

---

**Three Steps for Bullet-proof Wireless  
LAN Security & Management**



## Three Steps for Bullet-proof Wireless LAN Security & Management

*The only way for organizations to fortify their wireless networks is to use a layered approach to security mirroring the security of wired networks. This white paper will cover a systematic approach to secure all network components. This layered approach includes: locking down the wireless LAN's perimeter, securing communication across the wireless LAN and continuously monitoring network traffic.*

While a wireless LAN can be installed by simply plugging an access point into an Ethernet port, an enterprise wireless LAN deployment requires a more thought-out plan that incorporates advanced security and management technologies.

### **Layered Approach to WLAN Security**

Over the last year, analysts and media have documented and publicized vulnerabilities of wireless LANs, such as encryption that can be broken and rogue access points that allow intruders to connect to your network. These reports focus on breaking encryption, the risk of unauthorized access points connected to the wired network, and the failure of enterprises to incorporate security into their wireless LANs. The attention on the pitfalls of wireless LANs has inspired some enterprises to ban wireless LANs altogether, but any organization that utilizes laptop computers faces the risk of these easily becoming wireless stations that introduce security risks.



Figure 1: Layered Approach to Security

However, security-conscious enterprises are fortifying their wireless LANs with a layered approach to security that resembles the accepted security practices of wired networks. This layered approach to security addresses all network components:

1. Secure Wireless LAN Devices
2. Secure Communications
3. Monitor for Security & Compliance

In fact, Gartner outlined the three “must have” requirements for enterprise wireless LANs:

1. Install a centrally managed firewall on all laptops that are issued wireless network interface cards or are bought with built-in wireless capabilities. This protects against ad hoc WLAN connections and Internet attacks when users connect to public “hot spot” Internet providers.
2. Perform wireless intrusion detection to discover rogue access points, foreign devices connecting to corporate access points and accidental associations to nearby access points in use by other companies
3. Turn on some form of encryption and authentication for supported WLAN use.

## 1. Secure Wireless LAN Devices

Like installing a door on a building to keep passersby from wandering in, enterprises must control the perimeter of their enterprise networks. For the traditional wired LAN, this was accomplished by installing firewalls to control the entry point to the network. However, wireless LANs present greater challenges from the hard-to-control nature of radio transmissions

*"The use of wireless LANs and mobile workforce is on the rise; so is sophistication of wireless threats and attacks. Mobile users could get duped by hackers phishing for credentials or other sensitive information at hotspots and must be protected."*

Gartner

Perimeter control for the wireless LAN starts with deploying personal firewalls on every wireless-equipped laptop and also includes a deployment of enterprise-class access points that offer advanced security and management capabilities. The wireless LAN should be segregated from the enterprise wired network as part of a VLAN 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 organizations choose to establish set channels of operation for each AP to identify all off-channel traffic as suspicious activity.

To secure mobile users at hotspots etc, organizations can deploy the **AirDefense Personal** product. An industry first, AirDefense Personal protects mobile users of hotspots and other public Wi-Fi networks from wireless-specific risks that could expose private data and transactions. AirDefense Personal is a software agent that runs on Windows PCs and monitors for malicious or accidental wireless activity and wireless misconfigurations that may cause security exposures or policy

violations. The AirDefense Personal agent offers protection from a broad and growing set of new risks that directly target vulnerable wireless users and unobtrusively notifies the user when risky activity occurs.

**Table 1:** Data Protection Technology

Data Protection Technology	Description
<b>WEP</b>	Wired Equivalency Privacy – Original security standard for wireless LANs. Flaws were quickly discovered. Freeware, such as WEPCrack, can break the encryption after capturing traffic and recognizing patterns in the encryption. <i>(Industry standard)</i>
<b>802.1X</b>	As the IEEE standard for access control for wireless and wired LANs, 802.1x provides a means of authenticating and authorizing devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network. University of Maryland professor published vulnerabilities in early 2002. <i>(Adopted industry standard)</i>
<b>LEAP</b>	Lightweight Extensible Authentication Protocol – Based on the 802.1x authentication framework, LEAP mitigates several of the weaknesses by utilizing dynamic WEP and sophisticated key management. LEAP also incorporates MAC address authentication as well. <i>(Developed by Cisco)</i>
<b>PEAP</b>	Protected Extensible Authentication Protocol – Securely transports authentication data, including passwords and encryption keys, by creating an encrypted SSL/TLS tunnel between PEAP clients and an authentication server. PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs. <i>(Developed by Cisco, Microsoft, and RSA Security)</i>
<b>WPA</b>	Wi-Fi Protected Access – Subset of the future 802.11i security standard. Designed to replace the existing WEP standard. WPA combines Temporal Key Integrity Protocol (TKIP) and 802.1x for dynamic key encryption and mutual authentication. <i>(Industry standard adopted in 2003)</i>
<b>TKIP</b>	The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. <i>(Industry standard)</i>
<b>WPA2</b>	WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi® users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

