
**Wireless LAN Security:
Implications for Financial Service
Providers**

Wireless LAN Security: Implications for Financial Service Providers

This white paper will outline the WLAN security needs for all financial service providers to root out all unauthorized wireless LANs, lock down enterprise WLAN deployments, secure the integrity of customer information, and adhere to new industry regulations.

As the next step in the evolution of enterprise networking, wireless LANs are being deployed across all industries for their productivity and cost-saving benefits. However, financial service providers (FSPs) have viewed wireless LANs cautiously. The early security flaws and new regulatory demands have caused the most progressive IT departments to carefully evaluate all risks before deploying wireless LANs.

Even financial service providers that choose not to deploy wireless LANs must address the issue of unauthorized, “rogue” WLANs that are brought in by employees, vendors, and on-site contractors. With or without enterprise wireless LAN deployments, every financial service provider must address wireless LAN security to fully protect sensitive customer information and comply with evolving regulations.

Overview of WLANs

WLANs offer a quick and effective extension of a wired network or standard LAN. With a simple access point attached to the wired network, personal computers, laptops, handheld devices, printers, and other network devices can connect with the wired network at broadband speeds.

Productivity-Boosting & Cost-Saving Benefits

Wireless LAN technology allows untethered workers to connect to the corporate network from a conference room, the cafeteria, or a bench outside the building at broadband speeds. FSPs are quickly deploying new networks without the costs and time of wiring offices and workstations. For just a few thousand dollars a year, an institution can support a few hundred workstations connecting to the network at broadband speeds. Installation can be accomplished in days rather than weeks by simply attaching wireless access points to wired high-speed networks.

Some of the largest financial service providers in the United States deployed wireless LANs for mission-critical applications, such as:

- A new 50-story corporate headquarters using WLANs for employee mobility and reduced network operating costs;
- New branch offices deploy WLANs for a quick installation of the network and flexible design of the office for self-service kiosks; and
- Some banks are even testing methods to connect ATMs with WLAN “bridging” technology.

An Intel study from December 2002 reported that wireless LANs provide workers with an average daily time savings of 0.34 hours per worker for a yearly productivity benefit of \$4,049 per worker.

Business Drivers for Financial Services

Wireless LANs and their related security issues affect a wide range of executives across financial service providers. Chief information officers and IT executives deploy wireless LANs for increased productivity and reduced infrastructure costs. Chief security officers and other IT security managers are concerned about detecting rogue wireless LANs, locking down enterprise deployments, and identifying all wireless intruders.

Regulatory demands place wireless LAN security as a major issue for compliance and audit executives. Even line-of-business executives in areas, such as retail, commercial banking, and wealth management, should be concerned with wireless LAN security. As wireless LANs grow throughout corporate networks, public hotspots, and home Wi-Fi networks, FSP customers are familiar with the technology and potential security threats and are asking their financial institutions how they protect their confidential information from insecure wireless LANs.

WLANs & The GLB Act's Safeguards Rule

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, includes provisions to protect consumers' personal financial information held by financial institutions. While there are three principal parts to the privacy requirements – the Financial Privacy Rule, Safeguards Rule, and pretexting provisions, this white paper focuses on how FSPs should be concerned with how the Safeguards Rule applies to their state of wireless LAN security.

While the GLB Act's Safeguards Rule never mentions Internet security, encryption standards, or wireless LANs, the GLB Act has forever changed the way in which financial service providers address the security and privacy of their customers.

Safeguards Rule Objectives:

- 1.) *Insure the security and confidentiality of customer information;*
- 2.) *Protect against any anticipated threats or hazards to the security or integrity of such information;*
- 3.) *Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.*

(FTC Standards for Safeguarding Customer Information 314.3)

Without singling out any single technology, the Act's Safeguards Rule stated objectives broadly apply to all existing and future technology initiatives for all FSPs, which include:

- Banks, thrifts and credit unions
- Financial advisories
- Non-depository lenders and mortgage brokers/servicers
- Consumer reporting agencies and debt collectors
- Real estates, settlement servicers, tax return preparers, and credit counselors
- Other service providers that receive customer information for financial institutions.

With the stated intention to “to establish standards for (FSPs) to develop, implement and maintain administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information,” the act is broadly defined to keep pace with the perpetual evolution of technology and security threats. FSPs must in turn adjust their IT security programs in light of changes in technology and new or emerging threats.

