



Network Access Control for University Networks

Vulnerability Management

BENEFITS:

- Reduce IT cost and burden
- Automate policy enforcement
- Avoid time wasted manually remediating devices

System Compliance

- Verify endorsed anti-virus presence and status
- Verify critical OS patches
- Schedule scans with self-remediation
- Customize policies based on identity, device type, location, department

Network Activity

- Govern high risk applications such as IM and P2P
- Detect and isolate unauthorized servers and services
- Detect and isolate unauthorized routers
- Detect and isolate unauthorized WAPs

Identity

- Associate an identity with every device
- Leverage SSO for known devices (seamless user experience)
- Enforce LDAP group policies

Threat Detection & Containment

BENEFITS:

- Ensure privacy of sensitive student data
- Eliminate back to school fire drills
- Never waste time chasing threat propagation
- Ensure network bandwidth is protected

Malware

- Detect and isolate botnets
- Detect and isolate zero-day threats
- Detect and isolate worms and viruses
- Stop hacking attempts
- Detect and shut down reconnaissance
- Isolate VoIP threats

Physical Threats

- Track and recognize stolen devices
- Restrict segment access to specific device types

Compliance

BENEFITS:

- Eliminate credit card data privacy issues
- Meet audit requirements
- Eliminate IT time spent locating offenders

PCI

- Verify endpoint status
- Maintain internal IPS protection
- Detect and stop protocol violations
- Segregate server applications

RIAA

- Automate auditing to respond to RIAA
- Enforce acceptance of usage policy statement
- Identify P2P traffic
- Out of policy devices

HIPAA

- Protect un-patchable devices
- Log all packets from all devices, all sessions
- Prevent and respond to attacks and other system failures

Device Management

BENEFITS:

- Enjoy full wireless network protection
- Maintain accountability while allowing student freedom

Handheld Devices

- Detect and govern iPhones and smartphones
- Require authentication
- Control services that can be accessed by handhelds

Registration

- Register any device—gaming consoles, Tivos, Slingboxes, lab equipment

About Mirage Networks

Mirage Networks, Inc. is the leading provider of Network Access Control (NAC) solutions. Mirage's patented technology gives organizations control of all network devices, increases network uptime, ensures policy compliance, and reduces operational costs. Mirage's NAC appliances work in all network environments, deploy virtually inline, and require neither signatures nor agents to enforce policy and terminate zero-day threats. Mirage Networks is a consistent winner of industry awards and recognition. Learn more about Mirage Networks at www.miragenetworks.com, and visit the Mirage CTO blog at www.mirageblog.com.

Mirage solutions are made available through Authorized ChannelFirst Partners and can also be delivered as a managed service.

Corporate Headquarters

3600 N. Capital of Texas Highway
Suite B370
Austin, Texas 78746
Sales: +866.869.6767
Corporate: +512.874.7800
FAX: +512.874.7806

International Offices

EMEA
Zijdweg 26
2244BG, Wassenaar
Netherlands
Tel: +31 70 5170419
FAX: +31 70 5177676

Asia Pacific
3-23-7-702 Koishikawa
Tokyo, Japan
112-0002
Tel: +1 512 377 6978
Tel: +81 80 3002 0195



www.miragenetworks.com