## 2. Secure Communication – Authentication & Encryption

In deploying secure wireless LANs, IT security and network managers face the most difficult decision in choosing how to secure WLAN communication with multiple forms of authentication and encryption.

Like installing locks and keys on a door to control who can enter, the next layer of wireless LAN security is to control which users can access the wireless LAN. To provide basic authentication, most access points support 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.

Organizations that rely upon MAC address filtering for access control leave themselves vulnerable to simple identity thefts as mentioned in Chapter 2. Larger enterprises with more complex wireless LANs with hundreds of stations and dozens of access points require more sophisticated access control through incorporating remote authentication dial-in service (RADIUS) servers. Cisco Systems, Microsoft, and Funk Software are recognized leaders in this area.

In regards to industry standards, the IEEE introduced 802.1x to provide port-based access control, which incorporates a central authentication server. However, some versions of 802.1x have been shown to be vulnerable to hackers. (See “An Initial Security Analysis of the IEEE 802.1x Standard” a paper by University of Maryland professor William Arbaugh.) Cisco introduced Lightweight Extensible Authentication Protocol (LEAP) as a proprietary authentication solution that is based on 802.1x but adds proprietary elements of security. LEAP has its own security issues, and Cisco is moving away from LEAP toward Protected Extensible Authentication Protocol (PEAP).

Encryption provides the core of security for wireless LANs by protecting the data that crosses the airwaves. However, fail-proof encryption and authentication standards have yet to be implemented. Temporal Key Integrity Protocol (TKIP) has been introduced to address the flaws of WEP with per-packet key mixing, a message integrity check and a re-keying mechanism.

New industry standards and proprietary solutions are now being introduced to handle both encryption and authentication. Cisco, RSA Security, and Microsoft developed PEAP as one of these proprietary solutions. However, Microsoft and Cisco have separated their PEAP development efforts and introduced their own versions of the protocol. Microsoft's version of PEAP does not work with Cisco's version of PEAP. While Microsoft is bundling its version of PEAP on the desktop, Cisco's version of PEAP requires client software to be installed and managed on each WLAN user stations.

*“WPA access points must be configured to disable legacy WEP security because the access points may still accept WEP client connections ... Security is handled in the access point, reaffirming the need for validation of access-point implementation”*

**Gartner**

In April 2003, the Wi-Fi alliance launched Wi-Fi Protected Access (WPA) as a subset of the future 802.11i security standard based on TKIP. Most vendors have announced that existing access points can be upgraded to support WPA with a firmware upgrade. However, new access points will be needed once 802.11i is finally ratified.

Virtual Private Networks or WLAN gateways provide another alternative to standards-based encryption and authentication. Traditional firewall and VPN gateway vendors, such as Check Point

and NetScreen Technologies, offer VPNs that funnel all traffic through their existing VPN gateway. These VPN solutions are generally IPSec based and do not work well with wireless LANs where users roam between access points or signals may vary and drop off, which forces the user to re-authenticate and begin a new session.

Vendors, such as Bluesocket, ReefEdge, and Vernier Networks, offer wireless LAN gateways that include added features for network roaming and bandwidth management that are tailored to wireless LANs. Another segment of wireless VPN vendors, including Fortress Technologies and Granite Systems, offer more secure solutions with Layer 2 encryption.

While VPNs provide strong encryption and authentication, most require client-side software, which introduces management headaches.

### **3. Monitor for Security & Compliance**

Like a video camera that monitors all activity in a secure building 24 hours a day, a critical layer of wireless LAN security requires monitoring of the network to identify rogue WLANs, detect intruders and impending threats, and enforce WLAN security policies.

As an example of the need for monitoring, access points that are upgraded for WPA must be monitored to ensure the access point remains properly configured, according to Gartner.

WLAN monitoring must scale to fit the specific needs of an enterprise. Some piece-meal solutions work for smaller organizations but do not scale for large enterprises with dozens or hundreds of locations around the world. Large enterprises require a cost-effective solution that can be centrally managed and does not overtax personnel resources.