“Banks are taking privacy very seriously...the whole thing is gigantic...the GLB requires corporations to protect consumer data and is widely considered the most sweeping law melding privacy and security into one integrated mission.”

USBanker, July 2003

In applying the Safeguards Rule’s objectives to all financial service providers, the GLB Act defines five “elements” that can must applied to wireless LAN security for full compliance.

Regulatory Requirement	FSP’s Responsibility for Wireless LANs
1. Designate employee or employees for information security	The committed “owners” of IT security must also be responsible for wireless LAN security and rogue detection.
2. Identify & assess all risks & safeguards	Recognize the risk of rogue WLANs, WLAN policy violations, and insecure WLAN configurations that risk security and exposure of customer privacy.
3. Design, implement, monitor, and test a safeguards program	Implement WLAN monitoring for rogue detection. For WLAN deployments, deploy strong encryption, authentication, and intrusion detection. Report all incidents.
4. Oversee service providers for security and their safeguards compliance	Select partners based on their expertise with financial institutions and their understanding of wireless LAN security.
5. Evaluate & adjust security program based on results of testing & monitoring	Take action to eliminate all WLAN risks and vulnerabilities. Incorporate any changes into WLAN policy and configuration settings.

Table 1: FSP’s Responsibility for Wireless LANs

Element 1: Designate an employee or employees to coordinate your information security program.

(FTC Standards for Safeguarding Customer Information 314.4.a)

While most FSPs already have information security professionals in place, institutions should educate these employees on developing trends regarding wireless LANs security.

Element 2: Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

(FTC Standards for Safeguarding Customer Information 314.4.b)

This section of the Safeguards Rule broadly outlines areas for financial service providers to evaluate for these internal and external risks. Two areas directly apply to wireless LANs:

- Information systems, including network design and information transmission; and
- Detecting, preventing, and responding to attacks and intrusions.

The following sections will outline specific internal and external wireless LAN risks that FSPs must address for regulatory compliance.

Internal Risk: Rogue WLANs

Unauthorized, “rogue” wireless LANs are clearly a foreseeable internal risk to the security, confidentiality, and integrity of customer information. After first making headlines in the press in the spring of 2002, rogue WLANs are widely recognized as one of the top security concerns of any organization – especially those that have not already deployed wireless LANs.

Many Gartner clients have reported the discovery of “rogue” wireless LAN access points that users had set up in the enterprise’s buildings. We know of several instances in which corporate intranets were publicly exposed — in locations with public access and colocated with competitors — by wireless LAN access points hidden by clever users. Such unauthorized access points are common, and their number will increase in the future as they become easier and less expensive for end users to purchase and install.

Gartner, August 2002

Because a simple rogue WLAN can be easily installed by attaching a \$80 access point to a wired network and a \$30 WLAN card to a laptop, employees are deploying unauthorized WLANs when IT departments are slow to adopt the new technology. Other rogue access points come from on-site vendors or contractors who install temporary WLANs for quick and easy network access without thinking about the security implications.

Through year-end 2004, employees’ ability to install unmanaged access points will result in more than 50 percent of enterprises exposing sensitive information through WLANs.

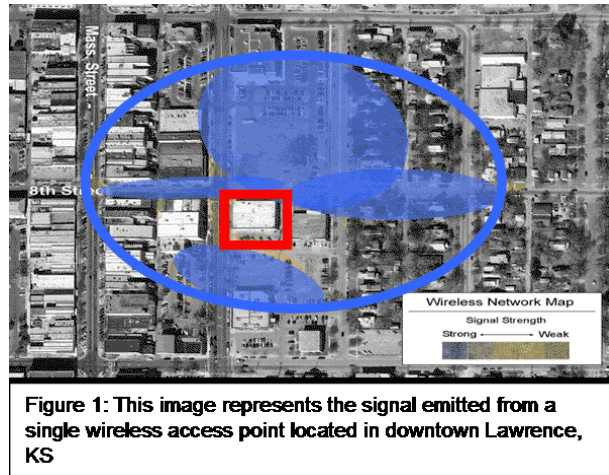
Gartner, September 2002

However, rogue wireless LANs include more than just unsanctioned access points. Other forms of unauthorized wireless LANs include:

- Wireless-ready laptops brought from home that operate in your WLAN airspace and are often in default insecure settings;
- Accidental associates from your wireless stations to neighboring networks;

- Ad hoc, peer-to-peer networking between stations without going through an access point; and
- Soft APs which are actually laptops that function as access points.

