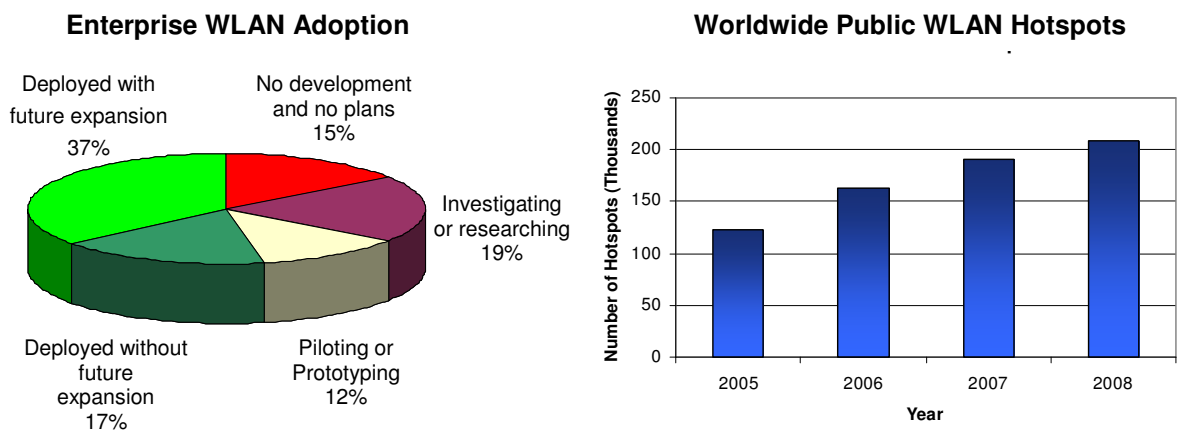

**TIRED OF ROGUES?
Solutions for Detecting and
Eliminating Rogue Wireless
Networks**

Tired of Rogues? : Solutions for Detecting and Eliminating Rogue Wireless Networks

This paper provides an overview of the different types of rogue wireless devices, risks faced by enterprises due to their proliferation and multiple approaches to detecting and mitigating them. The AirDefense solution allows enterprises to effectively detect and eliminate all types of rogues.

Wireless technology is growing in popularity. Businesses are not only migrating to wireless networking, they are steadily integrating wireless technology and associated components into their wired infrastructure. The demand for Wireless Local Area Networks (WLANs) is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants and a desire by users for continual connections to the network without having to “plug in.”



Source: Gartner Dataquest, Aug-2005

Wireless is the future of networking

Figure 1: Wireless LAN adoption trends

Figure 1 shows the trends in WLAN adoption based on a Gartner Dataquest survey. Over 50% enterprises have deployed wireless. The growth in wireless hotspots has also been astonishing. In fact, according to Dell'Oro, there has been an 87% increase in hotspots worldwide from January 2005 through January 2006 - from 53,779 in 93 countries to 100,355 in 115 countries. Forward Concepts industry analysts predict that WLAN equipment will continue growing at a higher rate in 2006 to the \$5.9 billion level as new IEEE 802.11n and voice over WLAN equipment is introduced

and the infrastructure for traditional WLAN expands¹. Dell’Oro estimates that the WLAN market will continue to grow at a compounded annual growth rate of 32% through 2009.

“By 2006, 80 percent of enterprise WLAN networks will remain vulnerable to intrusion. Action Item: Perform wireless intrusion detection to discover rogue access points, foreign devices connecting to corporate access points and accidental association to nearby access points in use by other companies.” Gartner

Experts and industry analysts agree that given the proliferation of WLANs, there is a very high probability of unauthorized WLAN devices showing up on an enterprise’s network. Any unauthorized wireless device that connects to an enterprise’s authorized network or device is defined as a rogue wireless device. Rogue wireless devices pose one of the greatest risks to an enterprise’s network security. Figure 2 shows typical rogue device scenarios that compromise contemporary wired and wireless networks, circumventing traditional security mechanisms such as firewalls and perimeter protection.

