

## Controlling Instant Messaging Applications

### The Problem

Recent articles offer evidence that threats to networks running instant messaging (IM) are on the rise, with numerous studies indicating that attacks over IM networks are up 80% in 2007. Meanwhile, organizations have little visibility into which IM applications are active on their networks. This problem is especially acute on university and college campuses and similar open computing environments, where many computing devices are outside the control of administrative staff. Organizations are left to balance the value of this highly collaborative tool against the inherent risks.

A typical IM attack resembles classic email malware, with a heavy social engineering component and a disguised link that launches malware when the recipient clicks on it. The obvious and profound difference is the delivery medium, in this case IM chat sessions. This is significant because most organizations implement email filtering technology, which can be quite sophisticated in thwarting attacks. However, most do not secure IM traffic and end users are not as educated about the threats inherent in the IM medium. Network administrators have varied reasons for allowing less secure IM, but most hinge on a lack of visibility into the volume and type of IM traffic on their networks.

Recent industry reports cite IM applications that leave the door wide open for malware, and attackers have taken notice. There have been almost 300 new IM threats reported in 2007, afflicting MSN Messenger, Skype, and other popular IM applications. Some experts identify IM applications as the most underrated threat today because most organizations have not deployed solutions to govern them.

### The Solution

Mirage Networks' patented NAC solution provides simple, out-of-the-box and easy to administer content that allows IT administrators to:

- » Gain visibility into which IM applications are active on their networks
- » Block the common threat vectors in IM applications
- » Design and implement cohesive policies around the use of IM

Whether driven by a compliance initiative, in response to recent threat outbreaks, or to gain additional infrastructure visibility and manage network bandwidth, exercising control over IM applications and protocols delivers measurable ROI for

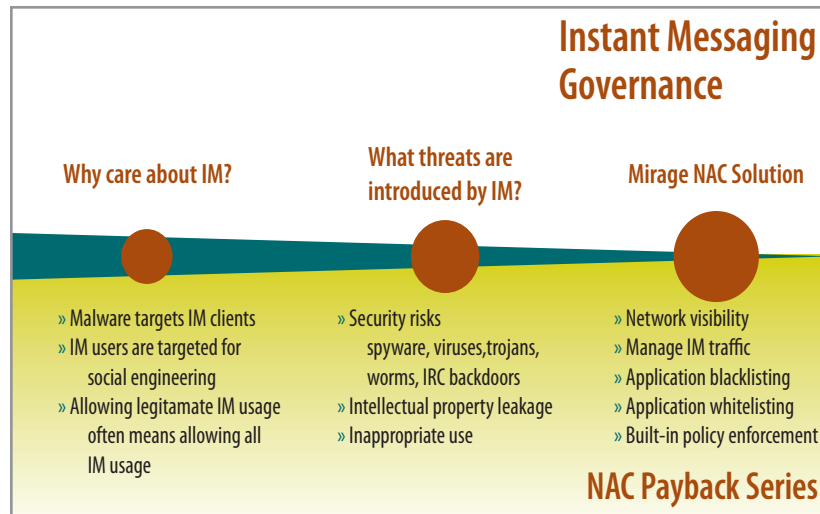
an overall NAC strategy. Using an out-of-band deployment model and flexible behavioral policy engine, Mirage combines pre- and post-admission policy to provide this critical functionality quickly, simply, and out-of-the-box.

Mirage's behavioral policies are highly flexible and configurable, allowing organizations to "whitelist" a particular application or protocol, and disallow others.

They also provide visibility into, and

protect their environments from, threats propagating across popular IM applications. Administrators can choose a variety of actions to take upon detection: ranging from notification to network and security staff, to notification to the end user, or complete removal of network access for the offending device.

For network administrators facing the threat of IM attacks, knowing what they're up against is half the battle. Mirage offers a comprehensive visibility into the network that's the backbone of its award-winning, easy-to-deploy NAC solution. By deploying Mirage Endpoint Control, organizations can protect their bandwidth and network security by monitoring IM traffic and preventing malware outbreaks before they start.



### 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)