All financial service providers – even those without sanctioned wireless LANs – must take action to identify rogue wireless LANs. In regards to compliance, the key is to report the state of security – whether rogues have been found or not – and any follow-up actions.



Internal Risk: Insecure WLANs

Insecure wireless LANs are a recognized security risk. While wireless LANs are often deployed for their productivity benefits, security is often an afterthought. In fact, most WLAN equipment ships with completely insecure settings to ensure that users can quickly get the WLAN up and running. Even wireless LANs that are properly secured upon deployment can be reconfigured by employees looking for easier use of the network. Some hardware has been known to default to their insecure factory settings upon a power surge.

Insecure wireless LANs put FSPs at risk by broadcasting an open connection to an enterprise network. The satellite photo on this page graphically depicts the coverage area of a single access point. How would this affect your financial institution’s regulatory compliance if the access point was not properly secured? Many have referred to this risk as extending an Ethernet cable to the parking lot which then allows anybody who drives by the ability to connect to your enterprise network.

FSPs that have deployed wireless LANs must monitor their WLANs to identify all insecure network settings.

***A firewall costing thousands of dollars can be completely compromised by a single incorrectly configured access point, even when the access point is behind a brick wall.
Network Computing, October 2001***

Internal Risk: WLAN Policy Violations

Similar to insecure wireless LANs, WLAN policy violations are a recognized internal risk to the security, confidentiality, and integrity of customer information. Essentially, an un-enforced WLAN policy can lead directly to insecure wireless LAN configurations and risky WLAN activity by employees that threaten regulatory compliance.

However, it's not good enough to simply have a written wireless LAN policy. FSPs must enforce their WLAN policy to identify policy violations, correct the problem, and take action to prevent recurrence of the violation.

Enterprises must be proactive in establishing policy for the adoption of wireless LANs, given the aggressive rate at which Wi-Fi will appear in corporate laptops and the security threat associated with rogue networks. ... Enterprises must establish corporate policies (relative to infrastructure, usage, and security) on the adoption of Wi-Fi or risk losing network integrity and increasing TCO.

META Group, January 2003

External Risk: Network Eavesdropping

Because wireless communication is broadcast over radio waves, eavesdroppers who merely listen to the airwaves can easily pick up unencrypted messages. Additionally, messages encrypted with the Wired Equivalent Privacy (WEP) security protocol can be decrypted with a little time and easily available hacking tools. These passive intruders put businesses at risk of exposing sensitive information.

For this reason, financial service providers should deploy higher levels of encryption from the developing 802.11i security standard (WPA is a subset of 802.11i) or other proprietary solutions. However, even with improved encryption in place, FSPs should monitor their WLAN traffic for policy compliance

External Risk: Theft of WLAN Credentials

The theft of an authorized WLAN user's identity poses one the greatest threats. Service Set Identifiers (SSIDs) that act as crude passwords and Media Access Control (MAC) addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an access point. Knowledgeable intruders can pick off approved SSIDs and MAC addresses to connect to a WLAN as an authorized user with the ability to steal bandwidth, corrupt or download files, and wreak havoc on the entire network.

Because of the foreseeable threat from "identity thefts" of WLAN credentials, financial service providers must have systems in place to detect, prevent, and respond to these attacks.

Element 3: Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of safeguards' key controls, systems, and procedures.

(FTC Standards for Safeguarding Customer Information 314.4.c)

Information safeguards can be implemented to lockdown wireless LANs with a layered-approach security that includes:

- Perimeter Control;
- Access Control;
- Data Protection; and
- Monitoring and Intrusion Protection.

FSPs that have not deployed wireless LANs should focus on monitoring and intrusion protection to enforce network policies that prohibit WLANs by identifying rogues and eradicating the threat they pose to exposing customer information.

