



You Can't Control People.
Control What's On Your Network.™



Endpoint Control from Mirage Networks®





How It Works.

Get zero-day threat and policy violation detection and containment

- » Stop threats spawned in the interior that perimeter solutions can't detect
- » Run vulnerability scans based on profile or rule violation
- » Ensure quarantining without cross-contamination of endpoints

Enjoy easy management and deployment

- » Ensure security without agents or signatures, even with unknown devices
- » Reduce network downtime, IT burden and help desk costs
- » Secure the network without re-architecture or new points of failure

Ensure user satisfaction and productivity

- » Speed return to productivity with self-remediation
- » Avoid disruption of legitimate traffic by revoking network access surgically
- » Ensure minimal false positives

Meet corporate and business objectives

- » Leverage incumbent IT infrastructure
- » Protect without user latency or white listing
- » Ensure fast ROI with immediate effectiveness

Leverage patented technology to thwart threats

- » Mitigate threats without external switches, routers or other security products
- » Contain threats without cumbersome router, firewall or switch reconfigurations
- » Deploy without disruption or user performance degradation

DETECTS THREATS

The core of Mirage Endpoint Control™ is a behavioral rule set: six categories of rules which detect behavior that is either out of policy or indicative of an attack. Examples include default rules to detect network scanning behavior, mass mailing exploits, protocol violations and the presence of unauthorized services. In these and other instances, a Mirage Endpoint Control rule identifies the behavior as suspicious, and follows through with quarantining and remediation activity according to your security policy.

Mirage Endpoint Control behavioral rules work out of the box to continually evaluate the behavior of every endpoint, with virtually no false positives, so no signatures or agents are required to catch even zero-day attacks. And because it's working all the time, it catches threats that propagate from within the network interior, protecting enterprises and users against the data and identity theft that is typical of today's malware.

DETECTS POLICY VIOLATIONS

Mirage Endpoint Control appliances come with built-in policy checks that determine the following characteristics about any device entering or on the network:

- » registered or unregistered device status
- » operating system
- » services running
- » threat and policy compliance history
- » VLAN entered

This enables IT to easily triage at-risk devices by defining critical risk characteristics according to security policy and user type, and to take user-appropriate action. For deeper endpoint checks, Mirage offers authentication, vulnerability scanning, antivirus management, and patch management. By way of its API, Mirage Endpoint Control can integrate into existing NAC frameworks, acting as either a Policy Decision Point or a Policy Enforcement Point.

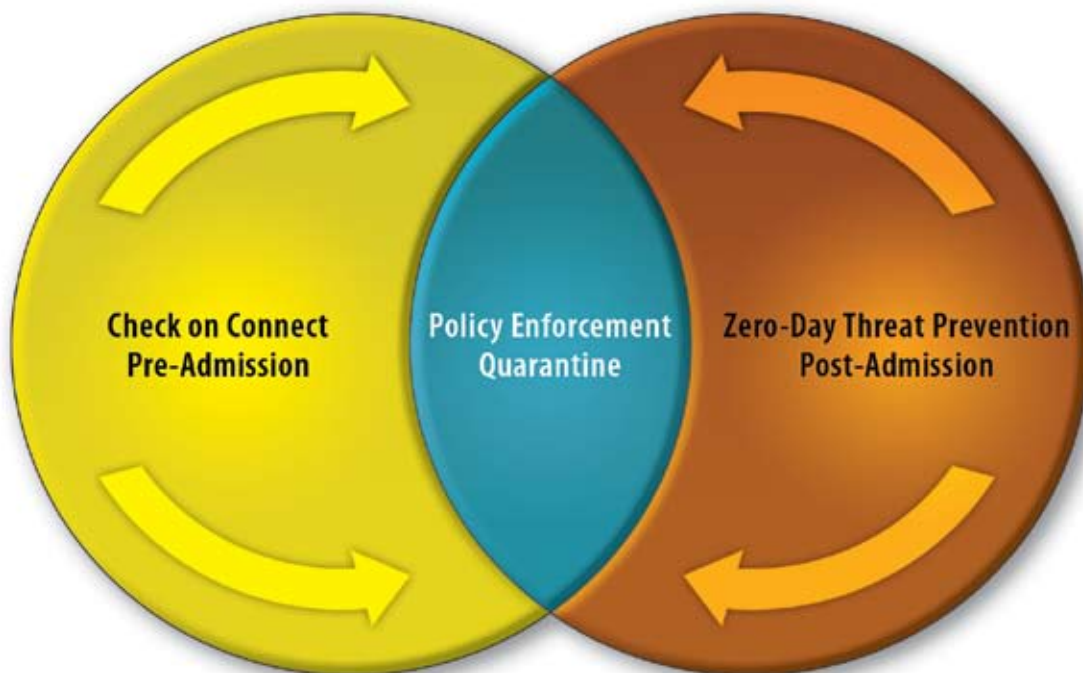
Unlike other solutions, Mirage delivers Real-World Endpoint Control

- » No endpoint agents
- » Out-of-band deployment
- » Zero-day behavioral detection



The Right Solution.

Mirage Agentless Endpoint Control secures the network against today's biggest threats with three core capabilities



PRE-ADMISSION SECURITY: CHECK ON CONNECT

Mirage Endpoint Control discovers devices immediately upon network entry, providing a real-time map of your IP space, and beginning the monitoring and compliance checking cycle. Upon discovery of an entering device, Mirage Endpoint Control determines if the device is registered in the system, its operating system, service ports and connection method. To verify the identity of users, Mirage Endpoint Control authenticates users by checking common credential stores, such as LDAP, RADIUS, and Active Directory.

