

**Wireless Security:
Ensuring Compliance with HIPAA, PCI,
GLBA, SOX, DoD 8100.2 & Enterprise
Policy**

Wireless Security: Ensuring Compliance with HIPAA, PCI, GLBA, SOX, DoD 8100.2 & Enterprise Policy

This paper is designed to guide network administrators and security managers to design, implement, and enforce wireless LAN security policies that enable every organization to fully reap the benefits of wireless LANs without experiencing undue management pains and security holes. This paper will also cover how organizations can comply with regulatory policies like HIPAA, PCI, GLBA – Safeguards Rule, DoD 8100.2, Sarbanes-Oxley Act etc.

Enterprises of all sizes are deploying wireless LANs for their many productivity and mobility benefits that come from employees seamlessly connecting to IT resources and performing daily tasks without requiring a wired connection. But just like wired networks, 802.11 wireless LANs require network policies that are designed, implemented, and enforced to maximize network performance and reduce exposure to the inherent security flaws in 802.11 wireless LANs.

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

The many benefits and expected return on investment of a wireless LAN can be wiped out if a security and management policy is not in place and enforced.

This paper is designed to guide network administrators and security managers to design, implement, and enforce wireless LAN security policies that enable every organization to fully reap the benefits of wireless LANs without experiencing undue management pains and security holes.

IS administrators should establish a written policy dictating that the airwaves inside the enterprise are a managed resource, no different from a wired resource.

META Group

Enterprise & Regulatory Policies

As wireless networks proliferate, the ever-present danger of new, more sophisticated hacking tools is also on the upswing. Hackers, armed with new tools such as AirJack, AirSnarf, Hunter_Killer, etc are launching more sophisticated attacks on the network -- networks that a year ago were said to be unbreakable. When an organization's network is left exposed by insecure wireless LAN devices, hackers can compromise an organization's network backbone, rendering the investment in IT security useless. Not only are there

financial implications from a security standpoint, but the breach can potentially impact the company's reputation and proprietary and regulatory information. These scenarios can lead to additional financial loss and legal ramifications.

Hence various regulatory bodies have defined policies that have to be complied with by organizations. Regardless of the WLAN deployment status, organizations have to ensure that they track all wireless activity and prevent the transmission of wireless data in clear text.

The Department of Defense issued a wireless directive, Number **8100.2** on April 14, 2004. This directive establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid. Healthcare organizations have to maintain the sanctity of patient data by complying with the **HIPAA** regulations. Retailers have to comply with the mandates made by the Payment Card Industry (**PCI**). Various regulations e.g. **OCC** Wireless Advisory, **GLBA** – Safeguards Rule etc have been defined for banking and financial institutions. A new section of the **Sarbanes-Oxley Act, Section 404**, requires all publicly traded firms to file an internal control statement which must attest to management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company. While corporate officers are accountable, IT systems and infrastructure are critical to the financial reporting process and the burden falls on the IT department to ensure integrity of the established processes. The IT department must document, test, monitor and report the effectiveness of internal control processes.

Essentially, policies are house rules with possible actions that work on an if-then structure and can prohibit, permit, or require actions for both people and the hardware and software on the network. A policy sets the threshold for an alarm, and another sets the policy for the resulting action by a network manager.

Gartner

In addition to the regulatory policies, organizations must define their enterprise policy and monitor for compliance. This process is described in detail in the next section.

The Policy Process

Policies for an 802.11 wireless LAN should become part of the greater enterprise network policy and mirror the standard six-step policy process.

- 1.) Policies are first defined and documented.
- 2.) Management must then buy-into the documented policies.

Six Steps for Policy Compliance

1. Define & Document the Policy
2. Management Buy-in
3. Educate Employees
4. Monitor & Audit for Enterprise & Regulatory Compliance
5. Enforcement
6. Revise & Fine-Tune

- 3.) The policy should then be communicated to all employees, contractors, on-site vendors, and anyone else expected to comply with the policy.
- 4.) The wireless LAN should then be monitored to audit for policy compliance.
- 5.) To deal with devices and individuals found violating the policy, enterprises should have an established procedure to take corrective actions for network devices or individuals found in non-compliance.
- 6.) Finally, a process to revise and fine tune the wireless LAN policy should be in place to handle evolving security standards, user behavior, and physical changes in the network.

