



“AirTight provides us security and network performance tuning we couldn’t achieve otherwise.”

Troy Wood, sr. network administrator, John C. Lincoln Health Center



**OVERVIEW**  
**JOHN C. LINCOLN**  
**HEALTH CENTER**

A not-for-profit health care provider network that includes two hospitals, several physician practices, and a number of outreach programs for Phoenix area residents.

- **Business Problem:** As its wireless network grew, the center needed to gain control over security and performance to ensure availability, privacy, and on-demand access to patient information.

---

- **Operational Challenge:** John C. Lincoln’s IT team found it difficult to manage 193 wireless access points manually, and attain the visibility needed for optimal security and regulatory compliance.

---

- **Solution:** AirTight® Networks’ SpectraGuard®

## Wireless Security and Performance Management: John C. Lincoln Finds the Cure

### The Challenge.

As this leading health care provider increased its use of wireless technology to streamline care, it needed to find a way to ensure optimal performance and security.

If you’re ever in the Phoenix, Arizona metropolitan area and find yourself in need of medical attention, chances are you’ll visit one of the facilities in the John C. Lincoln Health Network. John C. Lincoln is a not-for-profit network that includes two hospitals, several physician practices, and a number of outreach programs for Phoenix residents. Medical industry watchers consistently have ranked John C. Lincoln among the nation’s best providers, from business ethics to its nursing care.

Its stellar reputation wouldn’t surprise anyone who visited its children’s health care center, emergency and trauma care units, or any of its other facilities that provide wellness and support services. One of the first things you might notice at its hospitals is the lack of computer cables: John C. Lincoln has moved to wireless networking in a significant way.

Currently, facility dietitians use wireless-enabled tablet PCs to take meal orders for patients, while doctors and caregivers use wireless voice-over-IP devices to text and talk quickly throughout the campus. Even crucial medications are delivered and managed via wireless IV pumps. In fact, admission processes from admissions to the patients’ rooms all are managed wirelessly. Additionally, patients and visitors are offered free wireless Internet access so they can access information, check e-mail and stay in touch with their loved ones.

### The Problem—The need for wireless and mobile network integrity

Getting its network — which today includes about 500 wireless devices and 193 access points spread across two facilities — to its current level of high availability, security and performance wasn’t easy. Like many organizations, once Lincoln started deploying wireless devices, growth accelerated nearly exponentially.

“We simply dove in. And we realized quickly that we had no real control over the network, because each access point was set up individually,” says Troy Wood, senior network administrator, information systems. “Before we knew it, we had so many access points set up that the technicians couldn’t keep up.”

#### ABOUT AIRTIGHT NETWORKS

AirTight Networks, the industry standard for wireless vulnerability management, is the only company that offers customers a flexible, end-to-end solution that gives them visibility into their wireless security posture and a choice in how to manage it.

AirTight provides full wireless intrusion prevention systems (WIPS) and the world's first on demand wireless vulnerability management service. AirTight's patented technology delivers the key elements of an effective WIPS to eliminate false alarms, block wireless threats immediately and automatically and locate wireless devices and events with pinpoint precision.

AirTight's customers include global retail, financial services, corporate, education and government organizations.

AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit [www.airtightnetworks.com](http://www.airtightnetworks.com).

With that growth and increased access, Troy grew concerned about potential attacks. "It would have been possible to take two laptops, sit in our facility and bring down access to a considerable part of the network. We'd have no idea where the attack was coming from until the attacker left," he explains. "We had no way to view or control our airspace, and we needed a way to rein in control," says Wood.

That control would be essential not only to protect system availability, but also to protect the security and privacy of patient information, ensure optimal performance and comply with state and federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA).

That's when Wood and his team started investigating potential wireless security and performance management solutions to rein in control. "At first, we didn't know what we needed, because we had no wireless expertise," he says.

#### The Solution—AirTight Networks: Comprehensive Wireless IPS and Performance Management

After a careful evaluation of several wireless management and intrusion prevention vendor offerings, it became clear that SpectraGuard Enterprise, from wireless vulnerability management and intrusion prevention leader AirTight Networks, was the only solution that would get the job done. "AirTight Networks was more established, easier to maintain and could scale better to our needs than the other vendors we evaluated," he says.

AirTight Networks' WIPS solution provides rogue AP and client detection, prevents accidental connections to neighboring wireless LANs, and monitors, identifies and mitigates wireless attacks. In fact, the SpectraGuard Enterprise WIPS delivers levels of protection traditionally associated only with wired networks.

**"That's one of the greatest benefits. We can see every customer who comes into our network, and what he or she did while here. And we quickly can identify and avoid potential performance problems."**

—Troy Wood, senior network administrator, information systems, John C. Lincoln Health Network

"Some of other products we examined simply failed to perform as expected when we installed the number of sensors to the level we'd need. The system just wasn't workable" says Troy. "Then we turned to AirTight Networks and have been very happy with its performance and capabilities ever since," he says.

AirTight Networks' SpectraGuard line of wireless intrusion prevention systems and services provides enterprises around-the-clock wireless monitoring and automatic intrusion prevention. SpectraGuard is the industry's only solution that correctly classifies wireless devices and events and automatically identifies, blocks, and accurately locates wireless security risks and attacks. AirTight Networks' solutions protect both the wired and the wireless networks of organizations of all sizes, whether the need is to enforce a no-Wi-Fi policy, to secure a single laptop or millions of wireless devices. "AirTight provides us security and network performance tuning we couldn't achieve otherwise. Our ability to manage performance and security has increased dramatically," he says.

Essentially, the SpectraGuard architecture consists of a server and wireless sensor devices. The sensors scan the airwaves continuously and provide automatic protection against any unauthorized wireless activities. The system blocks all unauthorized access and rogue traffic without disrupting authorized wireless communication.

Following its deployment of 25 sensors, John C. Lincoln now has the control over its wireless airwaves that it sought initially. The health care provider now can track and record everything that comes across its network. "That's one of the greatest benefits. We can see every customer who comes into our network and what he or she did while here. And we quickly can identify and avoid potential performance problems," he says.

With its SpectraGuard deployment, John C. Lincoln went from near zero visibility on its wireless network to full transparency and control. "That's the big 'wow' factor. We now have complete control."

**Wireless Vulnerability Management**

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043  
 T +1.877.424.7844 T 650.961.1111 F 650.961.1169 [www.airtightnetworks.com](http://www.airtightnetworks.com) [info@airtightnetworks.com](mailto:info@airtightnetworks.com)

© 2008 AirTight Networks, Inc. All rights reserved. AirTight Networks and the AirTight Networks logo are trademarks, and AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. All other trademarks mentioned herein are properties of their respective owners. Specifications are subject to change without notice.