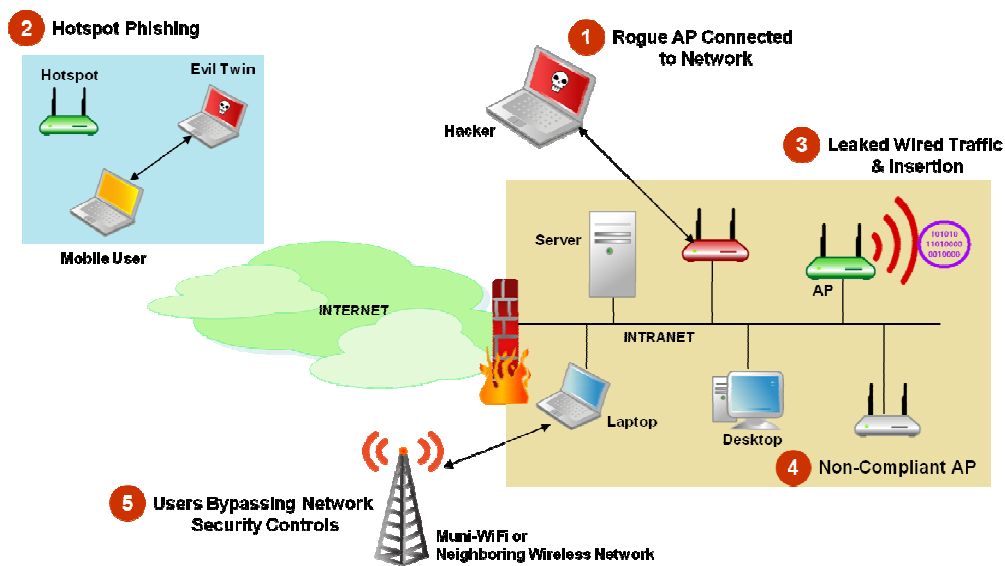


Figure 2: Rogue devices compromise traditional wired and wireless security

1. Evolution of Rogue WLANs

Just as employees first brought personal computers to the office in the 1980s for their many benefits, employees are installing their own WLANs to corporate networks when IT departments are slow to adopt the new technology. According to Gartner, enterprises that have not deployed wireless are at a higher risk of exposure from rogue wireless devices.

Even enterprises that are deploying wireless must tackle the problem of rogue WLANs from employees who do not have wireless access, contractors, auditors, vendors, etc., who bring in their own equipment while operating within the office, or potential espionage traps.

¹ <http://www.tekrati.com/research/News.asp?id=5764>

“At least 20% of enterprises already have rogue WLANs attached to their corporate networks, installed by users looking for convenience of wireless and unwilling to wait for the IS organization to take the lead.” Gartner

Rogue Access Points – Rogue WLANs most commonly refer to rogue Access Points (AP) that when attached to the corporate network broadcast a network connection. A rogue AP is any AP unsanctioned by network administrators and connected to the wired network. Most rogue APs are improperly secured with default configurations that are designed to function right out of the box with no security features turned on. Employees or even business units seeking to enhance their productivity deploy rogue APs innocently without comprehending overall security risks.

The Real Rogue Threat: Wireless Stations and Not APs – WLANs are comprised of APs that are attached to the enterprise network and WLAN access cards for laptops, hand-held devices, and desktop computers. Both unauthorized APs and unauthorized activity from WLAN access cards can pose significant security risks. As more and more confidential information is locally stored on mobile laptops equipped with WLAN access, these become the weakest link in the security infrastructure. Wireless laptops often run supplicants designed to effortlessly connect to available wireless networks making them vulnerable to wireless attacks.

Devices with Built-in WLAN Access – Major computer vendors are selling increasing number of laptops with built-in WLAN access cards. A rogue WLAN has traditionally been thought of as a physical AP unsanctioned by network administrators. Today rogue WLANs are further defined as laptops, handhelds with wireless cards, barcode scanners, printers, copiers or any WLAN device. These devices have little to no security built in making it easy for intruders to find an entry point. Increasingly, we are seeing ad-hoc networks in new networked devices such as printers, projectors, gaming consoles, etc. A simple printer with an open, unauthenticated, peer to peer ad-hoc wireless network (typically present for ease of use, troubleshooting, etc.) can provide a bridge to the wired-side network to which it is connected.

Soft APs – While hardware APs have been the focus of security issues to-date, wireless-enabled laptops are easily configured to function as APs with commonly available freeware such as HostAP or software from PCTel. Known as “Soft APs,” these laptops are harder to detect than rogue APs. These Soft APs pose all the risks of any typical rogue AP by broadcasting an insecure connection to the enterprise network. However, Soft APs are harder to detect than rogue APs because the Soft AP can appear as an authorized station to all wired-side network scans.