Perimeter Control

Enterprise wireless LAN security begins with perimeter control, which is like installing a firewall to the wired network. Perimeter control for the wireless LAN includes a deployment of enterprise-class access points that offer advanced security and management capability. The wireless LAN should be segregated from the enterprise wired network to allow for wireless-specific management and security policies that do not affect the wired network.

All access points should be completely locked down and reconfigured from their default settings. The SSIDs and passwords of the access points should be changed from their default names. Some FSPs choose to establish set channels of operation for each AP to identify all off-channel traffic as suspicious activity.

Access Control

The next layer of wireless LAN security is to control which stations can access the wireless LAN. Most access points come with simple MAC address filtering that maintains a list of approved stations' MAC addresses. While this is not foolproof, MAC address filtering provides basic control over which stations can connect to your network.

FSPs that rely upon MAC address filtering for access control leave themselves vulnerable to simple identity thefts where a novice hacker can spoof the MAC address of an authorized user and gain access to the network. Larger enterprises with more complex wireless LANs with hundreds of stations and dozens access points may require more complex filtering from remote authentication dial-in service (RADIUS) servers.

Data Protection

Encryption and authentication provide the core of security for wireless LANs by protecting the data as it's transmitted through the unregulated airwaves of a wireless LAN. Vendors of traditional wired-side virtual private networks offer wireless solutions for secure data protection. For FSPs that seek to avoid the

hassle of distributing and maintaining client software as required by a VPN, stronger encryption and authentication is available from vendors such as Cisco, which offers Lightweight Extensible Authentication Protocol (LEAP) and Protected Extensible Authentication Protocol (PEAP).

A new industry standard, Wi-Fi Protected Access (WPA) as a subset of 802.11i, emerged in the spring of 2003 to replace WEP as the encryption and authentication standard.

WLAN Monitoring & Intrusion Protection

The final layer of wireless LAN security requires monitoring to identify rogue WLANs, detect intruders and impending threats, and enforce WLAN security policies. Monitoring wireless LANs for compliance, risk, and effectiveness of security solutions is much different than monitoring typical wired networks. Because WLAN security threats are exposed through the air FSPs must monitor the airwaves to detect these risks.

Real-time, 24x7 monitoring of wireless LANs can only be provided with a distributed system of remote sensors that passively monitor all WLAN activity and report back to a central appliance that analyzes the traffic for threats, attacks, and policy violations. This approach scales to support wireless LANs in a single office or hundreds of access points in dozens of locations around the world.

Element 4: Oversee service providers by:

- 1.) Taking responsible steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
- 2.) Require your service providers by contract to implement and maintain such safeguards.

(FTC Standards for Safeguarding Customer Information 314.4.d)

FSPs should require their current service providers, with whom the FSP exchanges customer information with, to possess the same level of security safeguards, or higher, with regards to both wired network security and wireless LAN security. FSPs should also add Safeguards Rule compliance to their evaluation criteria in choosing such new service providers. Some specific examples include outsourced “core” back-end processors, check printing vendors that receive customer’s name, account and address information, credit card processors, financial statement fulfillment vendors and hosted internet banking providers to name a few.

Element 5: Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph C of this section: any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(FTC Standards for Safeguarding Customer Information 314.4.e)

FSPs should take action to respond to and remediate wireless LAN security risks identified by the monitoring requirement. Policies and procedures should be in place to define what actions should be taken to deal with employees who break the policy. As FSPs address various aspects of security and GLB-Safeguards rule compliance, testing and monitoring the system is a key part in doing so. However, remediation must be done in a timely manner and in accordance to the identified threat.

While a financial service provider may choose to delay its deployment of WLANs, the FSP still must monitor its airspace for rogue activity of unauthorized access points or accidental associations of the FSP's WLAN-ready laptops connecting to neighboring networks. Once an effective monitoring system is put in place and identifies such previously unknown activity, the FSP must address how to manage and control the activity with appropriate policy and continued monitoring to enforce and adjust policy continuously.

The AirDefense Solution

AirDefense solutions provide financial service providers with systems that address their wireless LAN security needs to root out all unauthorized wireless LANs, lock down enterprise WLAN deployments, secure the integrity of customer information, and adhere to new industry regulations.

AirDefense provides this comprehensive solution with an innovative approach to wireless LAN security and operational management that is based on a distributed architecture of remote sensors to monitor the airwaves for all wireless LAN activity and report to a centrally managed server appliance.

