



AIRDEFENSE HEALTHCARE SOLUTIONS

WIRELESS SECURITY SOLUTIONS FOR HEALTHCARE

AIRDEFENSE WIRELESS SECURITY SOLUTIONS FOR HEALTHCARE

Wireless Local Area Network (WLAN) deployments in healthcare institutions have accelerated as mobility has proven to play a vital role in efficient and accurate care delivery. However, the introduction of wireless technologies has also created a new avenue for data breaches, circumventing traditional security architectures. The Health Insurance Portability and Accountability Act (HIPAA) in the US and similar regulations around the world require healthcare providers to take necessary steps to protect confidential patient information. The AirDefense solution, currently deployed by several large healthcare providers, is designed to secure the provider's wireless airspace by eliminating rogue wireless devices, preventing wireless intrusions and facilitating compliance with policies such as HIPAA. The AirDefense solution also provides centralized wireless troubleshooting capabilities that reduces the WLAN management cost while improving overall wireless performance.

Wireless Risks

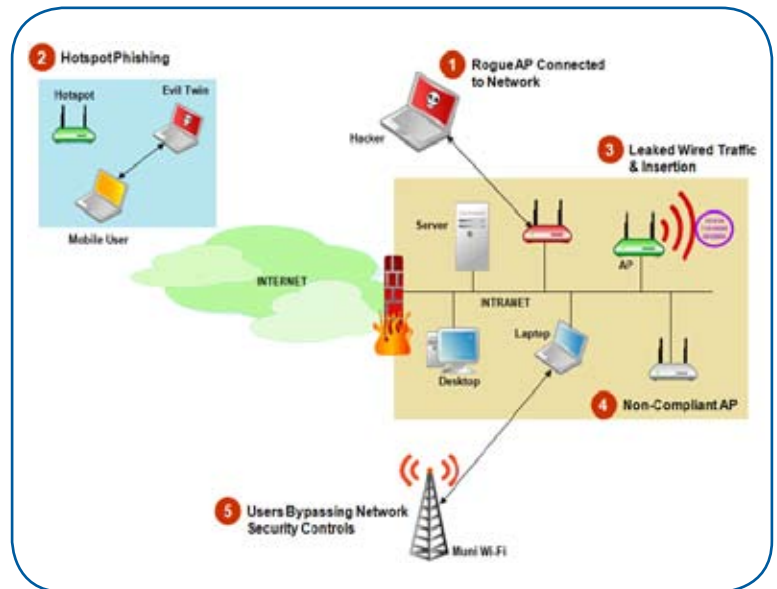
WLANs introduce the following vulnerabilities in a healthcare provider's data network that traditional security solutions cannot mitigate.

Rogue Wireless Devices - A rogue wireless Access Point (AP) is an unauthorized AP physically connected to the wired network. Rogue APs provide attackers with unrestricted access, bypassing firewalls and VPNs, to internal servers just as if they were connected to an internal wired port. Rogue APs can be installed on any network, including networks with no official wireless deployments and networks that have been intentionally segmented from regular wireless networks.

Identity Thefts - A hacker can masquerade as an authorized wireless device and connect to an authorized AP. MAC address based filters are useless since wireless MAC addresses are broadcast and hackers can easily change the MAC address of their device. WEP encryption can be cracked in a few minutes. WPA-PSK is easy to implement and does not have the vulnerabilities of WEP; however, one common key is used between many devices. Hackers have been known to steal portable wireless devices or use social engineering to obtain passwords. Once this common key is stolen or a password compromised, hackers can easily masquerade as an authorized wireless device without having to breach a secure physical perimeter.

Denial of Service Attacks - Hackers can easily perform wireless denial of service (DoS) attacks preventing devices from operating properly and disrupting critical healthcare functions. Wireless DoS attacks can cripple a wireless network despite the use of sophisticated wireless security protocols like WPA2. Hackers can insert malicious multicast or broadcast frames via wireless APs that can wreak havoc on the internal wired infrastructure of a healthcare provider's network.

