



# **NAC Solutions for Campus Networks**

**A Mirage Networks White Paper**  
January 2008

Mirage Networks offers the industry's most mature, easy to deploy, and effective Network Access Control technology. With the only NAC patent in the world, the Mirage solution includes both pre-admission and post-admission protection, or "Full-Cycle NAC." Mirage controls network access and ensures that all endpoints connected adhere to acceptable use policies. Mirage's appliance-based solution is built around a strong policy enforcement core that offers the ultimate flexibility for customized network policies. Mirage appliances deploy virtually inline, protect against malware without agents or signatures, and integrate into any environment without requiring network architecture changes.

### PRE-ADMISSION:

---

The Mirage NAC solution includes authentication, policy compliance, and risk assessment in its initial scans of entering endpoints. As soon as a device attempts to gain access to the network, Mirage immediately identifies the endpoint and runs a quick, effective policy check. The Mirage solution authenticates users against existing credential stores such as RADIUS, Active Directory, and eDirectory. The compliance check and risk assessment create a profile for each endpoint that determines which policies will be applied to that endpoint. Policies can be applied based on a vast matrix of properties including MAC address, OS type, OS patch level, presence and status of anti-virus packages, presence and status of anti-spyware packages, presence and status of host firewall, connection type (wired vs. wireless), open service ports, and much more. These out-of-box checks verify that each endpoint complies with the security policies in the network segment it is trying to join. Security policies are highly customizable, are easy to configure, and do not rely on the infrastructure for enforcement.

### POST-ADMISSION:

---

Mirage continues to monitor every endpoint once it gains access to the network, examining every packet for threatening or other out-of-policy behavior. A powerful threat detection engine protects the network from worms, viruses, botnets, unauthorized gateways, unauthorized servers, unauthorized applications, and much more. When Mirage detects unauthorized behavior, it zeroes in on the offending device and surgically isolates it. The quarantine can be complete, restricting the endpoint from communicating with any other device on the network, including other devices on its own segment; or a granular quarantine can be applied, allowing communication to specific endpoints, on specific ports, or based on other user-defined criteria.

### WHAT MAKES MIRAGE DIFFERENT

---

Mirage Networks offers the only Network Access Control product that is:

- **Patented:** the only NAC patent
- **Agentless:** does not require persistent endpoint agents
- **Virtually Inline:** requires no network re-architecture and does not introduce a single point of failure
- **Infrastructure Independent:** covers all devices, operating systems, and networks
- **Zero-day:** catches malware exploits immediately using behavioral threat detection and mitigation, not signatures or agents that must be updated constantly
- **Full-Cycle:** delivers pre-admission and post-admission policy enforcement out of the box
- **Layer Two:** quarantines without switch integration

The Mirage NAC solution is deployed on over 100 campus networks. The remainder of this paper discusses a sampling of those deployments and the value each organization realized.

---

## **WRIGHT STATE UNIVERSITY—AUTHENTICATING GAMING CONSOLES**

Wright State University of Dayton, Ohio estimates its students bring hundreds of gaming devices on campus each year. Gaming consoles such as the Microsoft Xbox and Sony PlayStation present a unique challenge for network administrators because they are purpose-built devices with non-standard operating systems that nevertheless have an IP address and connect to the Internet via the school's network.

"We originally required students to come in and register the MAC addresses of their games, which was time consuming for the IT department and the students," said Larry Fox, the director of networks for the school. The students' other option was to plug the consoles into their laptops and plug their laptops into the network, but that proved challenging. "It was a pain for them if they didn't know what to do," Fox said.

With the Mirage solution, Wright State University has optimized its network policies to allow students to register their gaming systems online and exempt them from the need to authenticate, while still identifying unusual traffic from those devices post-registration. The Mirage solution also allows network administrators the network visibility to match an IP address to a specific registrar, so if a gaming console exhibits unauthorized behavior, the IT department can immediately pinpoint the origin.

---

## **NORTHWEST MISSISSIPPI COMMUNITY COLLEGE—OS SCANNING**

When an infected student laptop introduced the Blaster worm to Northwest Mississippi Community College's (NMCC) network, the IT staff knew that they would have to focus on cleaning up student PCs every semester. At first, IT staff members performed all system compliance checks by hand, consuming IT cycles for the first two weeks of every new session—until the college installed NAC gear that automated the process.

The school deployed Mirage's NAC solution to perform an initial policy compliance scan on devices entering the network, and to handle post-admission screening to block devices exhibiting threatening or out-of-policy behavior. "Mirage Endpoint Control was exceptionally easy to deploy, and frees our IT staff to focus on projects instead of problems," said Chuck Adams, the network administrator for NMCC's Senatobia, Mississippi campus.

Adams marveled that Mirage's simple deployment and automated compliance checking has freed up six full time IT staffers, a net gain of man hours that essentially paid for the Mirage appliance in one semester. Now, when students try to login, their computers are automatically scanned for compliance with the college's PC health standard. If the endpoints fail, their owners automatically receive instructions on what to do to become compliant. Once they are compliant, the endpoints are granted network access.

