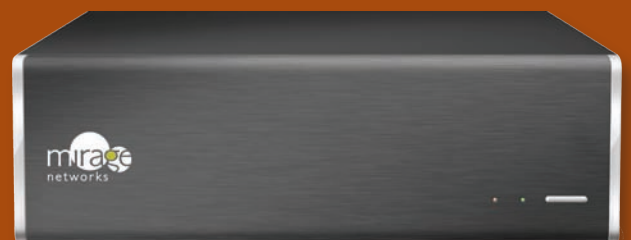




**You Can't Control People.**  
**Control What's On Your Network.™**

**Network Access Control from Mirage Networks**



the biggest threat to network security:

# your users

**The Problem:** Technology shifts like the explosion of mobile devices and the growing prevalence of IP telephony in the enterprise have changed the rules of the network security game. These productivity enhancers seem to conspire to thwart IT security pros charged with keeping networks both accessible and secure, and users make the difficult seem impossible. The greatest risks come from users who connect unmanaged, out-of-policy, or simply threat-infected devices to the network, completely bypassing existing perimeter security measures.

In yesterday's reality, perimeter security provided all the protection your network needed. You, unfortunately, have to operate in today's reality.

**The Solution:** Full-cycle Network Access Control (NAC) 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 NAC provides security that controls or revokes network access to devices that are unmanaged, out of policy, or threat-infected.

Judging by their so-called NAC standards, it would seem that some NAC providers believe that your network is homogeneous in terms of vendor and OS; that rearchitecting your network is fast, easy and cost-effective; that you manage each and every device that comes on your network; that requiring users to learn how to work with – or, more often than not, around – their solution is practical and effective.

This is clearly not the case. That's why Mirage Networks designed its NAC technology to cover all IP devices – from desktops and laptops to PDAs, IP Telephony, IP fax machines, and more – while being:

- » effective against day-zero threats and policy violations
- » flexibly integratable with other security technologies
- » network infrastructure- and OS-independent
- » easy to deploy and manage
- » IT- and user-friendly
- » scalable for both voice and data networks



**control who gets on your network**  
with NAC from Mirage Networks



# How It Works.

## Get day-zero 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 unmanaged devices
- » Reduce network downtime, IT burden and help desk costs
- » Secure the network without rearchitecture 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 whitelisting
- » Ensure fast ROI with immediate effectiveness

## Leverage patent-pending 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 NAC™ is a behavioral rule set: six categories of rules which detect behavior that is indicative of an attack. For example, a Windows® device probably has no need to access your IP telephony network. Alternately, your security policies may prohibit the use of instant messaging applications. And there are few legitimate reasons for a device to attempt contact with multiple unused IPs – so-called “dark IPs” – on your network. In these and other instances, a Mirage NAC rule identifies the behavior as suspicious, and follows through with quarantining and remediation activity according to your security policy.

Mirage NAC 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 day-zero attacks. And because it's working all the time, it catches threats that propagate from within the network interior, where the majority of threats originate.

## DETECTS POLICY VIOLATIONS

Mirage NAC 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

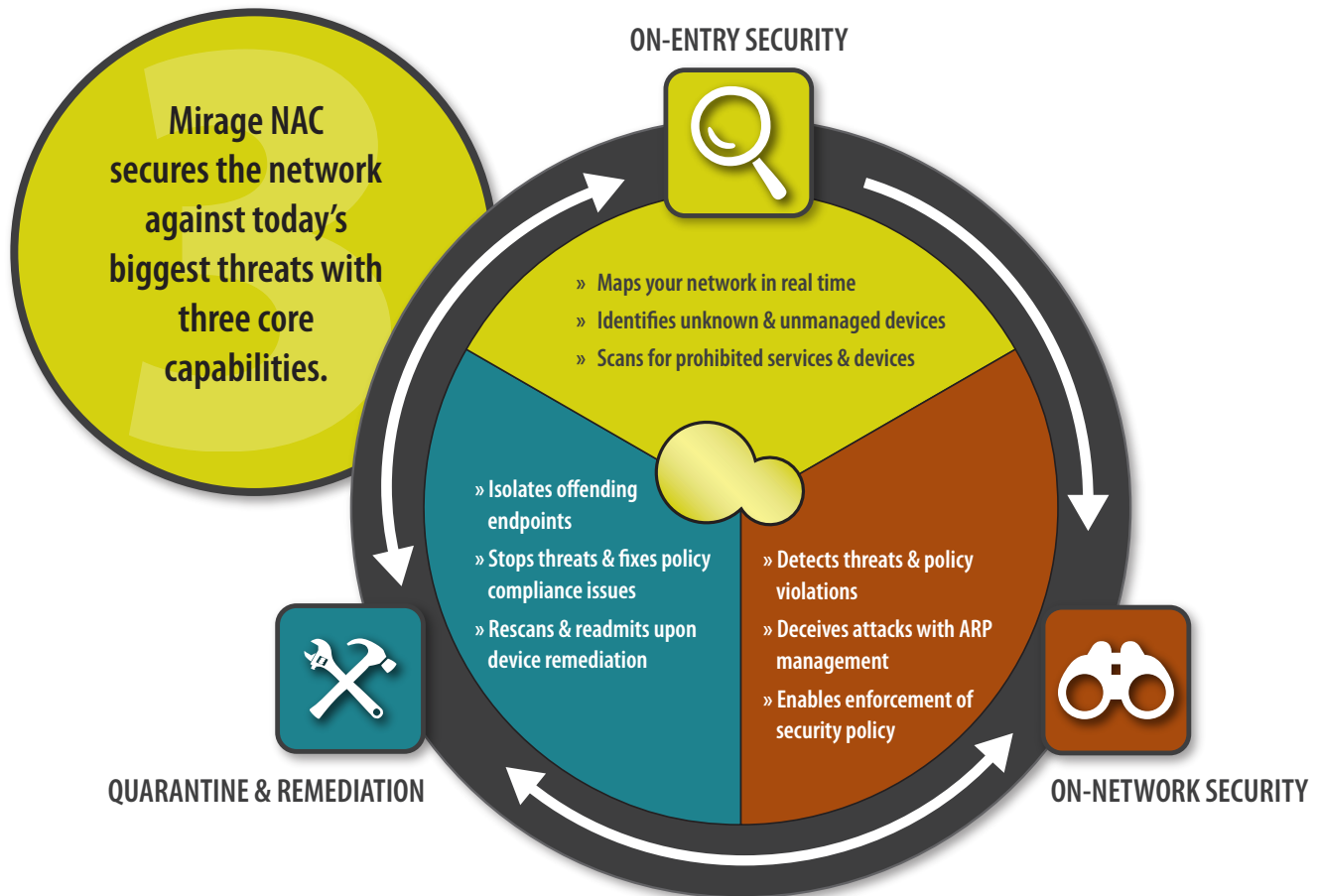
This enables IT to easily triage at-risk devices by defining critical risk characteristics according to security policy and user type, and to take user-appropriate action. For deeper endpoint checks, Mirage offers integrations with the technology of leading security vendors, including authentication, vulnerability scanning, antivirus management, policy management and enforcement, patch management and security information management. By way of the Mirage API, Mirage NAC can either trigger a third-party security action, or take direction from the third-party solution to serve as the point of policy enforcement.

