



*"The LANShield Controller is giving us places to start to learn what we don't know. It's also helping us know what we should know, such as the traffic between our PACS servers and, more importantly, between the PACS servers."*

## Mercy Medical Center

"Hospitals are a very open environment," says Mark Rein, the senior director of information technology at Mercy Medical Center in Maryland. "And it's a dangerous place for data these days. The only thing we trust within the network is the server core. Everything else is questioned."

The hospital's openness is just one of the security challenges Rein faces. He also has to grapple with the size and distributed nature of the medical provider's operations. The cornerstone is a large complex in Baltimore that includes a 230-bed hospital, an outpatient surgery center, women's health center, physicians' offices, administration offices, and IT. Scattered across the state are numerous physicians' practices, as well as a long-term care facility and a senior housing complex.

Some 3,800 medical users – physicians, clinicians, residents and interns – use the network, all of whom need access to centralized servers and applications such as electronic medical records and practice management software. Unfortunately, the IT team has very little control over certain users, such as those in the physician practices, or the computers they use.

Medical equipment poses another challenge. "I have wireless bar code readers, glucometers, and other modalities like x-ray, MRI, and CT machines," says Rein. "They're not a traditional client so there's no way to do access controls like 802.1X."

The IT team currently has traditional border security deployed, including email security, anti-spam, and anti-virus products. Now the CIO, Jim Stalder, has mandated that they go beyond protecting the perimeter and implement security controls within the network, ones that allow them to be proactive – rather than reactive – in restricting who accesses what. After evaluating a breadth of security products and vendors, Rein has turned to ConSentry Networks, with its LANShield platforms, to help Mercy achieve that goal.

### FIRST STEP: NETWORK ACCESS CONTROL

Priority number one is to identify who's logging onto the network and allow only authorized users to connect. Beyond limiting network access to authenticated users, Rein wants to implement host posture check, interrogating each user's machine for approved operating system revisions, anti-virus software, and other updates. Users who fail posture check would be directed to a remediation server. Those who decline remediation would be given limited network access.



### About Mercy Medical Center

Mercy Medical Center is a thriving hospital recognized nationally for its quality patient care, state-of-the-art facilities, and outstanding medical staff. Mercy has been named one of the nation's Top 100 hospitals, based on quality and performance standards, and was also named one of America's 10 Best Women's Centers. Mercy Medical Center is a teaching hospital affiliated with the University of Maryland School of Medicine and sponsored by The Sisters of Mercy.

### The Challenge

Mercy needed to gain better control over the hospital's very open and geographically distributed network environment. It also needed to deliver on the CIO's mandate to shore up security within the network.

### The ConSentry Solution

With ConSentry, Mercy will be able to deploy Network Access Controls, gain traffic visibility, and enable identity-based control all within a single platform. Richness of features, ease of use, and interoperability with other network and security solutions made the ConSentry LANShield platform attractive to Mercy Medical Center.

Finding the right host posture check solution has been a challenge. Every posture check agent Rein tested interfered with the browser-based viewers employed by many clinical applications and systems, such as the Picture Archive Communication System (PACS). He's interested in ConSentry's dissolvable agent, a clientless posture check implementation, as an alternative to agent-based solutions.

A temporary piece of code, the ConSentry dissolvable agent is downloaded from the ConSentry LANShield platform when a user launches a browser. It performs a complete compliance check on the host, including checking for compliant Windows Service Packs and Hotfix versions; anti-virus compliance checking; spyware detection, disablement, and logging; adware detection; and heuristic- and signature-based security scans. The agent is removed when the user closes his or her browser.

"In some place, like physicians' practices, we have very little control over what they do and how they do it," says Rein. "I want to be able to clientlessly remediate or at least interrogate the person coming into the network. Then after they've come in, I want to make sure it's the same machine that I interrogated before and that nothing else has been added to the machine that can cause a security issue or vulnerability on my network."

Rein's plan is to trial the ConSentry dissolvable agent with a test group of users, and then implement a remediation process for those clients that fail posture check. After the test period, Mercy will move to production deployment and isolate non-compliant clients and provide them with Internet access only.

### **SECOND STEP: TRAFFIC VISIBILITY**

Simply verifying each user and computer isn't enough – nor is it always feasible. The 802.1X authentication specification doesn't allow for the fact that users sometimes change computers, notes Rein. Nor can it support medical gear, such as CT and MRI machines, and other non-PC devices that have no client login.

