AN AIRMAGNET TECHNICAL WHITE PAPER

The Wireless LAN and Sarbanes-Oxley Compliance

by Jenny Coupe

WWW.AIRMAGNET.COM

Table of Contents

Introduction

On the face of it, the Sarbanes-Oxley Act of 2002 (SOX) addresses financial reporting and corporate governance in publicly held companies. The penalties for non-compliance are severe. Fines range between $10 million and $100 million[1], and corporate executives can face stiff jail terms[2].

The act covers a broad range of requirements:

- Severely limits the kinds of non-audit consulting services that auditors can provide to their clients.
- Establishes a Public Company Accounting Oversight Board to oversee audits of public companies
- Protects whistle-blowers
- Requires CEOs and CFOs to personally certify that earnings reports and financial statements are accurate
- Provides for increased penalties (including fines and jail sentencing) for corporate executives that commit certain types of crimes
- Requires investment firms to improve the objectivity of security analyst reports
- Bars executives from pressuring outside auditors to issue misleading financial statements

In execution, however, SOX has everything to do with technology, because today's corporate data and communications functions are based almost entirely on computer-based systems.

---

[1] "Make It Work for You," *Computer Weekly*, July 13, 2004 p30.
[2] "Attacking the Hacking From Out," *Journal of Internet Law*, Dec. 2004, v8 i6 p16.

Wireless networks are of particular concern to SOX compliance because they are leaky and easily breached unless adequate defenses are in place. This white paper addresses:

- the components of SOX that are most relevant to the corporation that deploys wireless technologies
- how the WLAN is vulnerable
- a comprehensive approach to WLAN security
- how AirMagnet's intrusion prevention technology can play an important role in ensuring your corporation's SOX compliance.

Sections 302 and 404 of Sarbanes-Oxley

Section 302

Section 302 deals with financial reporting and corporate officers' responsibilities for accurate reporting:

Periodic statutory financial reports are to include certifications that:

- The signing officers have reviewed the report
- The report does not contain any material untrue statements or material omission or be considered misleading
- The financial statements and related information fairly present the financial condition and the results in all material respects
- The signing officers are responsible for internal controls and have evaluated these internal controls within the previous 90 days and have reported on their findings
- A list has been issued of all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities
- Any significant changes in internal controls or related factors that could have a negative impact on the internal controls have been reported

- Organizations may not attempt to avoid these requirements by reincorporating their activities or transferring their activities outside of the United States[3]

Section 404

Section 404 requires businesses to document their financial reporting controls and procedures. This documentation must be comprehensively archived and readily retrievable. During an audit, any document that relates to the auditing process must be retained — even emails and Instant Messaging. (This applies to the auditing firm as well as to the company being audited.)

How Sections 302 and 409 Relate to the WLAN

> *Many IT professionals are learning the hard way that Sarbanes-Oxley has as much to do with IT as it does with determining the quarterly profit margin.*[4]

SOX makes no mention of what constitutes acceptably secure and accurate methods of acquiring, communicating and archiving financial data: this is left to the discretion of the individual corporation. Though the penalties for non-compliance with SOX fall upon C-level executives, the actual implementation of controls falls upon the IT Department. And the most vulnerable element of corporate systems is the wireless LAN.

Wireless networking technology has quickly become integrated into corporate operations — often with little or no security planning. John Pescatore, vice president for Internet security at The Gartner Group, a market research firm

---

[3] http://www.soxlaw.com/s302.htm
[4] "Sarbanes-Oxley is an IT Responsibility Business Opportunity." Brasche, Randy, *America's Intelligence Wire*, Dec 1, 2004 pNA

specializing in technology, estimates that 40% of firms have wireless technology that "they don't even know about,"[5] and some industry experts believe the percentage is even higher. The risk of an unsecured network — whether through insufficient security measures or through unintentional breaches of security — is that data can be either pirated or corrupted by hackers or malicious users. Sarbanes-Oxley auditors will very carefully examine a corporation's approach to WLAN security to see if there are any gaping "back doors" provided by rogue users, un-enforced security policies, or unsecured wireless devices.

