



Customer Case Study

# Leading Psychiatric Hospital Safeguards Key Healthcare Data

The Menninger Clinic improves network reporting to ease regulatory compliance and protects sensitive records with Cisco security solution.

## EXECUTIVE SUMMARY

### The Menninger Clinic

- Healthcare, nonprofit
- Houston, Texas
- 400 employees
- Affiliated with Baylor College of Medicine and The Methodist Hospital in the Texas Medical Center

### BUSINESS CHALLENGE

- Improve network visibility to help comply with government healthcare regulations.
- Protect sensitive medical information and applications from internal and external security threats.
- Control ongoing administrative expenses.

### NETWORK SOLUTION

- Cisco Security MARS helps IT staff detect and mitigate network security issues and enhance reporting.
- Cisco Intrusion Prevention System protects against external threats such as worms, viruses, and spyware.
- Flexible Cisco Medical-Grade Network integrates with existing systems and applications.

### BUSINESS RESULTS

- Prompt, detailed threat reporting improves health regulation compliance.
- Intelligent network security helps protect data, improve information integrity, and enhance network reliability.
- Scalable network enables Menninger to support additional healthcare applications on its network, while maintaining regulatory compliance.

## BUSINESS CHALLENGE

One of the world’s premier psychiatric hospitals for over 80 years, The Menninger Clinic has earned a reputation as a leader in mental health treatment, research, and education. Information technology plays a vital role in supporting Menninger’s state-of-the-art treatment programs. The network at its location in Houston serves 400 employees and spans seven buildings on 14 acres. Each building is connected via a fiber-optic backbone to a central server facility on campus that hosts information critical to treatment and hospital management.

“We depend on our network and servers to support our patient information databases and our medication administration applications,” says Michael Farnum, information security manager at Menninger. “We also depend on our network to document patient care on a daily basis.”

Network integrity and security are essential to keeping Menninger’s medical operations running. Like most healthcare organizations, Menninger must also comply with the Health Insurance Portability and Accountability Act (HIPAA), which establishes stringent regulations for handling and safeguarding patient records.

“Our biggest issue is HIPAA compliance,” says Farnum. “HIPAA requires that we document any network incidents and report them in a timely manner.”

Menninger is a medium-sized psychiatric hospital with an IT staff of six. Manually tracking and reporting the dozens of network events that occur each day made HIPAA compliance an increasing burden.

“One of the main issues that I was confronting was simply checking logs and keeping track of all the day-to-day activity on our network,” says Farnum. “I am the only dedicated security person, so it was a huge challenge.”

The importance of security was only expected to grow as Menninger began moving more of its key operations to the network. With an ever-increasing volume of data from network devices, applications, and servers, detecting and responding to threats were expected to become increasingly difficult.

“In the past, we tried to keep a low profile and avoid hosting a lot of data on servers that can be reached via the Internet, but that is starting to change,” says Farnum. “We are preparing to receive online contributions and migrate more of our key processes to the network, so our security needs will escalate.”

Menninger needed a comprehensive security solution that could not only provide the intelligent tracking and reporting needed for regulatory compliance, but could also help the clinic actively combat security threats to protect its most important data.

**“Cisco Security MARS helps us to quickly focus on understanding and remediating a network attack, instead of wasting time trying to sift through 20 or 30 separate alerts.”**

— Michael Farnum, Information Security Manager, The Menninger Clinic

## NETWORK SOLUTION

The Menninger Clinic teamed with Troubadour, Ltd., a Cisco® certified partner, to design and build a solution that would deliver the security and reporting tools that it needed. Winner of the Cisco Global Security Partner of the Year Award, Troubadour has extensive experience in helping organizations safeguard critical information and streamline operations.

“Menninger needed a solution that they could rapidly deploy and manage, without adding more employees,” says Jay Kirby, vice president of sales at Troubadour. “Like many customers of this size, Menninger was concerned about controlling its ongoing operational expenses.”

Menninger began deployment of a Cisco Medical-Grade network, a health-industry specific architecture that delivers fully embedded networkwide security to help support regulatory compliance. The solution featured the Cisco Security Monitoring, Analysis, and Response System (MARS), a component of the Cisco Security Management Suite. Ideal for healthcare applications, Cisco Security MARS lets Farnum visually detect and mitigate network threats, while retaining critical data for compliance reporting. Its convenient appliance form factor makes Cisco Security MARS easy to deploy and use, even with Farnum’s small staff.

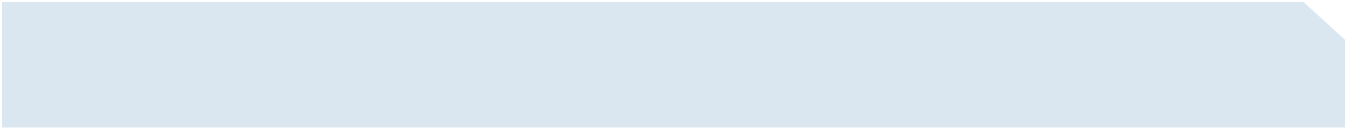
“I needed a device-based product,” says Farnum. “I did not want to have to build a server, harden it, then go through the intricacies of installing software on it. Cisco was the only vendor that offered an appliance-based solution with a set of reports that I could begin using immediately.”