The remote sensors are equivalent to wireless scanners but add 24x7 monitoring to provide 100 percent coverage against policy violations. The coverage area of the sensor varies upon the topology of the physical area, but a sensor typically provides a coverage area of 40,000 to 60,000 square feet of a standard office building. All wireless LAN activity is captured and reported to the backend server which analyzes the wireless traffic for policy violations, intruders, attacks, and the overall health of the WLAN. AirDefense then alerts IT network and security managers with an email or message to an electronic pager.

Rogue Detection

Because new risks can arise with the easy deployment of unauthorized Access Points or an intruder driving into the parking lot, WLANs must be constantly monitored for new unauthorized 802.11 devices. AirDefense provides 24x7 vigilance to identify rogue wireless LANs the minute they appear in your airspace.

Intrusion Detection & Protection

AirDefense provides the greatest level of WLAN security with effective measures that include 24x7, real-time monitoring of wireless networks, intrusion detection, attack prevention, and forensic auditing.

By statefully monitoring WLANs in real time, AirDefense provides critical information regarding suspicious or late night activities, unauthorized stations scanning your network, and attacks against your WLAN stations and access points.

AirDefense is designed to accurately detect:

- Identity theft – By stealing an authorized MAC address, an intruder has full access to the network. However, AirDefense tracks the digital “fingerprints” – vendor-specific characteristics and personal trademarks – of authorized users to identify intruders in the network.
- Denial-of-Service (DoS) attacks – AirDefense quickly recognizes the early signs and protocol abuses of a DoS attack that jams the airwaves and shuts down a WLAN.

- Man-in-the-Middle attacks – By posing as an Access Point, intruders can force workstations to disassociate from authorized Access Points and route all traffic through the intruder. The intruder can then gain access to the network by posing as an authorized user and simultaneously operating on multiple channels. AirDefense detects man-in-the-middle attacks by ensuring that Access Points only operate on set channels and proper protocols are used.

By monitoring wireless device traffic, AirDefense can isolate, prevent, or mitigate network intrusions and subsequent downtime.

InfoWorld, March 2003

AirDefense recognizes these and other attacks and can eliminate any direct attacks by using automated protection technologies. AirDefense integrates with enterprise WLANs and can command an Access Point to drop its connection to a malicious station.

AirDefense provides a forensic database to audit a WLAN with a minute-by-minute report on the status of each Access Point and wireless station. AirDefense documents all information it gathers into a relational database that becomes a source of detailed traffic history. The database can pinpoint which systems were targeted with what type of attack and can provide the play-by-play detail of how the attack occurred and can track if the attacker had previously visited the network for reconnaissance or a prior attack.

Policy Enforcement

With 24x7 monitoring of all WLAN activity, AirDefense powers enterprises to enforce WLAN policies to maximize network performance, and reduce exposure to inherent security flaws of 802.11 wireless LANs.

The policy manager is used to define, monitor, and enforce business rules for WLANs such as:

- Off-hours traffic – Notify security managers of late-night traffic.
- Ad hoc networking – Prohibit the use of this common feature where standard wireless networking cards can easily be configured to establish direct laptop-to-laptop connections without an Access Point.
- Channels – Limit Access Points to operate only on authorized channels.
- SSIDs – Prohibit unmasked broadcasts of Service Set Identifiers.
- WEP usage – Require all WLAN traffic to be encrypted with WEP.

Once a policy violation is identified, AirDefense can use its automated protection technologies to enforce most policies by reconfiguring network devices or commanding an Access Point to disconnect from a station that violates the WLAN policy.

Health Monitoring & Operational Support

By constantly monitoring wireless activity, AirDefense provides a comprehensive solution to monitor the health of the WLAN and provide operational support that maximizes network performance. AirDefense gives network administrators a complete survey of the network to troubleshoot problems, make better decisions, and plan for future implantations and upgrades.

Threshold monitoring enabled me to see the overall health of my deployed access points so I would know if I needed to deploy more access points in a certain area to alleviate wireless bottlenecks or if there was a possible access point failure that otherwise would have gone unnoticed.

