



Mirage NAC™ Safeguards Leading Hospitality Organization's Network Against Worm Attacks



INTRODUCTION

Recently a global enterprise found itself doing the following math:

unmanaged devices + geographic dispersion + few IT resources + worms = a network security nightmare

Unmanaged devices are at the heart of the majority of security breaches that stem from the network interior — where most threats originate. How do you ensure your authorized users have the access they need to be productive without opening the door to every new worm?

This is the story of one company that found an answer in Mirage NAC.

THE CHALLENGE

Following M&A activity, an organization was left with a large worldwide network, poorly designed and with few security mechanisms in place. The network grew out of acquisitions, creating a situation of uncontrolled, unmanaged and unknown connectivity into a critical, centralized business control system. Further complicating the matter was that, due to a buyout, the company's IT staff had been temporarily reduced to only two individuals.

The network was successfully attacked by a variant of the Sality worm. The attack began at a remote site and spread quickly across the network interior. The challenge faced by IT was not only to stop the attack, but determine which device was at fault and why it was vulnerable.

Most problematic was that, given the network setup, the IT staff had no fast way of determining which device was the guilty party: on average, IT required 1-2 days to locate infected devices. Once located, several applications were required to fix the offending endpoints: a freeware remote access application to reach the device, a vulnerability scanning application to determine the problem, and a proprietary exe removal tool. In all, IT spent an average of 4 hours a day fixing suspect endpoints whose users had manually put in calls to a central Help Desk.

In this instance, the PC in question was located in another country, and had been vulnerable to attack because it failed to take the antivirus patches that IT had pushed out the previous week — even though IT considered this a managed endpoint!

continued »

» executive summary

Industry:

- » Hospitality

Business Challenges:

- » Ensure security on a large, distributed network
- » Avoid damage of worm attacks
- » Provide access to unmanaged devices

Security Answer:

- » Mirage NAC immediately identifies the offender
- » Mirage NAC delivers fast quarantine and remediation

Business Value:

- » Frees up scarce IT resources
- » Eliminates need for cobbled-together applications
- » Keeps workers productive and the network safe

THE MIRAGE NAC PAYOFF

Mirage NAC was implemented in audit mode, to locate the offending device — which it did within 3 minutes of implementation. It also identified several other devices committing behavior indicative of infections; those endpoints were later also determined to be carrying and propagating active infections.

Because it maps the IP network in real time, Mirage NAC was able to ascertain the presence of any network-attached device quickly and easily. Mirage NAC frisks endpoints for policy violations as they come on the network, making it difficult for an out-of-policy device to achieve access in the first place. And its continual threat and policy checks mean that, should a device become infected or out of policy once on the network, the device can be quarantined and remediated before a threat can spread. Plus, Mirage NAC delivers centralized management capabilities that enable IT to reach and remediate offending endpoints immediately and automatically.

Best of all, Mirage NAC doesn't rely on agents and is device- and OS-independent, so it can check all IP devices, managed and unmanaged, with equal ease and effectiveness.



About Mirage Networks:

Mirage Networks is an Austin, Texas-based network security company dedicated to delivering real world, full-cycle network access control solutions, serving the enterprise through a strong channel of resellers, original equipment manufacturers and managed security service providers. Mirage Networks solutions ensure an IT- and user-friendly experience that never forces a compromise between business objectives, effectiveness and usability. The company's passion for innovation has paved the way for the development of patent-pending technology that gives IT managers control in an uncontrollable environment of infected, unmanaged and out-of-policy devices. Contact us today to learn more about the industry's only self-contained network access control solution.

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>