

Mirage Networks®
CounterPoint™
Defending the Network Interior™



Stop threats and enforce security policies
with Network Access Control from Mirage Networks:
the award-winning CounterPoint appliance.



Mirage Networks® CounterPoint™

Defending the Network Interior

Effective Network Defense

Revokes access of endpoints:

- violating policy
- propagating threats
- scouting the network

Simple Network Defense

IT-friendly technology:

- vendor-neutral
- no agents, no signatures
- virtually in-line

No False Positives.

"Gartner clients that have deployed Mirage's product report simple installation and effective security... without false actions during normal activity."

*—Gartner Cool Vendors
in Security, 2005*

The network interior has become the new battleground for faster, smarter and more destructive worms, viruses and hackers.

These electronic criminals are leveraging mobile endpoints—laptops, PDAs and the like—that enterprises rely on to do business, to bypass traditional security and take down networks, destroying intellectual property, reputations, and bottom lines.

And as the number of enterprise endpoints increases, the challenge grows exponentially.

The Solution: Mirage Networks CounterPoint

Mirage Network Access Control (NAC) technology extends the reach of traditional security solutions, providing a new level of control over threats that bypass existing security barriers. CounterPoint combines network-based behavioral detection and threat containment technologies in an out-of-band appliance, to stop interior network attacks on day zero without interrupting business-critical traffic while:

- generating low false positives
- delivering fast time to value
- requiring no agent software or in-line appliances

While other interior network security solutions rely heavily on signatures, agents or in-line deployment, CounterPoint's low-TCO technology avoids these pitfalls and their associated support and performance costs.

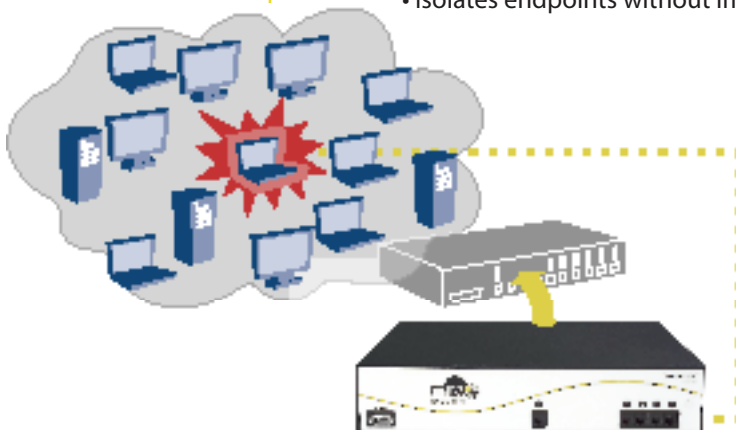
CounterPoint delivers behavioral threat detection without false positives. The appliance actively identifies, engages and mitigates threats through a simple connection to a switch port. This out-of-band deployment provides a solution that installs and configures quickly without impacting network traffic.

CounterPoint monitors the network for threats

- Behaviorally detects threats coming from endpoints
- Identifies violations of security policy

CounterPoint contains network threats proactively

- Automatically or manually revokes access for an offending endpoint
- Isolates endpoints without impact to other users



By plugging into the SPAN or R/W port of an access layer switch, CounterPoint monitors all network traffic and mitigates threats without impacting normal business.

The “LCD Factor”

CounterPoint was built by seasoned technologists who determined there had to be a better way to secure the network interior. They studied the primary types of network interior attacks to determine what they have in common—the Lowest Common Denominators—in terms of method of delivery, propagation, and so on. This led to the development of 5 core rule categories:

- Reconnaissance
- Threat Propagation
- Rogue Packets
- Spoofing
- Mass Mailer

This approach supplants the need for signatures—and that’s a good thing: signature-based solutions are not effective against day-zero threats, and are easily circumvented by encrypted threats.

A Critical Weapon in the Network Security Arsenal

CounterPoint’s value is at the network interior—where the majority of threats originate—to strengthen a network’s total approach to security:

Patch and policy management

- A required best practice, this methodology should be in use in every organization
- CounterPoint complements this by providing time for rational process and effective response
- *It is critical to protect the network interior before patching is possible*

Network-based Intrusion Prevention Software (IPS)

- In-line detection and mitigation causes network latency and additional points of failure
- In-line high availability requirements can double deployment costs
- *IPS can miss VLAN traffic, and cannot control access at endpoint granularity*

Host-based Intrusion Prevention Software

- Intended for predictable environments (servers), not dynamic (PCs and mobile endpoints)
- Locks down users’ machines to protect them from the network
- *A single misconfigured or unmanaged host can defeat an agent-based approach*

Conclusion:

An effective, low-TCO interior network security solution is key to managing enterprise security.

Security without headaches

- *No signatures to maintain*
- *No agents to deploy & manage*
- *No source of latency*
- *No single point of network failure*
- *No network rearchitecture*
- *No unreliable heuristics learning*

Did you know?

⚠ *Companies let patches age an average of 52 days to discover secondary impacts.*

⚠ *Slammer made it around the Internet in 15 minutes.*

Sources: Yankee Group, Gartner

It’s a fact.

Gartner recently found that best-of-breed organizations have control of only about 80% of the endpoints on their networks.

CounterPoint is a cost-effective way of securing the network—even from unmanaged endpoints.

2004 in Numbers

90+%: percentage of enterprises using antivirus, firewall and email filtering software

80%: percentage of enterprises experiencing 1+ successful attacks

\$204,000,000,000: global cost of network attacks

115,000,000: number of machines affected globally by malware

17 hours: average time it took to bring servers up after an attack

24 days: the average productivity time required to handle post-attack cleanup

Sources: mi2g Intelligence Unit, Malware Damage in 2004; IDC, Enterprise Security Survey, 2004; ICSA Labs, 9th Annual Computer Virus Prevalence Survey



Mirage Networks® CounterPoint™

Defending the Network Interior

“Worm writers want their noxious work to spread fast; CounterPoint detects and thwarts this devilish desire. Stars out of 4:

–Software Development Magazine Product Review, May 2005

The ROI of CounterPoint was evident immediately. Within 30 minutes of installation, Round Rock ISD found unwanted reconnaissance –that their industry-leading intrusion detection system missed –and were able to shut the intruder out.

–Jim Brigham, CTO, Kairos InfoSec Systems, a Mirage partner

We value our relationship with Mirage Networks because their product and strategy complement our offerings and ensure our customers receive the high quality and functionality they have come to expect from working with us. TheChannelFirst partner program continues to set Mirage Networks apart from the field, as it represents their dedication to our success and to our customers. It's a win-win.

–Media Landry, Vice President of Sales, igxglobal

With Mirage Networks, we are able to provide a revolutionary solution to protect important corporate assets from attacks that have continued to evade existing technologies such as firewalls, intrusion detection and intrusion prevention systems.

–Kazuhiro Nomura, President & CEO, Mitsui Bussan Secure Directions

With a global operation spanning 41 countries, network security is of utmost importance. Mirage fit our needs perfectly by giving us an agentless, hardware-agnostic and behavior-based appliance that stops RPTs on day zero.

–Brett Childress, Director of IT infrastructure, National Instruments”



Mirage Networks
6801 North Capital of Texas Hwy.
Building 2, Suite 200
Austin, Texas 78731
www.miragenetworks.com
866.869.6767

©2005 Mirage Networks, Inc. All rights reserved.

