

# Extreme Networks Healthcare WLAN



## FEATURES

### POINT-OF-CARE APPLICATIONS:



- With mobile applications running over a wireless network, caregivers can verify medication, access patient records, order tests, collect specimens, and more – right from the patient's bedside.

### VOICE COMMUNICATIONS:



- Voice-over-WLAN phones and badges, and Wi-Fi-enabled nurse call systems allow nurses and physicians to easily communicate, roam throughout the facility, and respond to patient needs instantly.

### PATIENT AND EQUIPMENT MONITORING:



- WLAN-enabled medical equipment allows nurses and other staff to monitor a patient's condition and the status of sensitive equipment, such as an IV pump, all in real time – wherever they may be in the hospital.

### SECURE GUEST ACCESS:



- The same wireless LAN that provides mobile voice and data access to healthcare staff can be utilized to provide patient and guest access to the Internet without impacting critical operations or jeopardizing the privacy of your data, ensuring HIPAA compliance while providing a valuable service for visiting family and friends.

## Patient Care Without Wires

In the mission-critical environment of healthcare, delivering the very best in patient care requires doctors, nurses, and other caregivers to be able to instantly reach colleagues and access a wealth of data. With an Extreme Networks wireless LAN solution, you can put 'right here right now' mobile access to voice and data in the pockets of your healthcare team, providing the tools they need at the point of care to define a new level of healthcare excellence.

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 Extreme 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 and network assurance capabilities that reduce WLAN management costs while improving overall wireless performance.

## Healthcare-Ready and Healthcare-Proven Wireless LAN

Just as your patients come to you for the best in healthcare, healthcare providers come to Extreme Networks for best-in-class mobility solutions. And every minute of every day, Extreme Networks delivers. With Extreme Networks, you get the peace of mind that comes from choosing a leading provider who understands the meaning of 'mission-critical' – we offer many years of experience providing critical mobile and network communications solutions for healthcare facilities as well as Fortune 500 companies and public institutions around the world.

Our advanced wireless LAN technology is designed to meet or exceed the needs of healthcare staff, allowing your caregivers to remain focused on the life-saving tasks at hand. Extreme Networks knows mobility – our breadth of experience and patented features provide the resilient, secure, and high-performance wireless connection required in healthcare facilities.

## Powerful Wireless - Built for Complex Healthcare Environments

Healthcare is one of the most complex environments for a wireless network. Many different types of devices, many different types of applications. Many different types of users. Add to this all the metal, glass, hard reflective surfaces, it is complex. These type of environment is ingrained in the DNA of ExtremeWireless WiNG solution.

When you choose Extreme Networks you get a network that is more intelligent, more reliable, more secure, and more manageable, with a reduction in infrastructure requirements and lower operational costs.

Healthcare-grade wireless provides physicians, nurses, and others with a resilient connection as they roam the facility - from the patient's bedside to the halls, nurses' station, to the pharmacy, and more - ensuring continuity of service for phone calls and data applications. Our wireless LAN includes application aware features that deliver voice and data with a difference. Higher quality voice calls, roaming assist that eliminates sticky clients, ensuring your connections are robust and your calls are clear.

### MORE INTELLIGENCE

Extreme Networks delivers a truly intelligent WLAN. With our distributed architecture, every point in your network - every single access point and controller - is completely network-aware, automatically choosing the best possible route for all wireless traffic. Network performance and the user experience are preserved - regardless of whether users are making VoWLAN calls, accessing clinical or operational applications, or using online reference materials.

### UNMATCHED RELIABILITY

Healthcare is a 24x365 business. Downtime is not an option for your healthcare staff. You need to know that the wireless LAN offers the same reliability as your wired network and your desk phone. With an ExtremeWireless solution, you enjoy wireless that simply works. Extreme Networks' wireless LAN automatically detects and seamlessly re-routes traffic around any malfunctioning equipment in your network. Should that access point fail, our management software automatically adjusts the power and channels of neighboring access points to eliminate any gaps in coverage, providing next-generation self-healing - no monitoring required.

### UNMATCHED SECURITY

At Extreme Networks, we understand that protecting the sensitive data and the performance of your wireless solution is critical - which is why we extend beyond the requirements of HIPAA to offer built-in, uncompromising security. Our hardware and software security solutions work together to create a fortress around your wireless network, protecting the wired and wireless network and your data from unauthorized access. The Layer 2 firewall on our access points add an extra layer of protection as your data travels from sender to recipient. And since our WLANs

automatically detect and respond instantly to any wireless threat from rogue devices to network vulnerabilities - security has never been easier nor compliance with government regulations more cost-effective, from HIPAA to PCI.

