



## The Top 10 Questions To Ask Your NAC Vendor

It's not always easy to separate hype from reality. Ask NAC vendors you're considering these **top ten questions** to determine which solution is best for you.

### Will your solution:

1. perform pre- and post-admission checks?
2. work in any network infrastructure?
3. quarantine out-of-policy endpoints without relying on infrastructure integration?
4. ensure end users understand why their access is being cut off, and what to do about it?
5. enforce security policies in a flexible and measurable way?
6. protect all current and emerging IP-enabled assets, regardless of operating system?
7. be practical for all business units, no matter location or size?
8. catch new zero-day threats, botnets, rootkits, trojans and keyloggers?
9. protect all key parts of the network — LAN, wireless and VPN entry points, and the network interior?
10. distinguish between device types like wireless and wired devices, or routers from ordinary endpoints?

**If your vendor can't say YES to every question, there are better NAC alternatives.**

### Your ideal NAC solution should:

- run continually, because threats don't just give up after the initial sign on.
- protect heterogeneous environments — without upgrades, agents or switch integration.
- keep at-risk and infected machines quarantined without relying on the infrastructure for enforcement.
- inform end users of what's happening to reduce downtime and streamline fixes.
- enable IT administrators to institute and enforce security policies.
- protect all IP-enabled devices.
- offer scalable solutions for every office size at an attractive price point.
- catch the latest threats in real time to supplement patching activity.
- protect every aspect of the network, regardless of how users access it.
- distinguish between different endpoint types like wired and wireless, and routers and endpoints.

### Mirage NAC Provides:

- » Easily customizable and infrastructure-independent quarantine and remediation capabilities to eliminate cross-infection while enabling issue-specific remediation.
- » The ability to detect and mitigate threats and policy violations on any IP device type — wired and wireless, managed and unmanaged, from the desktop to IP telephony and beyond.
- » A self-contained, full-cycle approach whose open design eases integration leverage ongoing current security technology.

**Mirage Network  
Access Control is  
the right solution.**

## 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](http://www.miragenetworks.com), and visit the Mirage CTO blog at [www.mirageblog.com](http://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](http://www.miragenetworks.com)