



Can you measure the ROI of your NAC solution? Mirage offers the NAC Payback Series to show measurable, real-world examples of how our solutions work for you.

## NAC Payback Series

# Controlling Peer-to-Peer Applications

### The Problem:

While P2P applications vary widely in both their technology and use, file sharing, by far, constitutes the primary usage of P2P networks worldwide. This usage poses significant security issues, particularly in the higher education space, where administrators must constantly balance providing an open collaborative network to their students against governing the appropriate use of the university's computing resources, which are disproportionately taxed by P2P traffic.

Peer-to-peer networking is clogging network throughput in many organizations, and a disturbing amount of the P2P traffic is the illicit distribution of copyrighted material such as pirated songs and movies. For example, the Recording Industry Association of America (RIAA) has made a point of singling out university students who are downloading and sharing this material, offering hefty fines in lieu of further litigation. In fact, pre-litigation letters are delivered directly to the universities, who are then obliged to find the students—even though the names aren't known by the RIAA. Matching student user names to computers they used on P2P networks some time in the past can consume significant IT staff cycles. The RIAA has also published lists of the universities with the highest amounts of illegal network traffic; appearing on a RIAA watch list can be bad news for a university, creating a public relations problem and risking future alumni contributions. The RIAA isn't the only organization calling for organizations to shoulder more responsibility for illicit P2P networking; the Motion Picture Association of America is also taking action and Congressional legislators are threatening to enact new laws requiring universities to implement technological filters to quash illegal P2P networking, as well as compelling educators to warn students about illegal file sharing.

However, the problem of governing P2P usage is not limited to educational institutions, because P2P networks also pose a significant threat vector that can be used for the purposes of identity theft, worm propagation, and spam. Government officials have gone on record claiming P2P file sharing to be a significant threat to national security. In a statement offered to a recent Government Reform Committee, Retired General Wesley Clark said his firm "found more than 200 classified government documents in a few hours' search over P2P networks." Clark's suggestions included the implementation of network monitoring systems that could prevent the leakage of sensitive government information through P2P file sharing. Clark noted that many of our national information security leaks often were distributed on home computers over P2P networks.

### The Solution:

Mirage Networks provides a comprehensive NAC solution that allows administrative staff to detect, alert on, govern, and block P2P usage. Mirage's configurable behavioral monitor provides detection capability for all of the major P2P networks

#### Peer-to-Peer file sharing risks:

- » **Losing the bandwidth you pay for.** P2P applications can turn any computer into an always-on bandwidth glutton because they run unattended, without any user intervention
- » **Opening the door for worms, viruses, spam, and identity theft.** Attacks on P2P networks increased 357% year over year
- » **Dealing with copyright infringement.** Twenty-three new schools to receive latest round of pre-lawsuit letters

(including BitTorrent, Gnutella, FastTrack, eDonkey, OpenNap, and more). Once detected, the unauthorized use of P2P applications can result in a wide range of administrative action, including logging and alerting, blocking the P2P application, and outright restriction of network access for the offending computer.

By implementing Mirage's NAC solution, organizations can not only define policies for acceptance into the network, but also policies for the ongoing usage of the network, all from a central management console. Unlike other systems that require third-party components for acceptance and usage policies, Mirage provides the only integrated architecture that allows organizations to fully incorporate admission and usage criteria, minimizing deployment and management complexity, while allowing for network growth over time. Mirage's P2P policy set is a component of this architecture, allowing organizations to weave P2P application usage into their overall network access policy portfolio, minimizing the chances for malware propagation, asserting control over their network resources, and allowing organizations to comply with the ongoing statutory regulations governing the unauthorized distribution of copyrighted content.

### 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)