Stealth Rogue Devices – Several new and sneaky rogue WLAN devices are constantly being exposed. Examples include rogue APs that look like power adapters plugged into a wall jack. These devices have a WLAN AP built in and use power-line communications as the wired-side link! Such a device will never be detected by wired-side network scanners. Nevertheless, it can be within the enterprise perimeter luring unsuspecting corporate users to connect wirelessly and reveal confidential information to a hacker well outside the perimeter. Other examples include stealth rogue APs that are completely silent until they hear a special “knocking” sequence over the air, upon which they wake up, communicate and go back to silent mode. These rogues cannot be detected by

occasional walk-around tests with handheld sniffers. They require, 24x7 “always on”, monitoring of the airspace.

Accidental and Malicious Associations – Accidental associations are created when a neighboring AP across the street or on adjacent floors of a building bleeds over into another organization’s airspace triggering its wireless devices to connect. Once those devices connect with the neighboring network, the neighbor has access back into the organization. Accidental associations between a station and a neighboring WLAN are recognized as a security concern.

A malicious association is when a company laptop is induced to connect with a malicious device such as a Soft AP or laptop. The scenario also exists when a malicious laptop connects with a sanctioned AP. Once the association has been made the hacker can use the wireless device as a launch pad to attack servers and other systems on the corporate network.

Ad-Hoc Networks – Similar to rogue APs, ad-hoc wireless networks represent another major concern for WLAN security because they can put a network at risk without security managers ever seeing the vulnerability. WLAN cards enable peer-to-peer networking between laptops without an AP. These ad-hoc networks can allow an authorized 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 little or no authentication management. A hacker’s station could directly connect to an authorized user, access local information and potentially gain access to the rest of the wired network if the user happens to be connected to the wired network as well.

2. What is at Risk?

Because WLANs operate in an uncontrolled medium, are transient in the way they connect, and come with insecure default configurations, they provide an easy open door to the wired network and wireless access devices. Insecure wireless networks can easily be sniffed acting as a launch pad to the wired network and an organization’s corporate backbone. Once accessed an insecure WLAN can compromise:

- Financial data, leading to financial loss
- Reputation, damaging the efforts spent building the brand
- Proprietary information, leaking trade secrets or patents
- Regulatory information, foregoing customer privacy or ignoring government mandates
- Legal or regulatory ramifications
- Wired infrastructure such as switches and routers

3. Requirements to Detect Rogue WLANs

In confronting the issue of rogue WLAN detection, a user must consider the functional requirements and return on investment of the solution. IT security managers should evaluate various approaches based upon technical requirements, enterprise scalability, cost, and ability to cover the future needs of network security.

Functional Requirements

A comprehensive solution to detect rogue WLANs must detect all WLAN hardware and activity that includes:

- Detection of all rogue devices and associations
- Ability to classify and clearly distinguish rogues on the network from unauthorized wireless devices sharing the airspace
- Detailed forensic analysis of rogue devices and associations
- Assessment of threat from a rogue device based on present and past behavior
- Physical and network location of rogue devices
- Termination of rogue devices using wired and wireless mechanisms

Scalable and Cost Effective for the Enterprise - Rogue detection 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 globe. Large enterprises require a cost-effective solution that can be centrally managed. In determining the cost of rogue detection, IT security managers must consider the initial costs of the solution and additional costs needed for on-going support.

Future Proof - Rogue detection should scale to meet the future needs of enterprise network security. An organization that bans all WLANs today is likely to move ahead with a pilot deployment in the next year. At this time, an enterprise with limited WLANs must maintain its rogue detection for unauthorized areas and secure the pilot WLAN from accidental associations and ad-hoc networks. As WLANs are deployed throughout an enterprise, rogue detection must be complemented with 24x7 monitoring and intrusion detection. Other value added benefits that can be leveraged such as performance and network health monitoring should also be considered in the decision process.

4. Techniques to Detect Rogue WLANs

Once an organization decides on a policy that bans WLANs completely or more precisely prohibits employees from deploying their own networks, the organization must decide how to enforce that policy across the enterprise. This section outlines several approaches that have been used to detect rogue WLANs and their strengths and weaknesses.