### UNMATCHED MANAGEABILITY

While the self-healing capabilities of Extreme Networks' adaptive wireless networks automatically spot and address many network problems before they impact service quality, other network issues do require human intervention to troubleshoot and resolve. Extreme's AirDefense Network Assurance solution allows IT to proactively and remotely optimize, identify, and resolve network issues - often eliminating the need to dispatch a technician to the site. The result? Network availability and reliability with minimal management, effort, and cost.

### APPLICATION AWARE: VOICE AND CONTROL

When you choose ExtremeWireless WiNG, you get superior support for advanced applications - a host of integrated capabilities ready to go right out of the box. With support for Voice over WLAN (VoWLAN), healthcare providers can put cost effective mobile voice in the hands of physicians, nurses and staff. Advanced support for VoWLAN enables push-to-talk and more for employees inside the four walls as well as in outside areas.

There are many applications running over your wireless LAN, but how are you managing and controlling them? ExtremeWireless WiNG incorporates application visibility and control for over 1500 applications, providing the granular control you need to prioritize critical applications, while throttling others, or even blocking others, to ensure the most critical applications can run at their required performance.

### LOW TOTAL COST OF OWNERSHIP (TCO)

Our WLANs are designed to minimize infrastructure requirements and management time, lowering the overall cost of purchasing and managing your WLAN. As a distributed architecture, controller services are available at every access point and remote branch office, minimizing WAN utilization and keeping costs low. Security and other policy enforcement is implemented at the network edge, providing a site-survivable network. ExtremeWireless WiNG gives you more license-free native features, from RADIUS servers and firewalls to wireless IPS, VPN gateways, DHCP servers, and zero-port controllers. No need to purchase additional equipment that must be integrated into your network and managed separately, further reducing capital and operational network costs.

### NETWORK SCALABILITY

Extreme's comprehensive wireless LAN portfolio can meet your networking needs, regardless of how small or large your facility's is today - from a long-term care facility to a large hospital campus or multi-facility network that includes hospitals, clinics, and other offices distributed across town, across the country, or around the world. Our wireless networks can easily grow as your organization expands.

## Securing Your Critical Wireless Resource

Hospitals are large, with hundreds, if not thousands of patients, staff, doctors, nurses, and guest. Unfortunately, this creates opportunity for security breaches, attacks, and identity theft. The hospital needs to complement a great wireless network with a great wireless security solution. Below are some of the common security breaches you should be aware of.

### 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 use 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 services 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.

## The Extreme AirDefense Solution

Extreme AirDefense security platform is a well-established leader in wireless network security, identifying up to 199 threat signatures. AirDefense is based on patented technology that incorporates distributed smart IEEE 802.11 a/b/g/n/ac 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.

There are a number of third party comparisons of AirDefense compared to competing solutions, which demonstrate AirDefense superior advantages.

### COMPREHENSIVE WIRELESS INTRUSION DETECTION/PROTECTION

Extreme AirDefense provides the industry-leading solution for rogue wireless detection and containment, and 24x7 wireless intrusion prevention. AirDefense 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 switchport suppression feature. To find the location of the rogue device, AirDefense provides accurate map-based location tracking using signal strength triangulation. 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
- Security Configuration Management
- Incident Reporting Procedures

### 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, and usage and performance problems.

AirDefense can help measure network usage and performance by determining over-utilized APs and channels, pinpointing network congestion, finding bandwidth hogs, and analyzing utilization and congestion trends.

## ONE COMPANY WITH EVERYTHING YOU NEED TO GO WIRELESS

Why choose Extreme Networks to empower your healthcare workers with mobility? Because we cover everything wireless - from hardware and applications to the industry expertise required to plan and deploy mobility solutions designed for a maximum return on investment. When you choose Extreme Networks, you have the assurance that comes with choosing a partner that truly knows wireless inside and out. We hold key wireless LAN patents that enable unique Extreme-Networks-only features that work together to provide "wired" performance levels on the wireless LAN.

Extreme Networks' unmatched wired and wireless portfolio allow us to offer true end-to-end healthcare solutions that provide the simplicity of a single accountable source. In addition to WLAN, our comprehensive product offering includes everything you need to get and keep your network and mobility solutions running at peak performance every day of the year.

For more information on WLAN solutions in healthcare, visit [www.extremenetworks.com/healthcare/](http://www.extremenetworks.com/healthcare/)



<http://www.extremenetworks.com/contact> / Phone +1-408-579-2800

©2017 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see <http://www.extremenetworks.com/company/legal/trademarks>. Specifications and product availability are subject to change without notice. 11253-0317-07