Essentially, policies are house rules with possible actions that work on an if-then structure and can prohibit, permit, or require actions for both people and the hardware and software on the network. A policy sets the threshold for an alarm, and another sets the policy for the resulting action by a network manager.
Gartner

Here is the detailed information on each of the aforementioned steps with example policies and thresholds.

Step 1: Define & Document the Policy

In establishing a documented wireless LAN policy, enterprises should consider four key components of the policy: WLAN Usage, Network Configuration, Security, and Network Performance. As every enterprise wireless LAN is different, policies for these four areas will vary for organizations and may overlap. For example, the proper configuration of an access point has a direct effect on the security of the wireless LAN.

WLAN Usage Policies

Organizations must first define the proper use of wireless LANs. This includes the applications that run across the wireless LAN and the exact locations where wireless LANs should and should not be deployed in the enterprise. Other considerations should determine roaming policies for stations between access points within a building or across multiple locations, and where employees can use organization wireless LAN devices in environments outside the control of the organization (i.e. hotspots, homes).

Applications – Wireless LANs can provide the high-speed connections required to run most applications. However, wireless LANs may not be well suited for applications with ultra-sensitive information. Because fail-proof wireless LAN security standards have yet to be adopted, organizations may choose to prohibit access to classified information and

related applications from the wireless LAN. Some organizations limit their wireless LANs usage for connecting to email and the Internet.

In addition to security concerns, bandwidth across the wireless LAN remains a limited resource. Bandwidth-intensive applications and network misuse, such as the downloading of MP3 files, can significantly drain the network and limit the wireless LAN's ability to serve multiple users.

Network Roaming – Some wireless LAN infrastructure allows for stations to seamlessly roam from access point to access point without dropping a connection. However, network roaming introduces security concerns that arise from the station not authenticating itself to each access point. Organizations should evaluate the benefits of roaming and counter them with the security risks to form a roaming policy for their wireless LANs.

Organization should map their wireless LANs and determine what stations need to connect to which access points. Some stations should only connect to a single access point or set of APs in the immediate work area and conference rooms. A manager may need to connect to access points throughout a building or corporate campus. An executive who often visits offices and organization facilities throughout in multiple locations should be allowed to connect to access points at all sites.

WLANs in Uncontrolled Environments – The widespread growth of wireless LAN technology into all new laptop computers forces organizations to decide exactly where and what types of networks employees are allowed to connect with. The growth of public wireless LANs – or hotspots – opens the door for convenient connections outside the office. However, these public networks offer little security and can potentially attract unscrupulous hackers who can take advantage of unsuspecting users. Stations are susceptible to accidental associations with neighboring networks and malicious associations with such wireless hackers.

WLAN Usage Policies	
Applications Across the WLAN	Bandwidth-intensive applications and extremely confidential enterprise data may not be best suited to run on the wireless LAN.
Network Roaming	Define the access points and WLANs that each station is allowed to connect to.
Uncontrolled Environments	Define where organization-owned, wireless-enabled laptops are allowed to connect to uncontrolled wireless LANs. Establish VPN capabilities for remotely connection to the enterprise network from home WLANs or hotspots.

Table 1: WLAN Usage Policies

The decreasing prices for consumer-grade access points fuels the home market for wireless LANs. While easy to set up, these networks default to insecure configurations. If organizations are to allow employees to use enterprise-owned laptops on home networks and use home wireless LANs to connect to the enterprise network, personal firewalls must be installed and proper authentication should be implemented. The policy should explicitly outline exactly how employees are to lock down their home wireless LANs.

Table 2: Configuration Policies	
Encryption & Authentication for All Wireless LAN Traffic	At a minimum, enterprises should employ the built-in WEP encryption. However, 802.1x, WPA and proprietary technologies (LEAP) are highly recommended for enterprise WLANs. Traffic should be monitored to ensure that traffic is encrypted and authenticated.
Authorization – MAC Filtering or RADIUS Server	MAC address filtering provides basic control over which stations can connect to an enterprise WLAN. Larger enterprise will require a RADIUS server to manage hundreds of stations and dozens of access points. Monitor the WLAN for unauthorized users.
Naming the Network – Changing Default SSIDs	Service Set Identifiers should be changed from default settings and renamed as to not draw attention from outsiders. (e.g. Avoid SSIDs of <i>CEO Office</i> or <i>Cash Register</i>) Monitor the WLAN for access points with default or improper SSIDs.
Reconfigure Default Windows XP Settings	Windows XP stations should be reconfigured from default settings that connect the station to the access point with the strongest signal – even if it's not an authorized access point. Monitor all stations for insecure stations and accidental associations.

