

CASE STUDY

Commercial Enterprise



Global Manufacturer of Healthcare Products Secures Business Critical Wireless Networks

To realize the many benefits of wireless technology, healthcare companies first must address the security vulnerabilities inherent in wireless networks. Strong security is mandated to protect patients and research participants, as well as essential to secure sensitive intellectual property and business information.

Vulnerabilities in 802.11 Limit Use of Wireless

A global manufacturer of healthcare products with over 12,000 employees and revenues over USD3.4 billion per year wanted to expand and upgrade their wireless networks. As with many manufacturing and supply chain operations, this company employed wireless technology for several years, using legacy 900MHz equipment, including DOS-based LXE barcode scanners, since 1998.

While evaluating whether to update their wireless equipment to 802.11-based platforms, they learned about vulnerabilities and other security issues with 802.11 wireless networks. Consequently, rather than updating and expanding, they were forced to adopt a "no-wireless" policy until they could find a real security solution that addresses their security concerns.

Search for Strong, Easily Managed Security

The company needed a strong security solution that would comply with all governing regulations, including HIPAA and SOX (Sarbanes-Oxley), and with FDA requirements. The right solution would allow them to accomplish the following:

- block unauthorized use of the network and bandwidth
- protect against Denial of Service attacks
- prevent lost or stolen devices from accessing the network, an important control mechanism for barcode scanners in an industrial environment.

Because of their investment in legacy wireless devices, the security solution also had to accommodate their existing legacy wireless equipment as well as support new and emerging technology. The ideal solution would be flexible, allowing them to apply different security policies to different types of devices—for example, the ability to require user authentication for laptops but not for barcode scanners, where such a policy is not practical.

The company understood that IPsec was not appropriate for wireless network security, and did not meet their requirement to accommodate DOS-based devices. Other solutions such as 802.1x, LEAP, or PEAP would take time to implement and present interoperability issues.

The Fortress Security Solution Meets All Requirements

When the company's CSO learned about the Fortress security solution from a security-focused reseller, he was immediately impressed with Fortress's ability to secure legacy and future wireless systems. Fortress' three-tiered security design, with its unique device authentication, also met the requirement to quickly act to deny network access to a lost or stolen device.

In addition to meeting all of their security requirements, Fortress provided the lowest TCO because it is so easy to install and manage. Other solutions considered rely on expensive "fat" APs that incur higher management overhead. The company's wireless network currently covers all warehousing and manufacturing areas of the corporate headquarters, supporting over 100 wireless barcode scanners and over 50 wireless laptops. The company plans to extend wireless access throughout the organization, including providing wireless guest access in conference rooms. Fortress' overlay solution provides a practical security solution that works seamlessly with this current wireless implementation and supports upgrade plans. It also remains viable as access points and RF technology change while still minimizing the costs and management burden.

This overlay solution also supports their business organization structure. The corporate IT department defines the security policy for other locations, but does not control what RF equipment other locations purchase. Standardizing on Fortress ensures that strong security is implemented without affecting the autonomy of the facilities throughout the U.S. and in six other countries. The Fortress security solution currently protects the manufacturing facilities in four of six foreign locations, and will cover all six by year's end.

Challenges

- Provide strong security for supply chain and warehouse operations
- Secure both legacy devices and newer platforms
- Provide transparent operation for users
- Support both current and legacy RF protocols (802.11b,g and 900MHz)
- Allow for device authentication
- Offer simple administration and low TCO

Solution

- Commercially available wireless access points
- Mix of barcode scanners, industrial devices and mobile computers
- Fortress Security Gateways
- Fortress Secure Clients for DOS and Windows

Results

- Fortress's overlay security model integrates with all existing technologies and equipment
- Strong FIPS validated security in place for wireless network
- Transparent operation for users
- Simple implementation and administration
- Supply chain and logistics applications run securely with low TCO



For more information about the Fortress product suite for your network:

phone: 813.288.7388

visit: www.fortresstech.com

email: info@fortresstech.com

Fortress Technologies Inc.
4023 Tampa Rd., Ste. 2000
Oldsmar, FL 34677