- 1.) Wired-side Intrusion Detection System
- 2.) Wired-side SNMP Polling
- 3.) Wired-side Network Scanners
- 4.) Wireless Scanners and Sniffers
- 5.) Wired-side Traffic Injection
- 6.) Wireless Traffic Injection
- 7.) AirDefense 24x7 Centralized Wired and Wireless Monitoring

1. Wired-side Intrusion Detection System

Wired-side intrusion detection system (IDS) offers virtually no ability to detect rogue WLANs but can be useful in a limited capacity. While intruders entering the network through a rogue WLAN appear mostly as authorized users, a wired-side IDS may alert IT security managers when the intruder tests wired-side security measures. A wired-side IDS fails as an effective approach to detecting rogue WLANs because it cannot identify APs attached to the wired network, soft APs, accidental associations and ad-hoc networks. These are typically below the radar for wired IDS.

2. Wired-side SNMP Polling

Simple Network Management Protocol (SNMP) polling can be used to query information from IP devices attached to the wired network, such as routers, stations, and authorized APs. This process requires that the IT security manager conducting the SNMP poll to know the IP address of all devices being polled, which must also be configured to enable SNMP. For these reasons, SNMP polling by itself is not an effective approach to detecting rogue WLANs. The IT security manager is not likely to know the IP address of the rogue AP, and the rogue AP is not likely to have SNMP enabled. In addition, an SNMP poll against an authorized station operating as a Soft AP would not detect any WLAN activity. SNMP polling also would not detect accidental associations or ad-hoc networking between stations.

However, SNMP polling of wired switches can reveal MAC addresses of wireless devices connected to them. Intelligent analysis of this information with correlation of wireless information can be used for rogue detection.

3. Wired-side Network Scanners

Wired-side network scanners work similar to SNMP polling to identify IP devices attached the network and key characteristics of those devices, such as MAC addresses and open ports. Rather than the SNMP protocol, scanners typically use TCP fingerprints to identify various types of devices.

Network scans can also be extremely intrusive and they require that an IT security manager have access to all the IP devices on the network and know all IP addresses. To locate every rogue AP, a scan would have to be performed on the entire network, which would cause personal firewall alerts and multiple alarms from network intrusion detection systems. Traditional wired-side network scanners are not an effective solution for enterprise rogue WLAN detection because wired-side scanners

- Require an accurate database of all IP devices
- Are limited to subnets unless routers are reconfigured
- Produce multiple false positives from network IDS and personal firewalls
- Cannot detect Soft APs, accidental associations, or ad-hoc networks.

4. Wireless Scanners and Sniffers

Wireless sniffers and scanners differ greatly from wired-side tools because wireless sniffers and scanners capture and analyze WLAN packets from the air. By monitoring the airwaves for all WLAN activity, wireless sniffers and scanners detect most APs and active wireless stations within range. They also can provide detailed information about the configuration and security employed by each device.

Both 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. A research brief from META Group questioned the viability of wireless sniffers and scanners for enterprise security.

“WIDS must continuously scan for and detect authorized and unauthorized activities. Continuous scanning is 24 hours/day, 7 days/week.” Department of Defense (DoD) Policy, June 2006

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 at any given time. New rogue APs and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network. In addition, since handheld sniffers do not have wired-side information, determining a rogue is typically done by walking right up to it and making sure it is connected to the wired network. Stealth rogue devices might go undetected as would transient station associations.

This approach is 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 monthly basis, rogue APs and other vulnerabilities can pop up the minute the survey is completed.

Smaller organizations operating in a single location without potential for growth may find sniffers and scanners to be their most cost-effective solution if the organization is willing to accept the threat of rogue WLANs popping up between network audits. 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 rogue networks operating between security audits. In addition, IT security administrators would find this decentralized approach extremely difficult to manage and collect information for multiple locations.

5. Wired-side Traffic Injection

Some vendors have used dedicated wired-side devices to inject special broadcast frames over the wired network segment. These broadcast frames are then transmitted over the air by any wireless APs present on the same network segment. By detecting these frames over the air, using wireless sniffers, and analyzing the transmitter’s MAC address, the user is able to determine if any unauthorized APs are connected to that network segment.