The Cisco Security MARS appliance efficiently aggregates and synthesizes all of Menninger’s network and security data, from Cisco devices and other vendor products as well. It uses intuitive topology maps, intelligent rule creation and threat notification services, and comprehensive reporting systems to track and report attacks in real time. These capabilities streamline and automate Farnum’s compliance tasks of identifying, tracking, and responding to suspicious network behavior.

“The correlation capability and visibility that Cisco Security MARS provides are the most important benefits,” says Farnum. “For example, a worm attack on my Web server might appear as five or six separate attacks, originating from different locations on the Internet. Cisco Security MARS does an excellent job of correlating the data up front, showing that all of these attacks are hitting one of my network devices, and indicating that they are all the same type of attack. It really helps us to identify and respond to threats more quickly.”

To detect and protect the network from outside threats like worms, viruses, and spyware, Menninger also employed the Cisco Intrusion Prevention System, featuring the Cisco 4215 IDS Sensor appliance. Used together with Cisco Security MARS, the solution helps Menninger track and address known security issues—as well as identify new or unanticipated threats that an individual security product might miss. Cisco Security MARS can not only identify a threat, but can also define an action to mitigate it.

“I can use the Cisco Security MARS event manager to set up baseline rules to track any network behavior that looks like an anomaly to me,” says Farnum. “The solution will alert me to network events that fall outside of the baseline—even if it looks like legitimate traffic to all my other defenses.”



For example, many of Menninger's staff work at specific hours of the day or night. Farnum can configure Cisco Security MARS to alert him if server logs show a high number of network logins at an odd hour. This type of unusual activity might go undetected by a standalone intrusion prevention system.

## **BUSINESS RESULTS**

The Cisco Security MARS solution has given The Menninger Clinic unprecedented visibility into its network operations and eased HIPAA compliance. By reducing the complexity of security reporting, the Cisco Solution helps Menninger's small IT staff spend less time trying to document security problems, and more time preventing them.

"Cisco Security MARS helps us to quickly focus on understanding and remediating a network attack, instead of wasting time trying to sift through 20 or 30 separate alerts," says Farnum. "Before we deployed the Cisco solution, I did not have any real-time knowledge of what was happening internally on my network. I knew what was coming in and going out, but did not know what was happening on the inside."

"One advantage is having a single dashboard to report to," says Kirby. "It gives Menninger a very quick view and the ability to address a threat or event that comes up in the dashboard. It is not just a reporting tool for compliance reasons, but also a proactive mitigation tool."

Menninger has had a sterling healthcare reputation since 1925, and the Cisco security solution helps The Clinic maintain the highest level of network integrity and confidentiality.

"Our servers host extremely sensitive data—everything from patient and financial records to donor contact information," says Farnum. "All of our patients require high levels of confidentiality, and at any time a network intruder might actively try to find out who our patients are."

Farnum has found that Troubadour has delivered the support that he needed in designing the new solution and fine-tuning it to support Menninger's specific network applications.

"I have had a great experience with Troubadour as a partner," he says. "They have provided a solution that is as close to turnkey as possible, and have done a great job at teaching me how the solution works, and how I can define my own rules, reports, and alerts."

Because Farnum can manage and support the Cisco solution himself, Menninger can keep its operating expenses down and accomplish more with its existing staff.

"We considered an outsourced solution, and it would have raised our operational costs considerably," he says. "The Cisco solution has turned out to be much less expensive than an outsourced vendor service, and provides a good return on investment from that standpoint."

## **NEXT STEPS**

As Menninger moves additional financial and healthcare applications to its network, The Clinic is considering adding Network Admission Control (NAC) to its network. The Cisco NAC Appliance can authenticate and authorize network users and their machines prior to network access.

Because its Cisco solution can easily grow and change to support new applications like NAC, Menninger already has an advantage for conforming to new regulations such as the Joint Commission on Accreditation of HealthCare Organizations (JCAHO).

"As we migrate to an electronic medical records system, JCAHO regulations will become increasingly important," says Farnum. "Our Cisco network will help us continue to step up security to meet new needs."

## **FOR MORE INFORMATION**

To find out more about Cisco security solutions, visit <http://www.cisco.com/en/US/products/hw/vpndevc/index.html>



## PRODUCT LIST

### **Routing and Switching**

- Cisco 2800 and 3800 Series Routers
- Cisco Catalyst Switches

### **Security and VPN**

- Cisco Security MARS
- Cisco ASA 5500 Series Anti-X Edition
- Cisco IDS 4215 Sensor



**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic  
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy  
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)