Table 2: Configuration Policies

Encryption & Authentication for All WLAN Traffic – Because of a wireless LAN’s uncontrolled medium, encryption and authentication are an essential step to network security. The vulnerabilities of Wired Equivalent Privacy (WEP), the first encryption standard for 802.11 wireless LANs, have been well documented. However, all wireless LANs should at a minimum activate this basic encryption to protect their data from the general public who can passively “sniff” the traffic in the air to get open access to all unencrypted data passed through the air. At a minimum, enterprises should establish a policy that mandates all traffic to be encrypted with WEP.

Stronger encryption and authentication is available from vendors, such as Cisco, which offers Lightweight Extensible Authentication Protocol (LEAP) and Protected Extensible Authentication Protocol (PEAP). Industry-standard solutions, such as 802.1x, are now available for the latest wireless LAN hardware, but equipment purchased before 2003 may not support these new encryption standards. Wi-Fi Protected Access (WPA) is expected to

replace WEP as the accepted encryption standard in the second half of 2003. Enterprises that seek to avoid the security flaws of WEP should deploy 802.1x, WPA, or LEAP and establish a policy that all WLAN traffic must use the selected encryption and authentication.

MAC Filtering or RADIUS Server – Most enterprise-class access points allow you to limit which stations can connect to it based on filtering of Media Access Control (MAC) addresses of authorized stations. While MAC addresses can be easily spoofed, MAC address filtering provides basic control over which stations can connect to your network. And much like the use of WEP, MAC address filtering provides some basic protection against the general public connecting to an enterprise wireless LAN.

Larger enterprises with more complex wireless LANs that allow hundreds of stations to roam between access points require more complex filtering from remote authentication dial-in service (RADIUS) servers. Enterprises should set WLAN configuration policies that force all access points to authorize users through a RADIUS server.

Naming the Network: SSIDs – Enterprises should change their access points' default Service Set Identifiers (SSIDs), which are essentially the names of each access point or set of access points. Cisco access points come with the default SSID of "tsunami", Linksys defaults to "linksys," and both Intel and Symbol access points default to "101." These default SSIDs alert hackers to vulnerable wireless LANs.

Because SSIDs can be observed by any wireless station within broadcast range of the access point, SSIDs should be changed to names that are meaningless to outsiders. An SSID of "CEO Office" or "East Cash Register" only calls attention to valuable information that a hacker would like to get into.

Reconfigure Default Setting of Windows XP – Windows XP is incredibly Wi-Fi friendly, which is great for usability but can leave a station open to exploits. Default settings of Windows XP will cause a station to scan the airwaves in search of wireless LANs and connect to the access point with the strongest signal. The station is at risk of accidentally associating with a neighboring network or hacker in the parking lot. A station connecting to a neighboring wireless LAN can divulge passwords or sensitive documents to anyone on the neighboring network. Accidental associations can even link the two companies' networks together through this end user station as it bypasses all internal security and controls.

Policies should be in place to mandate all Windows XP implementations be handled by the IT department, so that all stations employ the secure XP settings to reduce the risk of accidental or malicious associations. IT organizations should monitor Windows XP stations to ensure that all insecure XP wireless settings remain disabled.

Security Policies

Many security issues of wireless LANs can be addressed with a properly configured network. However, enterprises should also implement additional security policies for their wireless LANs to address unsanctioned wireless LAN hardware and unauthorized activity on the network.

Prohibit Unauthorized Access Points – An employee, vendor, or on-site consultant can unknowingly put all information assets at risk with a \$100 consumer-grade access point purchased from a local retail store. A single unauthorized access point – or rogue AP – attached to an enterprise LAN circumvents all existing network security by broadcasting an open connection to the corporate network. This rogue access point can enable intruders to view, modify, or steal corporate data from the parking lot outside the building. Laptops can also be converted to function as access points with freeware programs distributed as trojans. These “soft APs” are more dangerous than typical rogue access points because they appear as sanctioned devices on the wired network.

A single rogue access point essentially extends an Ethernet connection to anyone in the building and beyond. With this open connection, a hacker can get to the enterprise network. Intellectual property, financial servers, management files, confidential data, human resource records, and sensitive corporate information are put at risk of exposure, theft, or corruption. Enterprises should enforce a policy that prohibits anyone from installing an access point that is not approved and configured by the IT organization.

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 (0.8 probability).