Federal Computer Week, April 2003

AirDefense's WLAN management functionality is based upon:

- WLAN network view & characteristics – AirDefense gives network managers a real-time view of a WLAN with detail into network usage and inventory of Access Points and stations. Network administrators are given a survey of all authorized Access Points and stations and quickly view any new users, network failures, or new security threats.
- Fault diagnostics – A key management feature includes fault diagnostics that track CRC errors from failed connections, interference from neighboring WLANs, network misconfigurations, and a complete history of network and station failures. Rather than manually backtracking through the last known actions before failure, network administrators are given detailed information on exactly what happened leading up to the problem.
- Performance monitoring – Information gathered allows network administrators to monitor performance of WLANs by identifying usage characteristics and bandwidth hogs who tie-up the network with capacity-draining activities, such as trading MP3 files. Appropriate actions can then be taken to curb such network abuses and boost network performance.
- Capacity planning – With historical data of network usage related to individual Access Points and the overall WLAN, administrators can plan for appropriate network capacity by monitoring network usage over time to make better decisions for adding additional Access Points or wired-end capacity.

Overall system reporting is the key benefit of AirDefense, not only as an aid to security auditing but as a troubleshooting and performance-planning tool. ... I am not aware of any other WLAN product that provides the same level of detail and flexibility for reporting.
Network Computing, May 2003

Alarms & Reports

AirDefense includes a highly accurate alarm manager to alert IT administrators and security managers to identified rogue WLANs, intrusions and attacks, policy violations, and performance issue. The alarm manager intelligently filters and aggregates events. Alarms can be sent via email, page, or SNMP traps to other network management applications.

Detailed reports are provided to document and summarize all network activity. AirDefense comes with dozens of default reports and allows users to customize their own reports to query for specific information.

The State-Analysis Engine and Multi-Dimensional Detection Engine power AirDefense's core functionality to discover wireless LAN vulnerabilities, protect against intruders and attacks, and manage the wireless network.

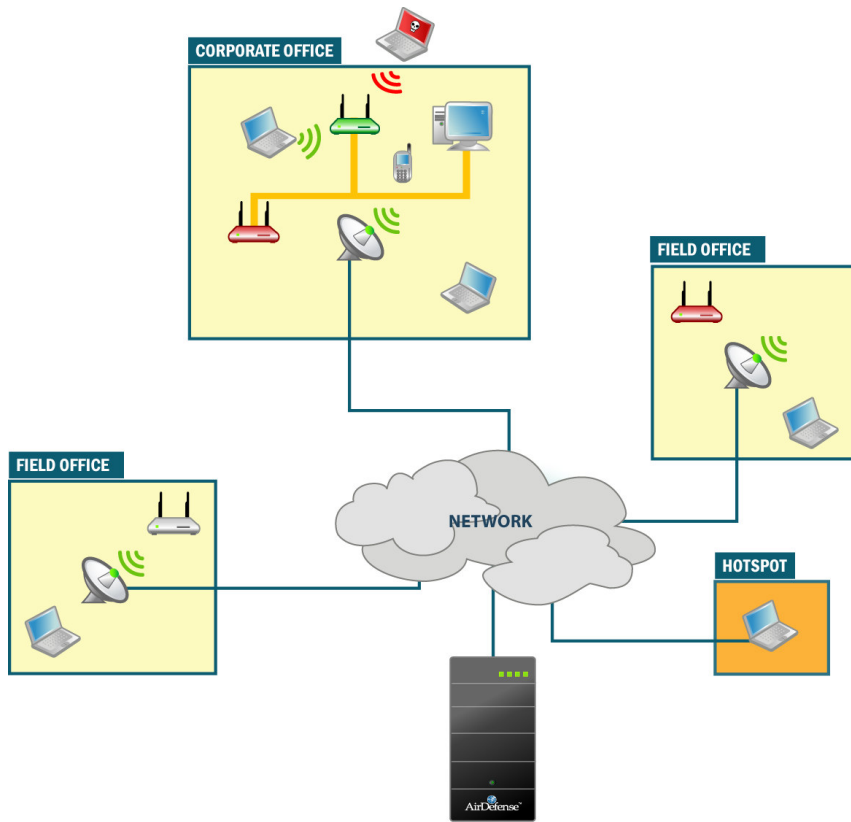


Figure 2: AirDefense Deployment Diagram

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. **All trademarks are the property of their respective owners.**