



A Case Study from Mirage Networks®

INTRODUCTION

Faced with several typical healthcare-provider IT challenges, Chicago-based Mount Sinai Hospital decided on an unconventional IT solution to keep its network safe.

The Mirage Endpoint Control™ solution, with its agentless, out-of-band technology, was implemented to address these three potential problem areas:

- Threats jumping onto the network from devices running on embedded operating systems (OSs), for which the availability of upgrades and patches can lag the rest of the market by six months or more
- Reconnaissance by unauthorized users of applications that require a server, managed by an external vendor, to be placed on the hospital network
- Policy violators, such as unauthorized or infected devices, that jeopardize HIPAA compliance and make patients' personally identifiable information vulnerable to prying eyes

THE CHALLENGE

Mount Sinai, like organizations in every industry the world over, has to deal with two factors that often complicate network security efforts: a mixed network infrastructure, and increasing numbers of new mobile access points, like PDAs and wireless laptop stations, that require network access. Furthermore, like many businesses, every day many salespeople and other visitors to the campus bring with them laptops capable of connecting to the network via either a hardwired or wireless connection. A contaminated device could do significant damage to the network unless unauthorized activity can be immediately suppressed.

However, Mount Sinai hospital's IT staff has some industry-specific challenges to securing its network: it has to support and enable point-of-care equipment and applications that can dramatically improve patient care, but which are difficult, if not impossible, for IT to manage.

Specifically, these tools present the following challenges:

1. *The entry onto the network of threats like viruses and worms, jumping into the network from devices running on embedded operating systems*

Life-saving machines on rolling medical carts, a boon to the fast and effective application of patient treatments, are a hospital must-have. However, many of these devices run embedded operating systems (OSs), which are contractually supported by a third party; development and deployment of OS upgrades and patches for these devices often lag the rest of the market by six months or more, and are dependent on third parties for delivery and implementation.

continued »

» executive summary

Industry:

- » Healthcare

Business Challenges:

- » Prevent threats from devices with embedded OSs with slow patch availability
- » Secure from reconnaissance while allowing server-level access to third parties
- » Address HIPAA regulations requiring the security of personal patient information

Mirage Endpoint Control Solution:

- » Controls network access to keep third parties within authorized areas
- » Catches threats behaviorally to ensure security before patches are available
- » Helps prevent authorized users from gaining unauthorized access to HIPAA-specified protected health information

Business Value:

- » Ensures maximum network uptime and availability for excellent patient care
- » Keeps patient data confidential to meet HIPAA regulations
- » Lessens drain on IT resources to increase productivity

Worm and virus builders, becoming ever faster and more targeted in their malicious duties, could easily target a vulnerability on one of these machines before the patch is available or implemented. From there, it's an easy hop onto into the network interior.

2. Outsider network reconnaissance through applications that run on internal servers managed by external vendors

To meet the stringent and unique requirements of healthcare providers, technology for healthcare has evolved to include applications that perform very specific functions. Increasing and training IT staff to be able to include management of these products is, for many, not feasible, so it has become *de rigueur* for these applications to be managed by external vendors, even though the servers hosting these applications are on the hospital premises and network. For IT, this could well represent a hole in the hospital's network security.

Mount Sinai needed the ability to control the access these vendors have to network areas, to ensure they do not venture into the network itself to conduct reconnaissance that could reduce network uptime and availability.

3. Violation of HIPAA regulations mandating the security of personally identifiable patient information

Healthcare IT not only has to enable maximum network uptime and access, it has to do so within very rigorous regulations concerning data security. Mount Sinai must maintain compliance with the Healthcare Insurance Privacy and Accountability Act (HIPAA), which demands the confidentiality, integrity and availability of all electronic protected health information; protection against unanticipated threats or security vulnerabilities and against unauthorized use of the data; and the compliance of all staff members with these safeguards. If a threat breaches the network and enables a cyber-criminal to download confidential data, the penalties can be stiff indeed.

To help maintain its HIPAA compliance, Mount Sinai required an effective, easily implemented way to prevent authorized users from accessing unauthorized information.

THE SOLUTION

Mount Sinai chose Mirage Endpoint Control out-of-band appliances to meet these challenges head-on, covering 60 VLANs across multiple buildings. With technology that covers any IP device, current and emerging, managed and unmanaged, it plugged into Mount Sinai's in-place infrastructure to provide an easy to manage, yet effective, approach that delivers:

- Network Access Control (NAC) – agentless, network-based NAC approach enables appropriate network access based on user role and device recognition; identifies rogue devices; and helps ensure high network availability
- Day-Zero Threat Detection – patent-pending behavioral technology finds threats even on day zero and is effective out of the box; generates nearly no false positives to maximize user uptime; and requires no signatures or updates to remain effective
- Policy Enforcement – infrastructure-independent quarantine isolates offending devices without encouraging cross-infection; enables customized remediation options; and lessens the drain on IT bandwidth by promoting user self-remediation

And Mount Sinai saw a very short time to value with Mirage Endpoint Control: immediately upon implementation, the solution identified four rogue devices seeking network access, several unauthorized devices attached to the network, as well as numerous misconfigurations in the network.

“We simply have too much to lose – Mount Sinai's stellar reputation, HIPAA regulations, and the availability of point-of-care equipment that improves our patients' outcomes, it can all come down to IT security. No other solution we looked at provided both the effectiveness and the flexibility we required to find and stop threats on all devices, even the hard-to-manage mobile machines. It's working so well, at this point, I honestly don't know what we'd do without it.”

*Peter Ingram
Chief Information Officer
Mount Sinai Hospital*

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>

©2006 Mirage Networks, Inc. All rights reserved. Mirage Networks, the Mirage logo, Mirage NAC, NAC-in-the-Box, and “You can't control people. Control what's on your network.” are trademarks or registered trademarks of Mirage Networks. All other names and products may be trademarks of their respective companies.