But lack of support for 802.1X isn't the only issue. Rein also needs a way to see the traffic from these medical devices and ensure that each device accesses only those applications and resources that it's supposed to, such as an x-ray machine only reaching the PACS infrastructure.

"I know that this MRI machine only talks back to PACS using a particular TCP/IP port, and there's a particular type of traffic we can expect from it. So anything different coming from this IP/MAC address to anywhere else on the network is an anomaly – and either somebody has spoofed the MAC address or has taken control of that machine," he notes.

Anomaly detection is a key for Mercy. Understanding normal vs. abnormal traffic flows is fundamental to defining control policies, which is Rein's ultimate goal. "We want to get very, very granular – to where a user sees only those servers and resources on the network that are required to fulfill their job function," he says.

### **THIRD STEP: IDENTITY-BASED CONTROL**

Using ConSentry's visibility capabilities, the IT team is gaining insight into the traffic on their network. Already the team has seen "some weird access between subnets," Rein says. "The LANShield Controller is giving us places to start to learn what we don't know. It's also helping us know what we should know, such as the traffic between our PACS servers and, more importantly, between the PACS servers and all the modalities poured into them. And we're also seeing when backup kicks on and when it completes successfully."

The LANShield Controller's visibility and malware capabilities turned up one major surprise. The IT team decided to scan for malware on the hospital computers, not expect-

*"The LANShield Controller is giving us places to start to learn what we don't know."*

**Mark Rein**, Sr. Director of IT

ing to find any since each production system is scanned at least once a day. Rein was dismayed to discover that even technically inclined members of his own team had malware on their desktops – they knew how to take the anti-virus agent off their systems. “Sometimes you’ve got to keep an eye on the very people you would least expect to be a problem,” he observes.

Once the IT team has a fuller understanding of the traffic patterns on its network, they will begin to implement ConSentry’s identity-based controls. The fact that these controls are integrated with Microsoft’s Active Directory (AD) is important for Mercy.

“We plan to use the visibility information coupled with Active Directory components to allow devices access only to the appropriate server and network resources,” says Rein. “To limit the possibilities of ‘bad’ activities, we will also stop peer-to-peer within the enterprise, with the exception of application-dependent requirements.”

The IT staff at Mercy will also be exploring other ways to use ConSentry’s identity-based controls. For example, they plan to take an aggressive stance toward remote users, stopping their traffic if they see any anomalies. They’re also considering location-based controls – for example, restricting doctors and nurses on the pediatric floor to accessing pediatric-specific resources.

**THE CONSENTRY ADVANTAGE**

Richness of features, ease of use, and interoperability with other network and security solutions made the ConSentry LANShield platform attractive to Mercy Medical Center. “The ConSentry product is further along in the market,” notes Rein.

He also purposely didn’t attend technical training on the product so he could see how much he understood about the system just through the user interface. He was pleased that he could successfully navigate the ConSentry InSight command center – the policy creation and distribution and LAN visibility platform – without this training. “That’s the ultimate sale – when you can go in and take a look at what’s going on and not have to read the manual,” he says.

“One of the strong points ConSentry brings to the table is intellectual capital – they’ve got a really good group of folks,” he adds. And the company’s design principal of delivering security products that are network independent is crucial.

“We have a heterogeneous network, so I need a solution that’s brand agnostic,” Rein notes. “ConSentry is – I can drop it into any environment and it will work.”

*“We have a heterogeneous network, so I need a solution that’s brand agnostic. ConSentry is – I can drop it into any environment and it will work.”*

**Mark Rein, Sr. Director of IT**

**ABOUT CONSENTRY NETWORKS**

The ConSentry Networks Intelligent Switching architecture delivers native user and application control at the LAN access edge. With this technology, ConSentry’s award-winning LANShield switch product family enables IT managers to improve the visibility, control, and performance of users and applications and radically simplify security, LAN deployment and operations. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital and is headquartered in Milpitas, California.

**Corporate Headquarters**  
 ConSentry Networks  
 1690 McCandless Drive  
 Milpitas CA 95035  
**Phone** 408.956.2100  
**Fax** 408.956.2199  
**Toll-Free** 866.841.9100  
 Email [info@consentry.com](mailto:info@consentry.com)  
[www.consentry.com](http://www.consentry.com)

**Worldwide Locations**  
 London, United Kingdom  
**Phone** +44 (0) 00870 351 9494  
 Frankfurt, Germany  
**Phone** +49 69677 33 4  
 Tokyo, Japan  
**Phone** +813 5532 7630

For a complete listing of all our office locations go to:  
[www.consentry.com/company.html](http://www.consentry.com/company.html)

