



## HEALTH SCIENCES CENTER RECOGNIZES NEED TO SECURE WIRELESS AIRWAVES

### Customer Description

The University of Utah Health Sciences Center (UUHSC) officially began with the opening of the University of Utah Hospital in July of 1965. Since then, UUHSC has developed into a variety of facilities including Community Clinics, the School of Medicine, Academic Colleges, and various institutes and centers. UUHSC excels in education, research, patient care and community outreach throughout Utah and the Intermountain West. The Huntsman Cancer Institute, Moran Eye Center, University Neuropsychiatric Institute, Eccles Institute of Human Genetics, University of Utah Orthopedic Center, and Intermountain Burn Trauma Center provide specialized patient care and research that serve Utah, the Intermountain West, and the world. Within the Community Clinics doctors and health care specialists provide outpatient primary care and multi-specialty services in eight health care facilities along the Wasatch Front.

### Problem

Wireless networking in healthcare institutions plays a vital role in healthcare delivery. Each day physicians and other care providers use laptops, PDAs, and wireless terminals to access electronic medical records, reports, medical images, and track vital signs of patients. The security and confidentiality of these records are critical to the care of the patient, but the insecure nature of a wireless network creates an environment where patient data could be transmitted in clear text. UUHSC's concern over wireless network security began nearly three years ago. Fascinated and astonished by a demonstration at a local training seminar in which a wireless signal was extended thousands of feet using a mere Pringle's can as an antenna, UUHSC's Information Security Analysts realized a need to take control of their wireless airwaves. Of additional concern, the Health Insurance Portability and Accountability Act (HIPAA) mandates healthcare entities take security measures to protect "Electronic Personal Health Information" (e-PHI). If e-PHI is not secured properly an institution runs the risk that their protected data could be accessible to hackers, which puts the entity at risk legally. The central IT support for UUHSC provides services to more than 12,000 end users. The wireless network consists of a menagerie of Foundry IronPoint and Cisco access points that stretch throughout the Salt Lake Valley to provide connectivity at most UUHSC sites. Serving the patient, academic, and research community, UUHSC also has several smaller IT groups, which provide various levels of support but nonetheless make decisions about network infrastructure in accordance with their specific needs. UUHSC realized the need to secure their WLAN to ensure patient confidentiality, prevent anonymous attacks, and comply with the regulatory guidelines of HIPAA.

### Requirements

UUHSC needed a solution that would uphold the foundation of information security – criticality, availability and data integrity. Among the requirements UUHSC needed a solution that would enable them to track and easily discover rogue access points, provide visibility into the performance of the wireless LAN in order to improve throughput and efficient channel utilization of the WLAN, track misconfigured APs that were incorrectly routing data and slowing the performance of the network, identify unauthorized people using NetStumbler to sniff for wireless access, and provide a centralized solution to manage a moderately fragmented wireless network.

## OVERVIEW

### Problem

UUHSC needed to secure their patient data in the wireless environment and comply with HIPAA.

### Requirements

A monitoring solution that could uphold their foundation of information security.

### Solution

AirDefense Enterprise

### Benefits

- Continuous network monitoring
- Rogue access point detection
- Performance troubleshooting and intrusion detection



*"AirDefense provides us with the tools, reporting and documentation that will sustain a successful implementation of a WLAN under HIPAA regulations."*

**- Bo Mendenhall**  
Principal Information Security Analyst

# CASE STUDY | Healthcare



## Solution

UUHSC sought a best-of-breed solution, which would ensure patient confidentiality, prevent loss of data integrity and availability while allowing mobility and ensuring compliance with HIPAA. An exhaustive search led them to select a layered approach to security including access point management, authentication and an overlay security monitoring solution to manage and protect the network.

UUHSC selected AirDefense to implement its wireless security and monitoring. AirDefense provided UUHSC with:

- Rogue detection, 24x7 protection for the network to ensure that it maintains the security and mission-critical reliability required in the healthcare environment
- Intrusion Detection, recognition of documented and undocumented attacks including, Identity thefts from MAC spoofing, Man-in-the-Middle attacks, Denial-of-Service Attacks, and Dictionary Attacks.
- Performance Monitoring, analysis of the wireless traffic flow by identifying usage characteristics, interference from neighboring WLANs, channel overlap, and performance degradation.
- HIPAA Compliance Documentation, audit trails of alarm events and response to ensure proper enforcement of policy violations, a sanctioned HIPAA requirement.

## About AirDefense, Inc.

AirDefense is the thought leader and innovator of wireless LAN security and operational support solutions. Founded in 2001, AirDefense pioneered the concept of 24x7 monitoring of the airwaves and now provides the most advanced solutions for rogue WLAN detection, policy enforcement, intrusion protection and monitoring the health of wireless LANs. As a key element of wireless LAN security, AirDefense complements wireless VPNs, encryption and authentication. Based on a secure appliance and remote sensors, AirDefense solutions scale to support single offices, corporate campuses or hundreds of locations. Blue chip companies and government agencies rely upon AirDefense solutions to secure and manage wireless LANs around the globe.

## RESULTS

Deploying AirDefense provided UUHSC visibility into the network resulting in:

- Increased throughput and performance of the network
- Location of out of sequence frames indicating identity theft
- Reduction and identification of rogue access points
- Reduction of and interference from neighboring floors
- Compliance with HIPAA regulations
- Increased efficiency of the IT department

*“AirDefense continues to innovate and provide feature rich functionality that is simply unavailable with other products.”*

**- Bo Mendenhall**  
Principal Information Security Analyst

## AIRDEFENSE DEPLOYMENT