---

## **SAN JACINTO COMMUNITY COLLEGE—CONTROLLING P2P FILE SHARING**

Citing fears of strong measures the Recording Industry Association of America (RIAA) is taking against file sharing, San Jacinto College, a community college based in Houston, deployed NAC technology from Mirage Networks on its three campuses.

"The RIAA is cracking down on illegal file sharing on campuses," said Will Sydnor, IT manager for San Jacinto College. "By implementing Mirage's solution, we can configure our sensor to detect and govern file sharing, and avoid the negative publicity that often comes with that type of activity. This also helps us avoid spending precious cycles tracking down students that are being pursued by the RIAA."

Mirage performed the deployment in conjunction with IT security service provider The Broadleaf Group, which formed a partnership with Mirage for delivering NAC solutions to the Houston area. San Jacinto College was the first customer of the new partnership. "In addition to their RIAA concerns, San Jacinto College was experiencing an uptick in the number of unmanaged student and faculty laptops accessing their networks, as well as an increase in hacking attempts" said Broadleaf's Jason Knight. With Mirage's NAC solution San Jacinto College's concerns could be solved with a single deployment, and the solution easily scaled to cover all three main campuses."

---

## **PENN STATE UNIVERSITY—POST-ADMISSION POLICY AND THREAT PROTECTION**

Pennsylvania State University of State College, Pennsylvania has an extremely heterogeneous network environment, as each college and department maintains its own budget and network architecture, and few university-wide standards are enforced. The university deployed a Mirage solution to protect their network from unpredictable threats that unmanaged endpoints can introduce.

“Institutions such as ours walk a fine line, ensuring that our networks are both available and secure. Given the sheer number of unmanaged devices needing access to our network, this means a tremendous strain on our IT resources,” said Kathy Kimball, Director of Computer and Network Security, Penn State University. “Managing each endpoint individually simply isn’t a realistic objective. That’s why a network-based solution as part of our overall security strategy makes sense—and why we selected Mirage Networks. Mirage gives us the ability to both watch network traffic and take action when an offending device is identified.”

With Mirage’s NAC technology, Penn State has the means to bring together its disparate network infrastructures into a unified security fabric. The University IT department gained the visibility to monitor network traffic for threats and the ability to pinpoint and avert dangerous and disruptive outbreaks before they start. The University can also leverage a robust set of configurable network policies to dictate the acceptable behaviors of all IP devices connected to the network.

---

## **ROUND ROCK ISD – POST ADMISSION ZERO-DAY THREAT & WORM PROPAGATION**

Round Rock ISD has a state-of-the-art network that serves more than 35,000 students and 4,000 staff across 43 schools and five administrative facilities. Despite having excellent perimeter security firewalls and intrusion detection systems, Round Rock ISD was unable to stop rapidly propagating threats that bypassed these defenses. Since installing Mirage’s NAC solution, Round Rock ISD has repeatedly discovered and stopped threats like Sasser and Welchia – without the need to use signatures or deploy agents.

RRISD deployed Mirage’s NAC Solution in a limited roll out in 2004; their current deployment adds appliances and a management server. “I read the articles in magazines today talking about how companies are touting ‘new’ ways to help secure networks. I think to myself, wait a minute, this is not new—Mirage has been doing this for years, which means we have been too,” said Dan Scott, Senior Systems Engineer, Round Rock ISD.

RRISD’s implementation of the Mirage Management Server enables their IT managers to integrate all their Mirage appliances into a single security fabric, creating a convenient centralized point for policy configuration, network visibility, and event reporting. Mirage Endpoint Control deployed seamlessly with RRISD’s existing network architecture, requiring no changes to their Cisco infrastructure. “We initially considered Cisco’s NAC offering, but decided against it when our research uncovered how complicated the deployment would be,” said Scott. “The Mirage Endpoint Control solution is effective and easy to deploy, and after reviewing our options it was the clear winner for us. The product has been rock solid from day one. In fact, the Sasser virus hit us during the install. Without Mirage, our network would have been a mess.”

“With our small network IT staff, it is essential that we have an automated solution to stop worms that get past perimeter defenses,” said Scott. “With the Mirage Networks solution, instead of 200 or 300 systems to clean up, we’ll only have the initial infection point, which will remain contained until we have the time to remediate that system.”

---

## HAMILTON COLLEGE—PRE- AND POST-ADMISSION

Hamilton College of Clinton, New York already knew the value of a Mirage post-admission behavioral monitoring solution. The college returned to Mirage when it decided to add pre-admission policy checking. The college has now integrated a full-cycle Mirage solution into their network architecture. The expanded solution adds pre-admission scanning to post admission behavioral detection and policy enforcement. Hamilton College now has a campus-wide security fabric that provides both a single view of the network and centralized policy management.

Hamilton College recently experienced a situation where a student laptop left unattended in the school library was stolen. A week later the stolen laptop reappeared on the network and Mirage immediately detected it and sent an alert, including the username of the person logged in to the laptop. This allowed the IT staff to notify campus security, who tracked down the alleged thief.

“We needed a way to automate the process of monitoring our network traffic and devices,” said Dave Smallen, vice president of information technology, Hamilton College. “The full-cycle Mirage Networks solution gives us the network visibility to analyze, detect, and stop network problems without disrupting workflow at the College.”