Manual site surveys are particularly unreasonable for enterprises operating dozens of offices around the country or retailers with hundreds of stores. Even if these organizations could feasibly devote a network administrator's full attention to survey each site on a daily, weekly, or monthly basis.

Wireless LAN security experts advocate 24x7 monitoring of the airwaves to secure wireless LANs by identifying rogue WLANs, detecting intruders and impending threats, and enforcing WLAN security policies.

*"To truly secure wireless LANs, enterprises must monitor their airwaves to detect intruders and threats that can come from unscrupulous hackers and well-meaning employees. Monitoring the airwaves of a wireless LAN is an essential element of security that should also include advanced encryption and authentication."*

**Gartner**

### ***Functionality Requirements of a 24x7 Monitoring Solution***

The 24x7 monitoring solution should be able to provide the following functionality:

- Ears and Eyes of the airspace
- Rogue Detection & Mitigation
- Intrusion Detection
- Active Defenses

- Policy Enforcement
- Forensic & Incident Analysis
- Fault Diagnostics & Health Monitoring

The self-deploying and transient nature of wireless networks often results in devices connecting with each other and forming ad hoc networks, accidental associations, and malicious associations. It is important for the monitoring solution to be able to provide a **complete view into the wireless airspace** including all devices (APs, stations, PDAs, wireless printers, etc.), relationships and behavior.

Also another challenging and widespread issue is the increase in rogue wireless devices like soft APs, wireless-enabled laptops and neighboring wireless networks that may bleed over, combining hostile rogues with friendly or unconnected devices. The monitoring solution should **detect all rogue devices** and associations. It should be able to analyze all communications including data transfer, time connected, assess the level of threat and protect against them.

As wireless networks proliferate, the ever-present danger of new, more sophisticated hacking tools is also on the upswing. Hackers, armed with new tools are launching more sophisticated attacks on the network -- networks that a year ago were said to be unbreakable. The monitoring solution should utilize its 24x7, real-time monitoring of 802.11a, 802.11b, and 802.11g protocols for the **most accurate intrusion detection of known and unknown attacks**. With stateful monitoring of all wireless LAN activity and multiple detection technologies (discussed in detail in the next section) anomaly, and policy violations, the solution should identify all Day Zero and documented threats including network reconnaissance activity, suspicious WLAN activity, impending threats, and attacks against the wireless LAN.

Monitoring solutions are not only responsible for detecting the existence of threats but also for **mitigating those threats**. Wireless intrusion prevention systems must immediately disable the true rogue devices by any method possible, and they must have the option of terminating the devices automatically. This implies two critical requirements: 1) accurate threat analysis to ensure that the administrator is terminating an access point connected to the network and 2) reliable and accountable termination methods that cripple the rogue device.

After first ensuring that the network is up and running, network managers must then analyze the performance of a wireless LAN to guarantee a maximum return on investment. Real-time monitoring of the airwaves identifies performance issues that can only be seen from the air, such as signal degradation from channel overlap, frequency interference from non-802.11 devices, and excessive overloading of an access point. IT managers should be alerted if there are policy violations in the areas of network usage, WLAN configuration, security and network performance. Examples of alerted policy violations include: network roaming, unencrypted traffic, off-hours traffic, unsanctioned hardware, etc.

By statefully monitoring all wireless LAN activity, the monitoring solution must maintain a historical database to power robust forensic analysis and historic trending, as well as incident investigation.

With a real-time view of all WLAN traffic and detailed traffic analysis, the monitoring solution must assist network managers to remotely troubleshoot problems, identify and respond to network misconfigurations and check for network availability.

## ***Technology Requirements of a 24x7 Monitoring Solution***

Traditional intrusion detection systems are plagued by false positives because they rely on a single detection technology – mostly attack signatures. Advanced intrusion detection should be based on **multiple engines** namely:

- Signature Recognition
- Policy Compliance
- Protocol Analysis
- Statistically Anomalous Behavior

Signatures are used to identify documented attacks as the WLAN monitoring system recognizes intrusions by their defined markings or the vendor-specific fingerprints. Policy compliance is determined on a customized basis for acceptable behavior for each device. Protocol analysis identifies attacks and threats that are not previously documented based on how an intruder breaks 802.11 protocols of communication. By identifying statistically anomalous behavior, the monitoring system alerts an enterprise to unusual behavior, such as a 10 MB file transferred from the wired network to a wireless station at 3 a.m.