WLAN Vulnerabilities

Most WLAN equipment is rated for ranges up to 300 feet. In actuality, many 802.11 cards can be accessed from up to a half-mile away in an urban environment.[6] Without adequate controls and protections, this makes WLANs vulnerable to external and internal attacks.

Internal Points of Weakness

According to Jack Gold, vice president of Meta Group, a Stamford, Connecticut-based technology research firm, the majority of internal security breaches are not

---

[5] "Monsters Inc.: the security risks unleashed by rogue technology may far outweigh any productivity gains," Banham, Russ, *CFO, The Magazine for Senior Financial Executives*, April 2004 v20 i5 p71(3)

[6] "A Survey of 802.11a Wireless Security Threats and Security Mechanisms," Welch, Colonel Donald J, and Lathrop, Major Scott D, Technical Report ITOC-TR-2003-101, Information Technology and Operations Center, Dept. of Electric al engineering and Computer Science, United States Military Academy, 2003.

the result of disgruntled employees attempting to cause damage. Most are caused by well-intentioned employees who are trying to work more efficiently, or who are ignorant of the risks they are creating. For instance, a salesman who uses a nifty new PDA to send emails with sensitive information to co-workers is probably not aware that those emails can be plucked out of the air by a "sniffer" in the parking lot. A hard-working analyst may be using her laptop in a restaurant to catch up on work, without realizing that her laptop is associating with the snoop sitting at the next tale with *his* laptop and Access Point (AP).

Rogue APs are an extremely common phenomenon. Employees who want better performance from the network than they're getting may go out and get a cheap AP on their own dime. APs are usually easy to set up and fairly inexpensive, instantly giving the employee more bandwidth. The rogues are not configured for security in most cases (the user, not understanding the consequences, often leaves the device's default settings turned on), and they are easily detectable by anyone sitting in the parking lot looking for a device with which to associate and penetrate the network.

Another type of rogue AP is when a neighboring WLAN's AP inadvertently associates with your network. While it may be inadvertent, a hacker associating with your neighbor's rogue device can get into your network through the neighbor's WLAN.

The problem with all these scenarios is that unsecured or improperly secured devices open up an invisible highway straight to your corporation's most sensitive data, defeating encryption, VPNs (Virtual Private Networks), firewalls, and most other types of security measures.

External Attacks

Some hackers are just wireless gypsies, merrily looking for a little free bandwidth. Unfortunately, KPMG International, a global accounting and analyst firm, estimates that some 12 percent[7] of them are actively malicious: they either want your data for their personal gain, they want to wreak random destruction, or they have a grudge against the organization. Hackers are an endlessly inventive group, but their attacks can be generally grouped into these categories:

- MAC spoofing
- Denial of Service
- Malicious association
- Man-in-the-middle attacks

MAC Spoofing

Hackers use MAC spoofing to impersonate a legitimate network user. All network interface cards (NICs), like PCMCIA or PCI cards, provide a mechanism for changing their MAC addresses, issued by the manufacturer, that identify a specific device. In many cases, the MAC address is used as an authentication factor in granting the device access to the network, or to a level of system privilege to a user.

The hacker will change his device's MAC address to that of a user and thus gain access to the network. If the hacker is using the MAC address of a top executive with access privileges to sensitive material, a great deal of damage can be done.

Attackers employ several different methods to obtain authorized MAC addresses from the network. A brute force attack uses software that will try a string of

---

[7] "Securing a wireless network means much more than just protecting against hackers," Reed, Chris, *Computer Weekly*, Feb 10, 2004 p30.

random numbers until one is recognized by the network. Another way is to monitor network traffic and fish out the authorized MAC addresses.

Denial of Service Attacks

DoS attacks may be launched merely as a form of vandalism, to prevent legitimate users from accessing the network, or they may be carried out to provide cover for another type of attack. In Layer 1 DoS attacks, the hacker uses a radio transmitter to jam the network by emitting a frequency in the 2.4GHz or 5GHz spectrum. As 802.11 equipment operates at a certain signal-to-noise ratio, when the ratio drops below that threshold, the equipment will not be able to communicate.

In a more common type of DoS attack, the hacker uses a laptop or PDA with a wireless NIC to issue floods of associate frames to take up all available client slots in the AP, severing the AP's association with legitimate users. Alternatively, the hacker issues floods of de-association frames, forcing clients to drop their association with the AP. Either way, if the attack is successful the hacker now controls access to the network.