The primary drawback of this method is that it requires a wired traffic injector in every network segment. This might make it infeasible with multiple VLANs. In addition, this method fails to detect any rogue APs that have built in routers. Routers will separate broadcast domains and the special wired broadcast frame will not be transmitted over the air. Since most common consumer APs that

end up as rogues have built in routers, this method is not very effective. Further, this technique provides zero client side rogue detection function.

6. Wireless Traffic Injection

This method is similar to wired traffic injection except it relies on a wireless device to inject a special frame over the air. If a sniffer sees an unauthorized AP, it tries to connect to it wirelessly and subsequently inject a frame that can be traced on the wired-side by a server or by another sniffer connected on the wired-side.

While this technique works with rogue APs that have built in routers, it fails if the rogue AP has security enabled. If security is enabled, the sniffer will not be able to connect with the device. Further, this technique exposes the wireless IPS system by forcing it to transmit frames over the air in an effort to detect rogues.

7. AirDefense 24x7 Centralized Wired and Wireless Monitoring

Enterprise rogue WLAN detection requires a scalable solution that combines the centralized management of wired-side scanners and radio frequency analysis of wireless scanners. AirDefense Enterprise provides this comprehensive solution with an innovative approach to WLAN security that includes a distributed architecture of remote sensors to monitor the airwaves for all WLAN activity and report to a centrally managed server appliance. The remote sensors are equivalent to wireless scanners but add 24x7 monitoring to provide 100% coverage against rogue WLANs the minute they are connected to the network or enter the coverage area. This approach to rogue WLAN detection and mitigation is akin to the security of physical buildings whereby video cameras are deployed at key locations for 24x7 monitoring and a central security station analyzes the incoming video for security risks. The video cameras reduce the need for costly security guards to walk through the building just as the remote sensors of AirDefense Enterprise replace the need for handheld manual wireless scanners.

The server appliance also maintains a detailed minute-by-minute forensic database of every wireless device in the airspace. By intelligently correlating real-time wireless information and wired-side data with historical behavior, the AirDefense system is able to determine and eliminate all rogues with the lowest false positive rate of any system available today. Table 1 compares the detection performance of several techniques under different rogue scenarios. The AirDefense system is capable of detecting virtually any type of rogue device.

Rogue Device Scenarios		Sensor Based Detection	SNMP Lookup Detection	Wireless Traffic Injection	Wired Traffic Injection	AirDefense
AP	Consumer AP	Yes	Yes	Yes	Yes	Yes
	Consumer AP with security	Yes	Yes	No	Yes	Yes
	Consumer AP/Router with NAT	No	Yes	Yes	No	Yes
	Consumer AP/Router with NAT & security	No	Yes	No	No	Yes
	Consumer AP/Router without NAT	Yes	Yes	Yes	No	Yes
	Consumer AP/Router without NAT & security	Yes	Yes	No	No	Yes
	Enterprise AP	Yes	Yes	Yes	Yes	Yes
	Enterprise AP with MBSSID	Yes	Yes	Yes	Yes	Yes
	Enterprise AP with security	Yes	Yes	No	Yes	Yes
	Enterprise AP with MBSSID & security	Yes	Yes	No	Yes	Yes
Client	Rogue Client connecting to Authorized AP	Yes	Maybe	No	No	Yes
	Rogue Client connecting to Rogue AP	Maybe	No	No	No	Yes
	Authorized Client with Unauthorized AP	Yes	No	No	No	Yes
	Authorized Client with Ad-Hoc connection	Yes	No	No	No	Yes

Table 1: Rogue device scenarios and detection capabilities of different methods

“For Carilion, rogue wireless LANs are a serious matter. AirDefense provides the peace of mind from knowing that we can identify and eliminate all unsanctioned wireless laptops, APs, ad-hoc networks and application-specific wireless devices as they enter our airspace.” Greg Walton, CIO, Carilion Health System

5. The AirDefense Solution

The centralized management and 24x7 monitoring of the airwaves provides a scalable and cost-effective solution that enables enterprise WLAN detection throughout multiple locations of an organization. A few sensors are deployed in each location to provide comprehensive, 24x7 detection of rogue WLANs. As new offices are opened, AirDefense Enterprise easily scales to secure that office with the addition of sensor(s) deployed in the new location. AirDefense provides comprehensive and advanced rogue management capabilities that go beyond simple alerts of broadcasting APs. The functionality includes:

Detection of All Rogue WLAN Devices and Activity - AirDefense recognizes all WLAN devices, which include APs, WLAN user stations, Soft APs, and specialty devices such as printers, wireless bar code scanners for shipping or inventory applications, etc. AirDefense also identifies rogue behavior from ad-hoc or peer-to-peer networking between user stations and accidental associations from user stations connecting to neighboring networks.