Non-Compliant APs - Wireless APs and client devices are frequently misconfigured. According to Gartner, a majority of all wireless security incidents will happen as a result of misconfigured devices. Misconfigurations happen for a variety of reasons including human error and bugs in wireless management software. A misconfigured AP at a hospital or a doctor's office can be detected and exploited by a hacker to gain access to the network allowing them to attack internal servers and applications. Poorly configured wireless laptops can be phished and compromised very effectively and with relative ease.



Wireless Security Issues in Healthcare

AirDefense Solution

The AirDefense Enterprise solution is based on patented technology that incorporates distributed smart IEEE 802.11a/b/g WLAN sensors reporting to a central server appliance. The sensors are deployed in the healthcare provider's relevant facilities e.g. hospitals, doctor's offices, etc. They monitor WLAN activity 24x7 in their local airspace and communicate with the AirDefense server, which correlates and analyzes the data to provide scalable, centralized management for security and operational support of the WLAN. Administrators access the system via management console software installed on their computer. AirDefense Personal protects mobile laptops from wireless-specific risks that could expose private data and transactions. It allows centralized wireless access policies to be enforced across all wireless laptops. The AirDefense solution addresses three key areas of healthcare network security and management.

Comprehensive Wireless Intrusion Detection/Prevention – AirDefense Enterprise provides the industry leading solution for rogue wireless detection and containment and 24x7 wireless intrusion prevention. AirDefense Enterprise can accurately distinguish neighboring devices from rogue devices that are connected to the wired network and can be setup to automatically terminate a rogue device over the air. Alternatively, the device can be blocked on the wired side using AirDefense's switch port suppression feature. To find the location of the rogue device, AirDefense provides accurate map based location tracking using signal strength triangulation. AirDefense Enterprise has the largest wireless attack library with over 200 alarms that can detect a range of attacks such as reconnaissance activity, identity theft, session hijacking or Man-in-the-Middle (MITM) attacks, multiple forms of DoS attacks, wired side leakage, dictionary based attacks, etc. AirDefense reduces false positives by correlating wireless and wired side information in conjunction with rich historical context maintained in its forensic database instead of just looking at the present snapshot. AirDefense recognizes documented and undocumented (day-zero) attacks, because it does not rely solely on attack signatures but also on advanced anomalous behavior analysis.



AirDefense Enterprise Solution for Healthcare

Once an accurate assessment of an intrusion is made, AirDefense Enterprise provides wireless and wired termination capabilities to mitigate the threat in real-time.

Wireless Policy Compliance – AirDefense provides healthcare provider's the ability to define granular wireless policies for how WLAN devices should be configured and operated and then monitors all WLAN devices 24x7 to identify when any device deviates from that policy. AirDefense can understand and monitor all WLAN authentication and encryption policies. Further, AirDefense allows network managers the ability to define WLAN device and roaming policies, channel policies for approved channels of operation and usage policies such as approved hours of operation. Upon deploying a WLAN, customers have an expectation for how the network should perform. AirDefense allows network managers to define these expectations for performance and audit the wireless network 24x7 for performance compliance. By statefully monitoring WLAN activity, AirDefense Enterprise maintains a historical database that powers robust forensic analysis and historic trending as well as incident investigation. AirDefense stores over 300 statistics for every wireless device on a minute-by-minute basis. AirDefense can quickly display the time of attack, what entry point was used, the length of the exposure, how much data was transferred, which systems were compromised, etc. HIPAA policy compliance reports are built into AirDefense Enterprise. The reports are available in several formats and can be automatically scheduled and sent to appropriate personnel or manually generated. In addition, AirDefense allows the creation of fully-customizable reports that leverage the forensic data stored by the system and facilitate compliance management against arbitrary policies. AirDefense Personal allows policy enforcement across laptops when they are outside monitored and secure healthcare facilities. AirDefense helps healthcare organizations address the requirements described in section 142.308 of the HIPAA draft standard as it relates to wireless LANs by:

• Security Management and Certification

AirDefense continually monitors the airwaves throughout the enterprise for internal security violations including rogue access points and stations, ad hoc networks, improper configurations and accidental associations. AirDefense provides a continuous review of security policy and vulnerability assessment.