Malicious Association

The hacker configures his device to behave as a functioning AP. When a user's laptop or station broadcasts a probe for an AP, it encounters the hacker's device, which responds with an association. At this point, the legitimate user's computer can be mined for any and all information, including MAC address, SSID, pass codes, etc. (Figures 1 and 2)

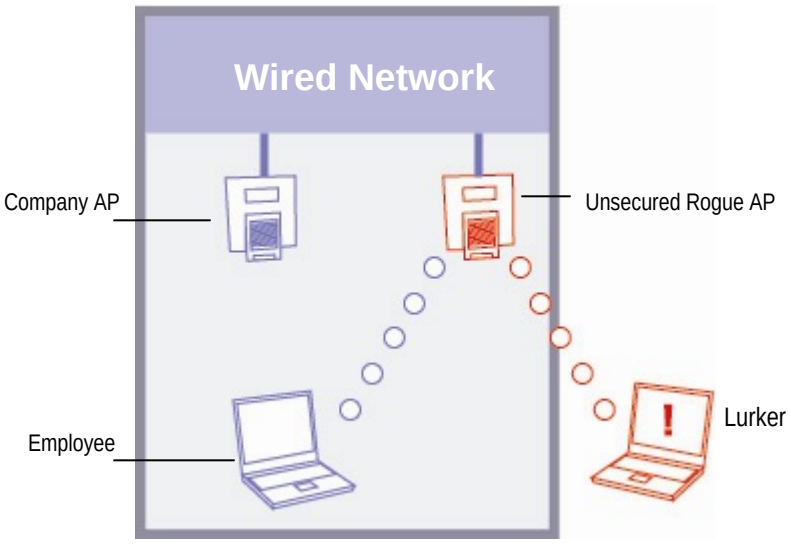


Figure 1: Unsecured Rogue Access Point allows anyone into the network.

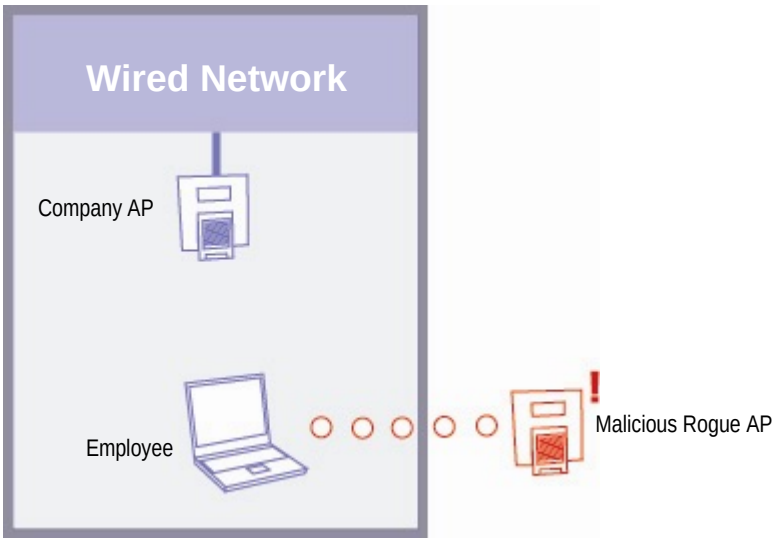
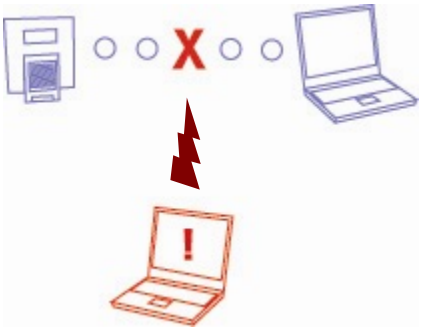


Figure 2: Malicious Rogue AP lures employees away from the corporate wired network.

Man-in-the-Middle Attacks

The hacker sends a de-authorization to a network device, which drops its association to its AP and begins searching for a new AP. It finds the hacker's station (configured to look like an AP), and associates with it. Using the information garnered from the legitimate device, the hacker's device now associates with the legitimate network AP and the network passes through the rogue user's device, allowing him to change or steal data at will. (Figure 3)

1. The attacker monitors both the AP and Client, picking up their MAC addresses and authentication information in the process.