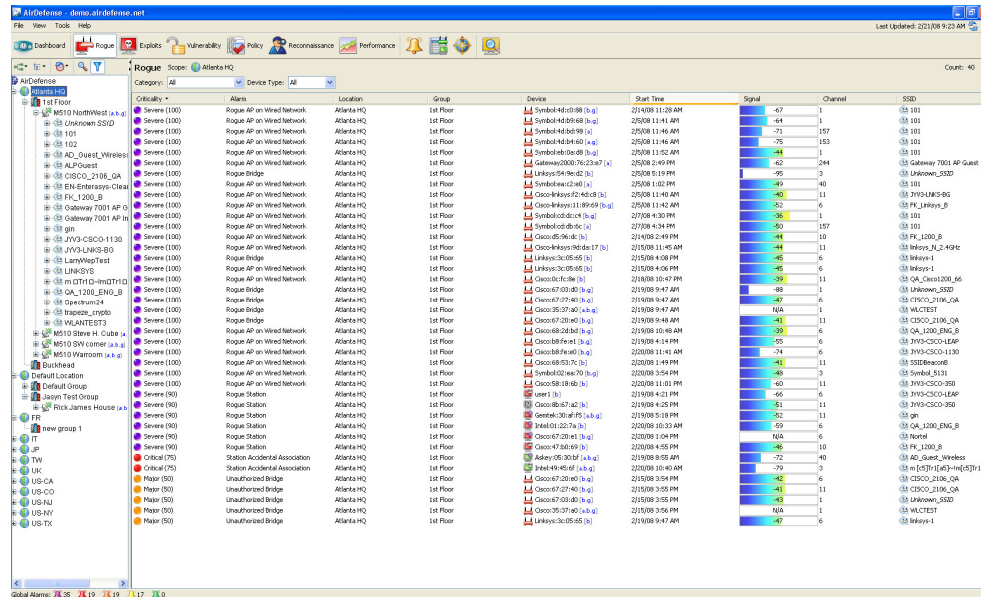


Figure 1: AirDefense Enterprise - Rogue Threat Analysis

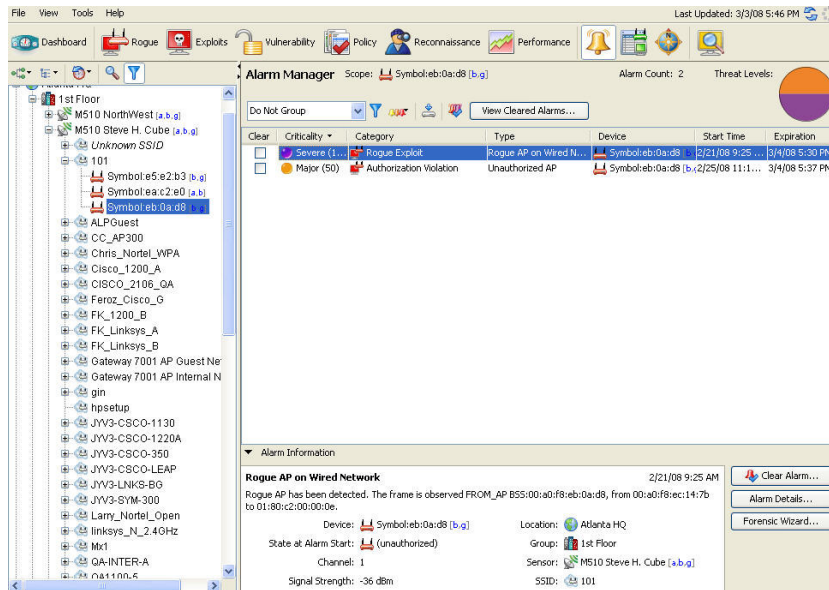


Figure 2: AirDefense Enterprise - Rogue Device Information

Threat-Based Rogue Management - AirDefense goes beyond simple detection of rogue devices and assesses the risk associated with an unknown device. Clearly not every unauthorized AP is a rogue device. In a business park, one is likely to see many unauthorized devices from neighboring buildings. AirDefense uses patented techniques to determine if a rogue is connected to the internal network, pinpointing those unauthorized APs that present the highest threat potential. AirDefense's advanced threat assessment capabilities enable the user to focus their attention on real threats and safely ignore neighboring APs.