If your security policy deems that any or all of these factors are indicative of an at-risk or simply unknown device, Mirage Endpoint Control can quarantine the device, enabling a customized remediation path that includes deeper scans, additional authentication, updates of anti-virus and OS patch levels and malware removal. Unlike many products in the space, the remediation path presented by Mirage Endpoint Control can be customized according to the detected violation.

POST-ADMISSION SECURITY: THREAT PREVENTION

Mirage Endpoint Control's award-winning behavioral design leads the industry in effective post-admission threat detection. Combining authoring flexibility with a highly effective set of out-of-box defaults, Mirage Endpoint Control monitors behavior and device characteristics throughout the endpoint's life cycle on your network. Just as with violations detected at admission time, threat and policy violations can trigger an automated quarantine and present the endpoint user with a remediation path customized to the detected violation.

POLICY ENFORCEMENT: QUARANTINE AND REMEDIATION

Mirage Endpoint Control delivers powerful quarantine and remediation options. Quarantines initiated by Mirage Endpoint Control are holistic and complete, eliminating the risk of cross infection and network downtime. User notification and remediation options are presented via a captive web portal and completely customizable to meet organizational needs and minimize help desk calls.

Meets Your Needs.

INFRASTRUCTURE-INDEPENDENT MITIGATION

Mirage Endpoint Control delivers targeted and highly flexible quarantining of offending endpoints, and enables user-appropriate mitigation options. To ensure the most flexible, customer-friendly approach, Mirage Endpoint Control's quarantining capabilities can be customized with remediation options based on user type, profile and other characteristics. For example, the CEO may be permitted network entry with an out-of-policy PC, while in the background, Mirage Endpoint Control scans the device and sends an alert to IT to provide in-person diagnosis and remediation. On the other hand, a contractor who requests access to the network with an unknown device may be directed to a quarantine server which enables policy diagnosis and self-remediation with AV patches, OS updates and the like. This not only allocates IT resources in line with business objectives, it allows organizations to leverage their investments in tested security technology.

These options include allowing:

- » No network access until remediation is complete
- » Limited network access, such as Internet access only, until remediation is complete
- » Redirection to a Web server for user-appropriate remediation

MANAGEMENT CAPABILITIES

Mirage Endpoint Control offers one-to-many management, enabling change management for software patches and policies across all Mirage appliances in an enterprise. It also delivers persistent data storage across multiple devices, enabling analysis that reflects your network's history and usage. For example, you can now pinpoint the percent of infections from mobile devices, or quantify resources spent specifically on bringing contractors' machines in-line with your security policies. This gives you the ability to take precise and accurate action, both preventative and reactive.

sensor options for networks of all sizes



N-120

50
endpoints

N-125

100
endpoints

N-145

1,000
endpoints

N-245

2,500
endpoints

The Mirage solution scales to any network size and complements your existing security technologies. Mirage appliances deploy off a Layer 2 network switch, leveraging in-place IT and infrastructure investments, without introducing a point of network failure.

advanced compliance server



N-145

syncs with existing credential stores to authorize and policy scan endpoints before granting access to the network

centralized management & monitoring

M-2060



enterprise deployments

N-245

small scale
deployments

Mirage Product Suite
your complete
Endpoint Control
solution

the biggest threat to network security:

your users

The Problem: The continuing trend of outsourcing, contracting and business partnerships has resulted in a revolving door of non-managed computing devices accessing your network. This trend combines with technology shifts such as the prevalence of embedded IP devices (phones, copiers, cameras, vending machines, etc.) to change the rules of the network security game. IT security pros charged with keeping networks accessible and secure are struggling to ensure some level of compliance for computing assets that are not managed by them, as well as find a way to protect embedded OS devices that tend to be “unmanageable.”

In yesterday’s reality, perimeter security provided all the protection your network needed. Today’s reality mandates that you extend that perimeter to all of your network connection points, from wired to wireless to VPN.

The Solution: Agentless endpoint control from Mirage Networks® is the only solution developed for the real world, to help you control what gets on your network – and what is allowed to stay. Mirage Endpoint Control™ provides security that controls or revokes network access to devices that are unknown, out of policy, or threat-infected.

In a perfect world, your network would be homogeneous in terms of vendor and OS, and re-architecting your network would be fast, easy and cost-effective. In this perfect world, every device that comes on your network would be managed easily, and user updates to the access control agent or signature file would be practical and effective. This is clearly not the case.

That’s why Mirage Networks designed its technology to cover all IP devices – from desktops and laptops to PDAs, IP telephony, IP fax machines, and more – while being:

- » effective against zero-day threats and policy violations
- » integrated with other security technologies
- » independent of both network infrastructure and device OS
- » easy to deploy and manage
- » IT- and user-friendly
- » scalable for both voice and data networks
- » agentless: no signature file ever needs to be updated



control who gets on your network
with Endpoint Control from Mirage Networks

"Mirage gives us the ability to protect our business against attacks that cause downtime, keeping our IT staff productive and focused on business-enabling technologies."

- Chuck Stanton, SVP of IT,
Paul Financial

"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 and Privacy, 2005

"Mirage Networks' solution fits our needs perfectly by giving us an agentless, hardware agnostic and behavior-based appliance that stops rapidly propagating threats on day-zero."

- Brett Childress, Director of IT Infrastructure,
National Instruments

"Mirage gives us the ability to both watch network traffic and take action when an offending device is identified."

- Kathy Kimball, Director of
Computer & Network Security,
Penn State University

TNS

built by professionals

TelExcell Networking Solutions Pvt. Ltd.
F-2/9, Okhla ,Phase-1, New Delhi-110020
INDIA

Tel : +91 11 30851100 ; Fax: +91 11 30851104

Email: info@tnspl.in www.tnspl.in