2. The attacker associates with the AP and Client.

3. Attacker spoofs MAC addresses to fool both the AP and client into connecting to him.

Figure 3: The hacker using the man-in--the-middle attack masquerades as a legitimate user to network devices and clients.

The WLAN and SOX Compliance

WLAN security in the age of Sarbanes-Oxley demands a multi-tiered approach. Corporations must view WLAN security as a matter of implementing the right security technologies, staying abreast of hacker innovation, and changing employee behavior by educating employees about security policy. (Once people understand the implications of breaching policy, they are much more likely to comply.)

The National Institute of Standards and Technology (NIST) recently issued recommendations for securing the WLAN and other wireless connections, such as Bluetooth (an open specification using the globally available 2.4 GHz frequency to

enable short-range wireless connections) and handheld devices.[8] NIST recommendations include:

- Maintaining a full understanding of the topology of the wireless network.
- Labeling and keeping inventories of the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

In addition to these measures, AirMagnet recommends implementing a robust intrusion prevention system that will prevent attacks from getting underway in the first place.

---

[8] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology" Karygiannis, Tom and Owens, Les, NIST Special Publication 800-48, U.S. Dept. of Commerce, Gaithersburg, MD.

Wireless Intrusion Prevention

Even if a corporation faithfully follows all of NIST's guidelines, takes the time to educate employees about security protocols, and enforces security policy rigorously, security cracks in the wireless network will still occur. A wireless network is a dynamic system. It is extended and reconfigured on a regular basis to meet the needs of a changing environment. And there is always at least one cowboy employee who thinks that rules are made for other people and ignores the guidelines for configuring wireless devices.

Given that even the most rigorously policed WLAN will develop leaks, it is imperative to have an intrusion prevention system overlay in place. An effective intrusion prevention system monitors your WLAN to allow you to see what's happening in your airspace at all times, assures you that security policies are being followed, sounds the alarm when an intrusion or policy violation is detected, and isolates and cuts off any unauthorized device or user. Wireless LAN infrastructure devices come with some built-in monitoring capabilities, but a specialized overlay monitoring product will provide a richer set of capabilities.[9]

It is essential to be able to detect rogue and/or neighboring APs associated with your WLAN. Once rogues are detected, it is critical to be able to physically locate these APs and take them out (or go have a polite discussion with the administrator of the neighboring WLAN). Locating a rogue AP requires triangulation, made possible by physically locating intelligent sensors around the area covered by the WLAN. Intelligent sensors detect the rogue AP or user, sound the alarm to the network administrator, and isolate the AP until it can be physically removed.