Risk and Damage Assessment - AirDefense tracks all rogue communication and provides forensic information to identify when the rogue first appeared, how much data was exchanged, and the direction of traffic. With detailed analysis, AirDefense assists IT personnel assess the risk and damage from the rogue. Packet capture can also be enabled for further analysis of the rogue in a packet analyzer.

Rogue WLAN Location - To find the location of the rogue device, AirDefense provides accurate location tracking using signal strength triangulation and fingerprinting techniques. Location tracking enables the IT administrator to locate and track rogue devices in real-time. Location determination is also available in AirDefense Mobile, a complementary product to AirDefense Enterprise, which allows administrators to locate and track down rogue devices during walk around tests.

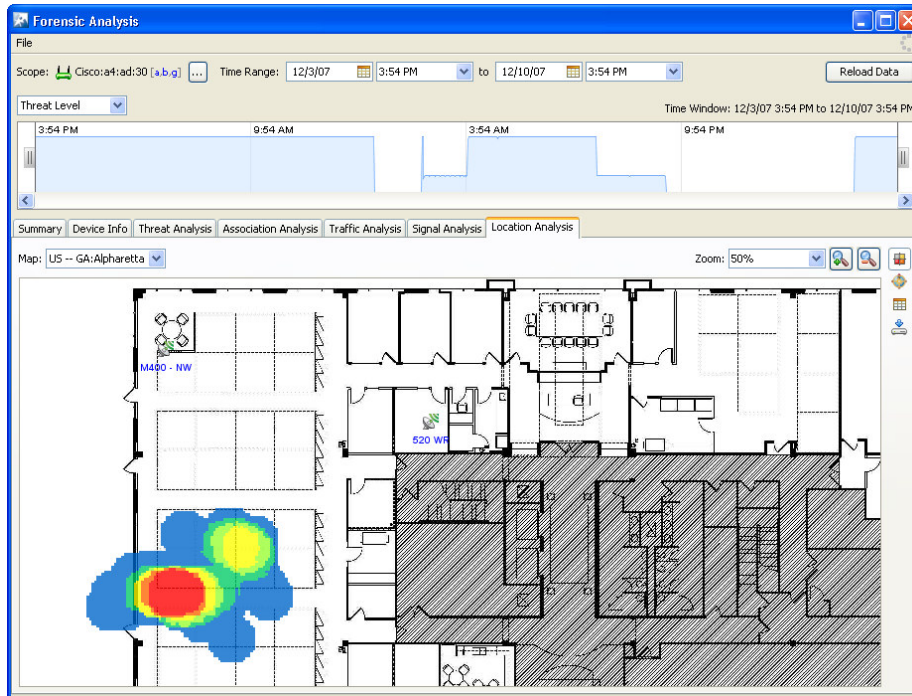


Figure 3: AirDefense Enterprise - Rogue Device Location Tracking

Rogue Termination - 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 using predefined policies. AirDefense uses multiple methods to ensure that the wireless network is secure and protected.

"The company has only a small Cisco WLAN, but it uses AirDefense to monitor WLAN activity. (AirDefense Enterprise) lets network managers immediately and remotely disable a rogue device with a single keystroke." Frederick Nwokobia, Lehman Brothers

AirTermination - AirDefense can protect against wireless threats via the air by terminating the wireless connection between any rogue device and an authorized device using AirDefense patented methods.

Wired-side Port Suppression - The Port Suppression feature enables the administrator to suppress the communications port for any network device. The Port Suppression feature turns off the port on the network switch through which a device is communicating.

Conclusion

With the proliferation of rogue wireless devices and unauthorized wireless connections, it is imperative for organizations to understand the risks caused by these rogue devices and employ 24x7 real-time monitoring solutions to detect, locate and disable these devices. By utilizing patented techniques that use real-time wireless and wired-side information along with historical behavior, the AirDefense system is capable of detecting and eliminating all types of rogue devices with the highest accuracy and effectiveness compared to any solution available in the market today.

About AirDefense

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.**