Gartner

Prohibit Ad Hoc Networks – WLAN cards enable peer-to-peer networking between laptops, PCs or other devices without an access point. These ad hoc networks can allow a user to transfer private corporate documents and intellectual property to unauthorized users without going over the corporate network. While WLAN cards operate in ad hoc mode, the user must be able to trust all stations within range because ad hoc networks offer poor authentication.

IT security managers should treat ad hoc networks in the same manner as rogue access points because they can put a network at risk without security managers ever seeing the vulnerability. For these reasons, policies should be established and enforced to prohibit ad hoc networks.

Security Policies	
Prohibit Unauthorized “Rogue” Access Points	All access points should be securely deployed through the IT organization. Organizations should monitor all WLAN activity to detect rogues WLANs attached to the wired network.
Prohibit Ad Hoc Networks	Stations should be configured to not allow peer-to-peer, ad hoc networks between stations. Monitor the WLAN to identify ad hoc networks and recognize stations that are configured to allow ad hoc networks even if no peer-to-peer network exists at that time.
Limit Off-Hours Traffic	Turn off the access point during non-use hours and monitor the airwaves for off-hours traffic.
Vendor-Specific Hardware	Limit WLAN hardware to select vendors which support the deployed security measures and monitor for unauthorized vendors.

Table 3: Security Policies

Disable Access Points During Non-Usage – Enterprises that operate during set business hours should limit their wireless LANs to operate only during those hours at which the networks should be in use. Because an access point extends an open connection to the enterprise network beyond the walls of a building, enterprises should limit WLAN traffic to defined business hours. Policies should be in place to limit off-hours traffic across a wireless LAN.

Vendor-Specific WLAN Hardware – Enterprise wireless LAN deployments should be based on enterprise-class access points that support the advanced security and management settings and applications, which are essential to network fidelity. However, consumer-grade wireless LAN access cards may not support the advanced security and management applications and settings. An enterprise wireless LAN policy should establish a list of acceptable wireless LAN card vendors that can be used on organization-owned laptops to connect with the enterprise network. For these security concerns, employees should not be allowed to install consumer-grade wireless LAN cards to organization-owned laptops.

Network Performance Polices

To maximize performance of an enterprise wireless LAN, organizations should establish policies for performance metrics that ensure that the wireless LAN delivers the expected return on investment. A policy for performance metrics should include:

- Maximum number of stations associated to a single access point at a single time – usually 5 to 15 depending on bandwidth requirements of stations.
- Maximum bytes allowed between an access point and the wired network to guard against the overloading of a single access point.
- Maximum bytes allowed between an access point and individual stations to guard against a single station consuming so much bandwidth that other stations on the network are severely affected.
- Traffic patterns of the wireless LAN that provide valuable operational details for use when assessing degradation and overall usage.

Step 2: Management Buy-In

Once a wireless LAN policy has been defined and documented, the next step is to have executives approve the policy and agree to its strict implementation. A wireless LAN policy without management buy-in lacks the teeth required make the policy effective.

While technical staff focus on what can and cannot be technically feasible in a wireless LAN policy, managers should focus on the business case of the wireless LAN. Performance policies work to guarantee the network's promised productivity gains. Security polices are necessary to guard against the potential monetary losses that can come from exposed corporate data, open enterprise systems, and the public embarrassment of ending up in the press for such attacks.

Organizational politics and the lack of stakeholder support can cause a wireless LAN policy to fail miserably. Strong management buy-in can circumvent these potential mine fields.

Step 3: Educate Employees

After receiving appropriate approval and support from management, the policy must be communicated to those expected to comply with the policy. In the case of wireless LANs, this can include employees, independent contractors, on-site vendors, and any frequent

visitor. Effective education of the policy can be accomplished in a variety of ways. Everyone should receive a written copy of the policy and then be required to sign a statement saying they agree to strictly follow the defined policy. For more proactive education, 15- or 30-minute sessions can be conducted periodically to go over the highlights of the policy, go over recurring problem areas, and reinforce key messages.

Step 4: Audit & Monitoring

Well-defined wireless LAN policies are essential for organizations to reap the expected benefits and eliminate unnecessary risks associated with 802.11 wireless LANs. However, policies can become useless if an enterprise does not monitor for policy compliance. IT security and network managers have few options in monitoring the wireless LAN to enforce the established policies.