Additionally the monitoring solution should **correlate events across the network and its intrusion detection engines**. By correlating WLAN traffic across multiple intrusion detection technologies, the solution reduces false positives while providing more accurate results.

**AirDefense** pioneered the concept of 24x7 monitoring of the airwaves. AirDefense Enterprise is the industry's first Self-Managing wireless Intrusion Prevention System (IPS) and now provides the most advanced solutions for:

- Accurate Intrusion Detection
- Advanced Rogue Management
- Active Defenses and Automated Protection
- Policy Monitoring & Enforcement
- Forensic & Incident Analysis
- Remote Troubleshooting

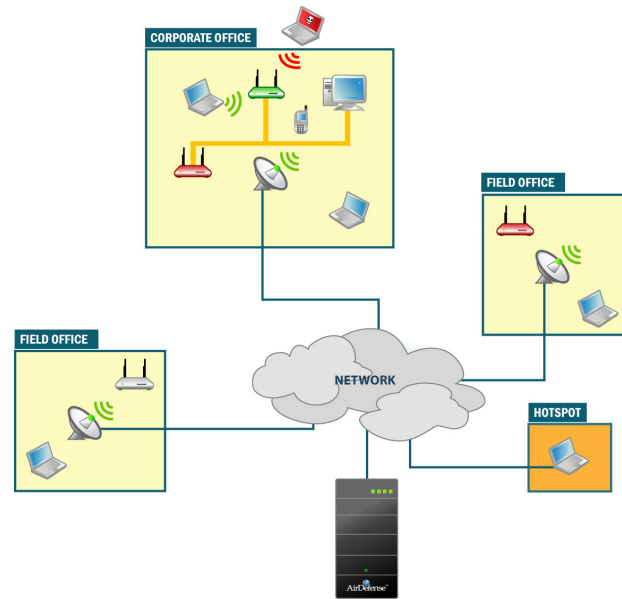
With a distributed architecture of remote smart sensors that work in tandem with a secure server appliance, AirDefense monitors all wireless LAN activity in real time for the highest level of security, policy enforcement, and operational support. While AirDefense proactively notifies IT personnel of alarms for security threats, policy violations, and performance issues, the system also allows for network administrators to access a single interface for a complete view of the wireless devices and access to management-critical intelligence. The system also enables IT managers to take action either on-command or via pre-defined policy-based termination to eliminate the threat presented by rogue devices.

The AirDefense Enterprise system provides the most comprehensive and accurate detection of all threats and intrusions. With more than 200 alarms, AirDefense has integrated protection for every known and Day Zero wireless security threat.

AirDefense provides the most comprehensive rogue management capabilities. The solution automatically detects and analyzes all rogue devices and pinpoints those that present the highest level of threat. Using our patent-pending technology, AirDefense has the ability to distinguish a rogue

connected to the internal network. With minimum intervention, this empowers security managers to confidently use AirDefense mitigation tools to eliminate the threat either on-command or automatically.

AirDefense not only detects all intruders and rogue devices in an enterprise's airwaves, but allows them to actively protect and respond to threats manually or automatically by predefined policies. AirDefense uses multiple methodologies to ensure that the wireless network is secure and protected.



**Figure 2:** AirDefense Deployment Diagram

AirDefense allows organizations to manage and enforce customized wireless LAN policies based on the desired security and acceptable uses for each WLAN device. These security and usage policies are defined under configuration, authorized devices, performance, vendor, and channel policies. Management-approved policy templates can be applied globally or to subsets of the network.

With a single click, administrators have the ability to review the conditions under which an event occurred or measure exposure after a security event. Records of device activity, connection history, traffic volume, traffic direction, and other details are available.

With a real-time view of all WLAN traffic and detailed traffic analysis, AirDefense assists network managers to remotely troubleshoot problems, identify and respond to network misconfigurations and check for network availability. AirDefense can provide the administrator with a live streaming view of all devices, channels, bands and networks to identify: hardware failure, network interference, network misconfigurations and usage & performance problems.

The architecture provides the secure foundation for AirDefense to offer a scalable and manageable solution for wireless LANs in a single office, a corporate campus, or hundreds of locations around the globe. Trusted to monitor over 1 million wireless devices in the Fortune 500 and government organizations, AirDefense instills enterprises with the peace of mind of a secure, risk-free wireless network.

**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](mailto:info@airdefense.net) or call us at 770.663.8115. **All trademarks are the property of their respective owners.**