

Controlling Rogue Devices

The Problem:

The past five years have seen a rapid expansion of new classes of devices connecting to business and campus networks. These devices pose unique challenges for IT and security staffs, as they look to set, establish, and enforce acceptable use policies for their networked environments. Examples include Mobile Internet Devices (MIDs) such as iPhones and other Wi-Fi-enabled handheld devices, and personal routing devices. Both highlight the issues rogue devices can pose to open environments, and even in the most highly controlled networks.

Mobile Internet Devices (MIDs)

MIDs pose unique challenges for enterprises and on college campuses, which have a tradition of open connectivity for all devices. Recently publicized broadcast storms involving the Apple iPhone and Cisco wireless controllers are examples of the risks that can arise between unknown wireless devices and the wireless infrastructure – whether caused by the device or the wireless infrastructure.

Even in tightly controlled corporate environments, new rogue wireless devices can connect unless some form of manual inclusion is employed to block unknown devices. Most organizations strive to avoid manual processes, so wireless access points are typically a vulnerable entry point to the network. Worse still, unlike corporate networks where an IT staff may be able to prohibit connection of these devices, higher education environments have a tradition of openness and collaboration that removes outright prohibition as an option.

Personal Routing Devices

Routing devices are now available for less than \$50, and include features that add to the risk posed to the environment, including encryption, wireless radios, and DHCP servers. Unlike the MIDs, where staff must typically allow the devices to connect and then manage them, IT staff can more easily enforce a policy to block connection of personal routing devices altogether.

The Solution:

Mirage Networks' family of agentless, full-cycle Network Access Control (NAC) appliances provides an innovative set of options to bring control to any network environment. Mirage's unique approach to NAC combines an out-of-band deployment model with an extremely effective means of quarantine, and a broad set of admission checks with the industry's most robust behavioral detection engine. These combinations work together to provide organizations with the broadest possible set of options for managing the risk of these devices.

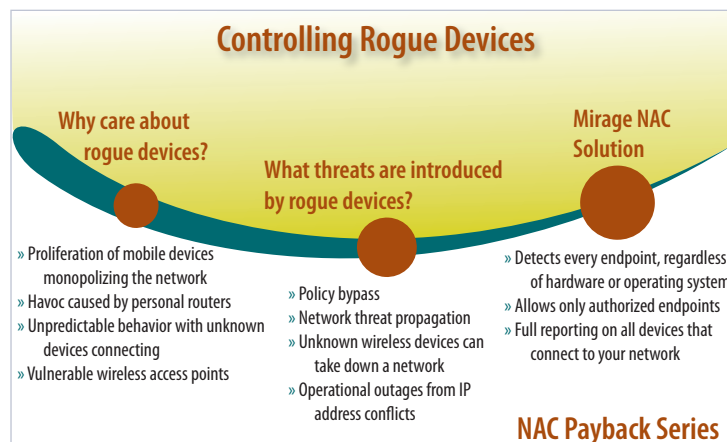
With MIDs, whether they're iPhones or Windows Mobile devices, Mirage's OS detection and agentless model allow IT to craft governance and risk management policies

specific to the device type or OS type. Because saying "no" is often unrealistic, Mirage enables staff to say how devices can connect.

Because most personal routing devices were built with the intention of building out a home-based network, connection of these devices to a large established network can have unexpected results, including operational outages from IP address conflicts, policy bypass, and

even threat propagation. The Mirage family of appliances gives the option to detect and manage these devices with a set of behavioral profiles specific to the device class, or to detect and block rogue routing devices entirely.

Providing network services in an enterprise or campus environment often means allowing a variety of new types of devices to connect. Managing the risk that is both inherent and explicit in desktops and special purpose devices is a key function of most security staffs as they struggle to find balance between the need for governance and the need to provide an open computing environment that truly serves the organization. Mirage supplies the solution to set realistic policies that strike this balance in a highly effective manner.



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