Wired-Side Network Scanners

Wired-side scanners provide limited insights into the real activity across the wireless medium. By polling network devices for key characteristics, such as MAC addresses and open ports, wired-side scanners typically use TCP fingerprints to identify various types of devices.

Wired-side scanners can identify some rogue access points, but they are not an effective solution for enterprise rogue wireless LAN detection because wired-side scanners:

- Require an accurate database of all IP devices;
- Cannot cross subnets unless routers are reconfigured to allow for such intrusive scans;
- Produce multiple false positives from network intrusion detection systems and personal firewalls; and
- Cannot detect Soft APs, ad hoc networks or accidental associations.

When monitoring the WLAN for compliance with policies other than rogues, wired-side scanners can analyze traffic between the wired network and the access point. However, these scanners cannot monitor policy for encryption and authentication of wireless LAN traffic, SSID names, ad hoc, peer-to-peer networks, channels of operations, data rates between wireless devices and performance thresholds for connections between access points and stations and wireless LAN traffic patterns.

Wireless Sniffers & Scanners

Handheld wireless scanners and sniffers can be used to periodically survey the airwaves for policy compliance. However, sniffers and scanners are limited by their need for a network administrator to physically walk the area with a laptop or hand-held device running the sniffer or scanner application. Additional limitations include a lack of reporting capabilities needed to document results or findings of the scanning initiative. A September 2002 research brief from META Group questioned the viability of wireless sniffers and scanners for enterprise security and policy monitoring.

While this process requires the physical presence and valuable time of a network manager, the effectiveness is limited because it only samples the airwaves for threats. New rogue access points or other policy violations can arise after a scan and will not be detected until the next time a network administrator surveys the network. Like a camera that takes a snapshot of a single moment in time, wireless sniffers and scanners only provide information on a single stationary moment.

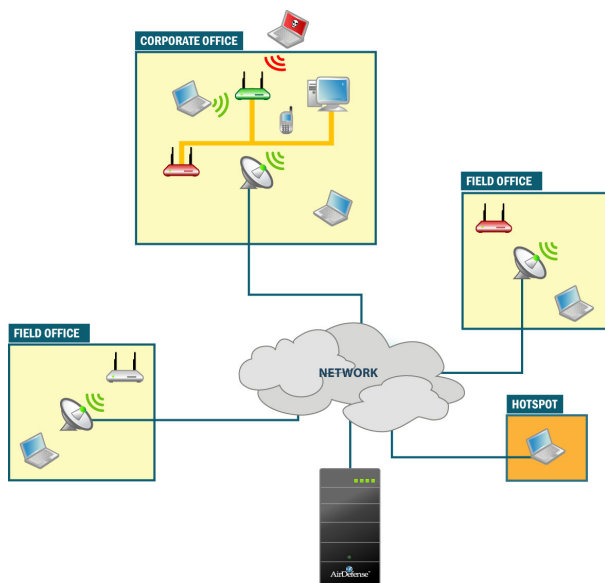
Current radio frequency scanning tools such as Sniffer Wireless and AirMagnet are limited in their ability to perform scalable and repeatable audits.

META Group

The vast limitations of physical site surveys and the demands for personnel time limit the effectiveness of sniffers and scanners for large enterprises. Sniffers and scanners are simply not cost-effective for an enterprise with multiple locations or sensitive information that cannot risk performance degradation and security breaches from policy violations. In addition, IT security and network administrators would find this decentralized approach extremely difficult to manage and collect information for multiple locations.

24x7 Policy Monitoring – The AirDefense Solution

Monitoring wireless LANs for policy compliance across an enterprise requires a scalable solution that combines the centralized management of wired-side scanners and radio frequency analysis of wireless scanners. AirDefense provides this comprehensive solution with an innovative approach to wireless LAN security and operational management.



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.

With patent-pending technology, AirDefense solutions monitor WLAN traffic 24x7 and identify policy violations for:

- Rogue wireless LANs – including Soft APs;
- Unencrypted or unauthenticated traffic;
- Unauthorized stations;
- Ad hoc networks;
- Default or improper SSIDs;
- Access points and stations operating on unauthorized channels;
- Insecure stations with default Windows XP settings;
- Off-hours traffic;
- Unauthorized vendor hardware;
- Unauthorized data rates; and
- Performance thresholds that indicate the overall health of the wireless LAN.

The centralized management and 24x7 monitoring of the airwaves provides a scalable and cost-effective solution that enables enterprise wireless LAN detection throughout multiple locations of an organization. One or two sensors are deployed in each location to provide comprehensive, 24x7 policy monitoring for wireless LANs.

