



Health Access Solutions

Background

Health Access Solutions (HAS) is a leading application service provider located in Foster City, California. HAS



is the software marketing division of Pacific Partners Management Services, Inc. (PPMSI). Their Access Express™ system distributes patient demographic and clinical information to more than 13,000 physicians affiliated with hospitals, medical groups, and health plans. Access Express software manages and automates managed care referrals, communication, and care for more than 1.8 million HMO and Medicare patients.

Health Access Solutions' healthcare technology team has worked together for years to develop a streamlined information technology and management strategy.

Challenges

As a healthcare company that deals with confidential patient information daily, many HAS policies and procedures are mandated by Health Insurance Portability and Accountability Act (HIPAA) regulations. HIPAA requires all

healthcare organizations, including hospitals, physicians, health plans, and public health authorities, to protect the confidentiality and security of all individually identifiable health information.

Health Access Solutions endeavored to improve the corporate network environment for two years before imple-

menting Mirage Endpoint Control for network security in 2005. While they had a solid security backbone in place when they first began speaking with Mirage Networks, they were keenly aware that endpoint control was a major security consideration that needed to be addressed.

Simply put, endpoint control ensures that the devices that access the corporate network will not introduce viruses or other malware that can risk the stability of the network. (Malware is malicious software designed to damage a computer system.) An endpoint control system assesses the devices that enter the HAS network for policy compliance and malware before they are allowed access, and

the system continually monitors those devices continually once they enter the network. Health Access Solutions employs 120 local network users housed in two buildings, and ten remote users who access the network via virtual private networks or remote desktop connections. HAS hosts its own application, as well as several client applications, so they have thousands of individually authorized users in the state of California who log on 24/7 to access their data via the web. Each user has

"Mirage network access control is a solution that provides complete control over the endpoint devices on a corporate network. The solution is considered "full-cycle" network access control because it includes both pre- and post-admission security, ensuring that devices comply with network policy before they enter the network, monitoring their behavior the entire time they're on the network, and surgically quarantining any at-risk devices. These ongoing security checks and the assurance of rapid remediation of violators help us ensure that no single device will threaten the stability of the HAS network."

Marc Fernandez, Regional Director, Mirage Networks

a unique user ID and password that gives them access to only the limited confidential information they need to know in order to do their job.

Such unmanaged, dispersed users can unwittingly introduce viruses and other malware from infected or out-of-policy computers. Malware can potentially

"We were looking for a managed solution and wanted to leverage our existing network service account with SBC/AT&T. We were introduced to Mirage Networks by SBC/AT&T, a major channel partner of Mirage Networks. After considering other vendors, as well as an in-house solution, we ultimately determined that the Mirage network-based approach to endpoint control would be the most effective and reliable solution to meet our continuing security requirements."

Gary D'amato, Systems Manager, Health Access Solutions

bring down the network, compromise the security of our patient data, and affect the productivity of HAS as well as the productivity of its clients.

Technology Issues

The HAS network environment is one of multiple users and unmanaged devices, which greatly increases the chances of vulnerabilities threatening the network. Such vulnerabilities can include out-of-date patches (temporary fixes for software defects), missing anti-virus updates, malware, and other threats.

Part of HAS' existing challenge was simply protecting network users from themselves. Most of the HAS network's regular users do not really think before they act, they just click—and that can mean clicking on a virus disseminating email that might have gotten through existing network defenses.

Solution provided by Mirage

The installation of Mirage NAC technology at HAS took place in January 2006. The Information Technology department of Health Access Solutions installed two Mirage 245 Endpoint Control devices, one for each of its two buildings, and one Cisco ISP 4240 in the data center.

The precision with which the Mirage network vulnerability assessment technology identifies malware and isolates offending endpoints is critical to the HAS network environment of multiple users and unmanaged devices. The Mirage solution uses behavioral rules to assess endpoints seeking network access and to identify virtually any vulnerability that might threaten the network. The solution addresses the vulnerabilities to which HAS was prone: out-of-date patches, missing anti-virus updates, malware, and other threats. The solution can achieve this even if the threat is new and patches are unavailable or not yet installed.

Once a vulnerable endpoint is identified, Mirage places it in a surgical quarantine to allow repair and remediation, circumventing potential damage to the network without impeding the productivity of "healthy" endpoints. When

the vulnerable endpoint has been remediated, it must authenticate against HAS' in-place servers before being allowed to return to the network. Mirage Endpoint Control continues to check the device for vulnerabilities once it has reentered the network,

Summary

Health Access Solutions has long been aware of the potential dangers that lurk behind every one of the thousands of devices that attempt to connect to its network. Using a NAC solution from Mirage Networks, bolstered by the AT&T/ Mirage IPS, HAS now has their cost-effective, painless, and essentially transparent security solution that provides the network protection they need, given the realities of remote logins, zero-day malware exploits, and mobile computing. HAS and its clients conduct their business with the peace of mind that any network security vulnerabilities will be immediately identified, quarantined, and remediated. In the world of healthcare information management, such security assurance is not a luxury; it is truly essential.

Mirage Networks has the Only Patented NAC Solution that:

- » Is agentless—requires no agent software to effectively defend against malware attacks
- » Enforces surgical isolation—devices can be completely isolated, or granular access can be granted based on the device or the infraction
- » Deploys out-of-band—no network re-architecture, no single point of failure
- » Is infrastructure independent—The Mirage solution integrates with all networks, all devices, and all operating systems

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.

Mirage Networks

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

phone: 866.869.6767

fax: 512.874.7806

mail: info@miragenetworks.com

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