## Unlike other solutions, Mirage Delivers Full-Cycle NAC

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



# The Right Solution.



## ON-ENTRY NAC: RISK ASSESSMENT

Mirage NAC identifies devices immediately upon network entry, which provides a real-time map of your IP space, while kicking off threat and policy violation detection. In less than one second, Mirage NAC determines if it has seen a device before, and if it has, that device's past policy compliance and threat history; whether it is entering wired or wirelessly; and device type and services running.

If your security policy deems that any or all of these factors are indicative of an at-risk or simply unknown device, Mirage NAC can trigger a third-party security solution to run deeper policy scans, authenticate, update antivirus and more, or it can simply send the device to a designated quarantine server.

## ON-NETWORK NAC: THREAT MITIGATION

With its award-winning behavioral design, Mirage NAC wrote the book on effective post-admission threat detection. Additionally, it scans all network traffic for indications of policy violations, continually or on demand. If a threat or policy violation is detected, Mirage NAC enables action dictated by your security policy, which could include quarantining, triggering a third-party security action, or taking direction from a third-party solution.

## QUARANTINE AND REMEDIATION

Mirage NAC delivers first-level quarantine and remediation options by surgically removing offending devices from the network and informing users of this status through a browser window. While in quarantine, the offending devices are isolated to prevent cross-infection with other at-risk devices.

# Meets Your Needs.

## INFRASTRUCTURE-INDEPENDENT MITIGATION

Mirage NAC delivers targeted and highly flexible quarantining of offending endpoints, and enables user-appropriate mitigation options. For example, the CEO may be permitted network entry with an out-of-policy PC, while in the background, Mirage NAC 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 unmanaged 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.

To ensure the most flexible, customer-friendly approach, Mirage NAC's quarantining capabilities can be customized with remediation options based on user type, profile and other characteristics.

These capabilities 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 NAC 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.

## MIRAGE NAC PRODUCTS: YOUR FULL-CYCLE NAC SOLUTION

### nac appliance options: for networks of all sizes

- » **N-245 HA:** for networks of up to 32 VLANs/2,500 endpoints, with redundancy & failover
- » **N-245:** for networks of up to 32 VLANs/2,500 endpoints
- » **N-145:** for networks of up to 12 VLANs/1,000 endpoints
- » **N-125:** for networks of up to 4 VLANs/100 endpoints



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

### appliance management options: centralized management & monitoring

- » **M-2060:** hardware/software option for managing up to 50 appliances
- » **M-2050:** hardware/software option for managing up to 20 appliances
- » **M-SW:** software-only option for managing up to 5 appliances



"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**

"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 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**

"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**

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

- **Kazuhiro Nomura, CEO,  
Mitsui Bussan Secure Directions, Inc.**

### **About Avente:**

Avente is a systems integrator that specialises in the provision of converged networks. With a concept to conclusion philosophy, it is our aim to design, supply, install and maintain turnkey solutions that deliver a true value to our customers. Avente has the expertise to deliver IP solutions across many market sectors such as finance, education, health and engineering. Our project engineers are dedicated to providing high levels of service throughout the project lifecycle, and with our investment in training you can be assured of a professional and highly skilled service delivery. With our best of breed approach to solutions, we aim to provide network infrastructures that not only fit the requirements of today, but allow your business to grow when, and how it needs, without the need for major network redesign or reinvestment.

### **Contact Us Today:**

Avente Ltd.  
15 CP House  
Otterspool Way  
Watford, Herts WD25 8HR  
UK

phone: +44 (0) 1923650547  
fax: +44 (0) 1923650487  
email: [info@avente.co.uk](mailto:info@avente.co.uk)  
web: <http://www.avente.co.uk>