

The core of Mirage Endpoint Control™ is a behavioral rule set:
six categories of rules, which detect behavior that is indicative of an
attack, either internal or external.

Threat Propagation

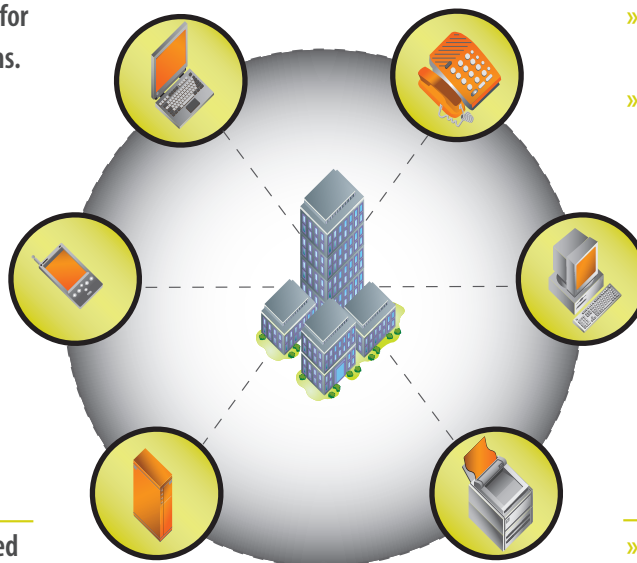
- » Monitor a sender's communications for unusual frequencies and destinations.
- » Track traffic to unused IPs and use deception technology to slow and block attacks.

Mail-Related

- » Only mail servers should perform a DNS Lookup—when any other machine does so, it is likely propagating threats.

Custom Rule Profiles

- » Allow or disallow any user-specified device or behavior.



Reconnaissance

- » Catch cyber criminals looking for a chink in the armor via a ping flood.
- » Certain packets only exist to commit reconnaissance, and are identified by their violation of protocol standards.

IP Telephony

- » Prevent unauthorized traffic on IPT network segments, DoS, and spoofing.
- » Detect infected cell phones.

Spoofing

- » Detect spoofing, in which the initiator changes the appearance of a packet's source, and which can result in a DDoS.

Behavioral Rule Scenarios

EMAILED THREATS

Many worms spread by downloading an SMTP mailer onto the device they are infecting to enable a rapid spread. A user's PC or laptop will generally send out less than 50 emails in one day; Mirage Endpoint Control's behavioral rules can identify excessive email traffic as potentially threatening, so the offending device can be quarantined.

IP TELEPHONY THREATS

When setting up an IP telephony network, IT should be able to prevent specific device types from entering areas designated for IP telephony devices. For instance, if a Windows® device attempts to access IP telephony network assets, Mirage's rules detect this traffic and can block it, stopping a potential threat in its tracks.

You Can't Control People. Control What's On Your Network.™

About Mirage Networks

Mirage Networks, Inc. is the leading provider of network access control (NAC) solutions, including both pre- and post-admission security. The company's patented technology gives organizations control over unknown, out-of-policy, and infected devices resulting in increased network uptime, policy compliance and reduced operational costs. Mirage's NAC appliances work in all network environments, deploy out-of-band and require neither signatures nor agents to enforce policies and terminate zero-day threats. Based in Austin, Texas, Mirage Networks' Endpoint Control is a consistent winner of industry awards and recognition.

Contact Us Today:

Mirage Networks
6801 North Capital of Texas Highway
Building 2, Suite 200
Austin TX 78731

phone: 866.869.6767

fax: 512.874.7806

email: info@miragenetworks.com

web: <http://www.miragenetworks.com>