web browser login page (when supporting the device) or directly by an administrator.

Mirage Networks

Endpoint Control NAC Solution

Feature Validation of Network Access Control Capabilities

TOLLY Up to Spec CERTIFIED

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

Mirage Networks
Endpoint Control NAC Solution

Benefits:

- Meet compliance requirements
- Stop zero-day threats on your network
- Clean up one infected device instead of hundreds
- Know every device that connects to your network
- Know every user that connects to your network
- Stop or just contain rogue applications and devices
- Regain control of your network bandwidth

Features:

- The only patented NAC solution
- Agentless
- Out of band
- Infrastructure independent
- Works for all network-connected devices
- Surgical device restriction
- No infrastructure integration
- Policy tied to device, user or behavior
- Supports Active Directory, eDirectory, RADIUS, LDAP authentication
- Supports over 300 anti-virus applications out-of-box
- Supports over 100 anti-spyware applications out-of-box
- Supports over 100 personal firewall applications out-of-box

For more information, contact:

Mirage Networks, Inc.
6801 N. Capital of Texas Hwy.
Building 2, Suite 200, Austin, TX 78731
Phone: 866.869.6767
URL: http:www.miragenetworks.com

Mobile Device Detection and Restriction

iPhone & Windows Mobile Device Detection

The Tolly Group validated that the Mirage NAC solution detected mobile communication devices like Apple iPhones and Windows Mobile powered PDAs and/or Smartphones connecting to the wireless network and blocked network access entirely, or until the devices was authenticated.

Test Bed Setup

The Mirage Endpoint Control solution was deployed in Mirage Networks' Microsoft Windows based enterprise network in the company's Austin, TX premises. The network consisted of the usual Windows Server-based Active Directory, DHCP, SMTP servers, and numerous enterprise-class core-, aggregation- and workgroup-class switches and routers from vendors such as Cisco and Extreme Networks.

The switching/routing and server infrastructure in Mirage's network are representative of a typical medium to large enterprise network, but is too varied to mention in this document.

The Mirage Networks Endpoint Control solution version 3.1 consisted of the Endpoint Control N-145 Advanced Compliance Server appliance that performed deep inspection of endpoints to check for OS patches, anti-virus/anti-spyware software, and host firewall. The Endpoint Control N-245 sensor appliance that detects new endpoints connecting to the network and enforces compliance policies set in the MOC application.

The Windows XP and Windows Vista Ultimate endpoints were run as virtual machines using VMWare Workstation version 5.5.2 running on a server running Windows Server 2003 SP2. Endpoints running Ubuntu Linux 6.06 and Macintosh OS X 10.4.5 were using dedicated hardware.

The Mirage Endpoint Control N-145 Advanced Compliance Server appliance and the Endpoint Control N-245 sensor appliance connected to a Cisco Catalyst 4500 switch. The MOC was running on a PC with Windows XP Professional SP2.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at:
Web: http://www.tolly.com,
E-mail: sales@tolly.com

All the server and client computer endpoints, game consoles, and wireless routers connected to the Cisco switch through intermediate switches and hubs. Mobile endpoints like the Apple iPhone and the HP iPaq rx1950 Pocket PC connected to a Linksys WRT54GS wireless router which was in turn connected to the Cisco switch.

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.