As new offices are opened, AirDefense solutions easily scale to secure that office with the addition of a sensor deployed in the new location. Regardless of the WLAN deployment status, AirDefense provides comprehensive monitoring against all WLAN activity provides the most advanced solutions for policy definition, monitoring and compliance. In addition, it supports an advanced wireless LAN security and operational management with functionality that includes:

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

AirDefense has a variety of regulatory compliance reports for healthcare organizations, retailers, financial service providers and government agencies (HIPAA, GLBA, PCI, DoD Directive). In addition, AirDefense offers enhanced reports to demonstrate effective internal control over protection of confidential data for Sarbanes-Oxley compliance. (See Appendix 2 for

Step 5: Enforcement – Get Proactive

After monitoring for WLAN policy compliance, enterprises must take corrective measures to alter network configurations, eliminate rogue stations or APs, and deal with the people responsible for such violations. As part of the written WLAN policy, an enterprise should document exactly how violations should be corrected and who is responsible for taking the necessary actions. In the case of an improperly configured access point with a default SSID and disabled encryption, the policy could read to the effect of:

Insecure enterprise access points should be viewed as a major security threat. Network managers should view improperly configured access points as high priority to be corrected within 30 minutes of detection. The network manager must reconfigure the AP as defined by the WLAN policy and monitor the AP's configuration over the next hour. If the AP cannot be reconfigured according to the WLAN policy or a greater problem with the AP is detected, the access point should be disabled until a solution is found.

Similar policies for enforcement should be in place to deal with various levels of priority for usage, configuration, security, and performance policies.

Because of the proliferation of rogue access points and the major security threats they represent, enterprises struggle with exactly how they should enforce a policy that bans all unsanctioned access points. Productive, well-meaning employees are the most likely to violate this policy. However, the deployment of such rogue devices can also be a malicious act of corporate espionage or sabotage. The strictest enforcement of a WLAN policy calls for an employee to be fired for installing unauthorized access points to the enterprise wired network.

The more common means of dealing with rogue access points is to disable the access point as soon as it is detected. The access point should be confiscated, and the employee who violated the policy is given a written warning with the explicit understanding that repeated violations will result in termination or suspension.

Many organizations find departmental wireless LANs that were deployed outside the knowledge of the IT staff. The wireless LAN policy should require all wireless LAN networking equipment to be registered with the IT staff. Once an unknown wireless LAN is identified, the IT staff should take immediate steps to ensure the wireless LAN complies with the enterprise wireless LAN policy for usage, configuration, security, and performance. The AirDefense solution described in the above section can be used to terminate rogue devices or associations. There are two methods that can be utilized

RF AirTermination: AirDefense can protect against wireless threats via the air by terminating the wireless connection between the intruder and an authorized AP, or by terminating the connections of authorized stations to a rogue access point. AirDefense has partnered with Cisco Systems to provide the most accurate and automated, closed-loop wireless protection system.

Wired-side Port Suppression: AirDefense detects rogue devices and passes required information about them to CiscoWorks WLSE which in turn leverages Cisco switching infrastructure to suppress the port the rogue access point or intruder station is connected to. Tracing the port of the rogue device is not a trivial task and with Cisco integration, AirDefense is the only solution can accurately and reliably protect against all intruders and attackers, every time.

Step 6: Revise & Fine-Tune the Policy

After a wireless LAN policy is defined, implemented, and enforced, organizations must evaluate the policy's effectiveness and limitations. Network managers that oversee the policy's implementation should solicit feedback from WLAN users and those who enforce the policy. By conducting a formal review process, the WLAN policy should be revised to fit the specific needs of the organization. In many cases, the WLAN policy may need to be tightened for greater security and management. However, other organizations may be required to loosen their policy to allow for greater WLAN adoption, usage, and productivity.

Once the policy is revised and fine-tuned, the policy process must be repeated to document all changes, have management buy-into the new policies, communicate the policies to all who are expected to comply, monitor for compliance, enforce the policy, and finally refine the policy.

Conclusion

Wireless LAN policies will vary based on an organization's wireless LAN deployment, risk tolerance, and needs for performance and usage. However, the documented policy is just the first step toward maximum security and network performance. Monitoring for policy compliance plays a critical role that ensures that the policy does not become a useless, unread document. Without auditing the network for policy compliance, the policy cannot be enforced.

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.**