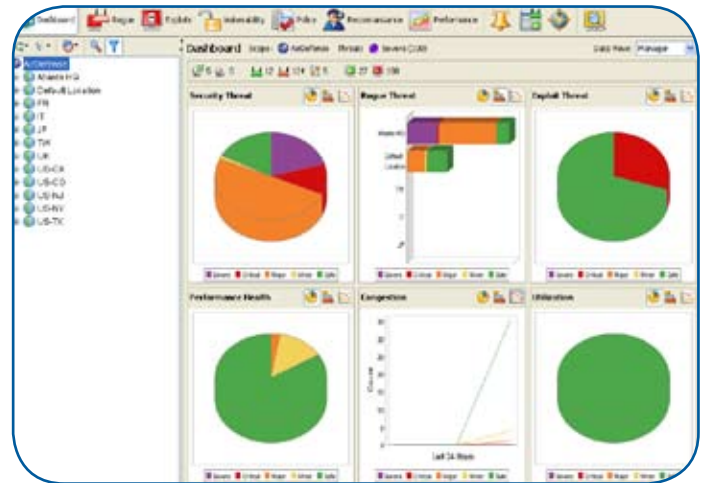
• Security Configuration Management

AirDefense monitors access points to provide real-time equipment inventory and verify that additions or changes to the network do not violate configuration policy.

• Incident Reporting Procedures

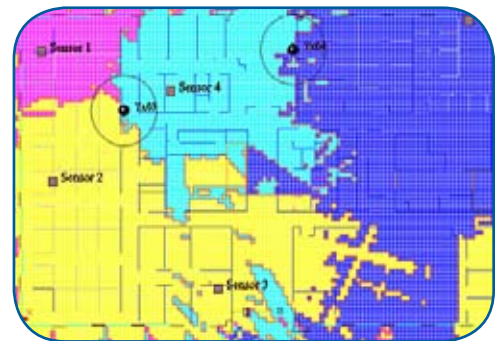
AirDefense immediately detects intruders and alerts security managers of malicious acts, such as NetStumbler scans, spoofed MAC addresses, and “man-in-the-middle” hacking attempts. The alarm can be routed to an email address, pager, or cell phone. Response to the event is logged to track the timeliness and outcome of the event resolution.

AirDefense provides the tools a healthcare organization needs to ensure that the wireless network is secure from unauthorized rogue access points or ad hoc networks, configuration errors or malicious attempts to gain access by exploiting weaknesses in wireless LAN security. AirDefense provides constant enforcement of security policies and immediate notification of violations, along with the information needed to address issues in a timely and effective manner.



AirDefense Dashboard

Remote Wireless Troubleshooting – AirDefense Enterprise can significantly reduce the management cost of wireless networks by providing powerful tools for remote troubleshooting. AirDefense can provide the administrator with a live streaming view of all devices, channels, bands and networks to identify hardware failure, RF interference, network misconfigurations, usage and performance problems. AirDefense can help measure network usage & performance by determining over-utilized APs & channels, pinpointing network congestion, finding bandwidth hogs & analyzing utilization & congestion trends. AirDefense Enterprise features a LiveRF module that provides healthcare network administrators the ability to remotely visualize real-time RF coverage from an application’s perspective and assess the impact of noise and interference on different applications that are using the WLAN. Given the transient nature of RF interference, LiveRF is indispensable for remote troubleshooting of physical layer wireless problems in real-time. AirDefense Enterprise also features a Spectrum Analysis module that can detect and classify common types of RF interference sources such as microwave ovens, frequency hopping phones, Bluetooth devices, etc.



Remote Troubleshooting

About AirDefense, Inc.

AirDefense, the innovator and market leader of anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection. Ranked among Red Herring’s Top 100 Private Companies in North America, AirDefense provides the most advanced solutions for rogue wireless detection, policy enforcement, performance monitoring, troubleshooting and intrusion prevention, both inside and outside an organization’s physical locations and wired networks. AirDefense provides protection for all protocols (802.11 a/b/g and Bluetooth), and enterprises and their mobile users. As a key element of wireless LAN security, AirDefense complements wireless VPNs, encryption and authentication. With Common Criteria certification and FIPS compliant cryptography, AirDefense’s enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.