---

[9] "Watching the Waves," *Network Computing*, Mar. 4, 2004

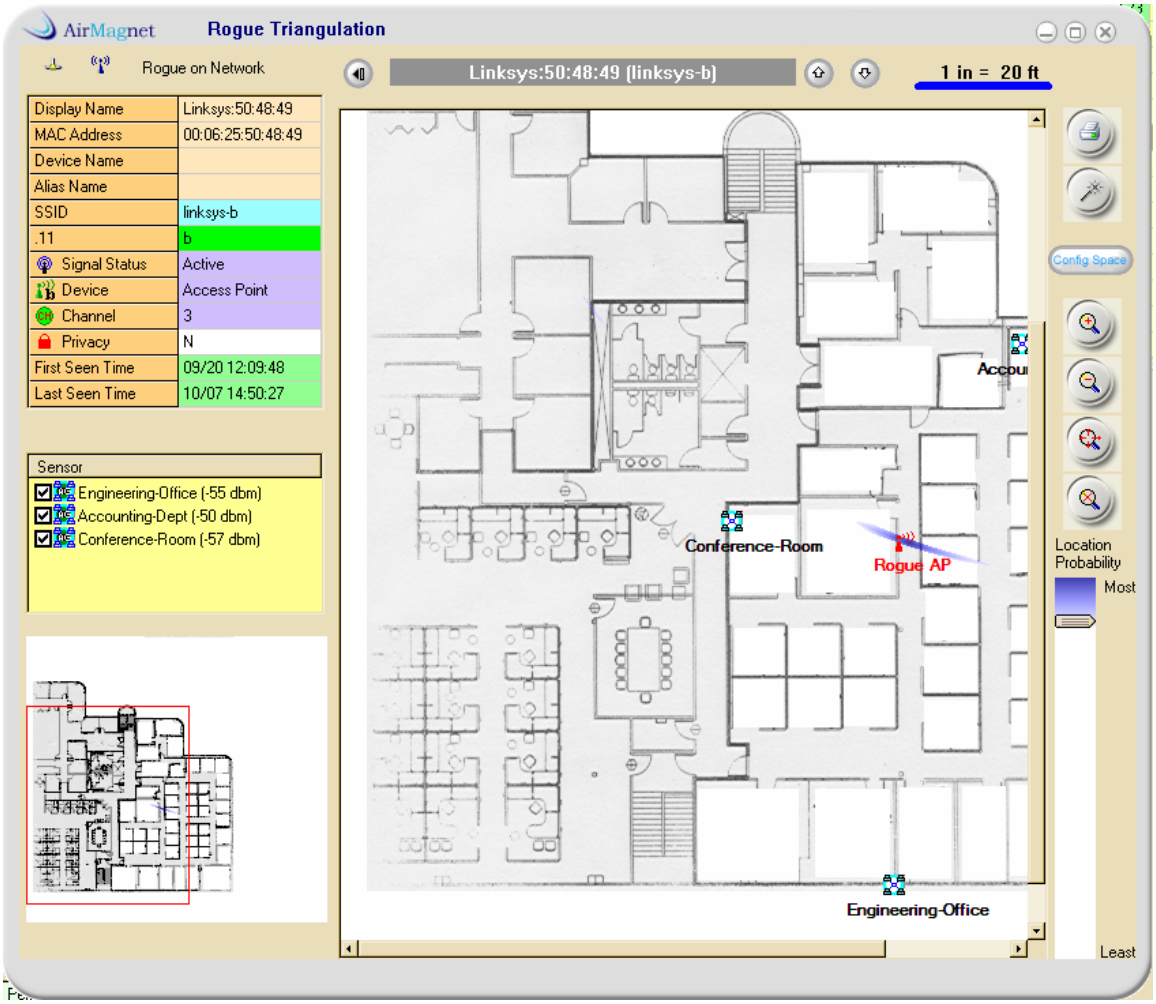


Figure 5: ***Triangulating Rogue APs.*** *A screenshot from AirMagnet Enterprise™ shows how AirMagnet's SmartEdge Sensors geographically distributed triangulate and pinpoint the location of a rogue AP. Once the rogue's physical location is known, it can be removed without delay.*

SmartEdge Sensors can also monitor users' devices and determine whether a user is inside or outside your network perimeter. If a user is outside the perimeter – whether the rogue user is a hacker or a neighbor who has unwittingly associated

with your WLAN — the sensor will generate an alarm and isolate the rogue from the network.

One of the most useful aspects of a robust intrusion prevention system is the ability to set security protocols, and modulate the system's response to protocol violation. For instance, the system response to a low-level violation such as multipath detection, which could be merely a malfunctioning AP, might be just an email notification to the administrator, or a log notation. But a high level violation such as a user detected outside the network perimeter might result in a phone call alert.

It's essential to be able to manage WLAN security from a centralized console, where all information is quickly available to the administrator. The system should provide detailed information, such as activity at any single sensor, specifics on any alarm, and a view of network traffic at any given time. Troubleshooting tools, detailed logs, and the ability to measure network performance against established standards are all necessary to good network security. It is especially important to get reports in highly granular detail, customized to the needs of the network administrator. These reports are key to studying network performance and usage over time, pinpointing and eliminating potential trouble spots *before* they become problems.

And the network administrator needs an intrusion prevention system to be flexible. For instance, access privileges granted to a C-level executive need to travel with that executive when he or she works from home or leaves on a business trip. The administrator must be able to configure related alarms into a coordinated policy instead of being limited to a fixed hierarchy. When the network is expanded, the intrusion prevention system must be scaleable to grow with it.

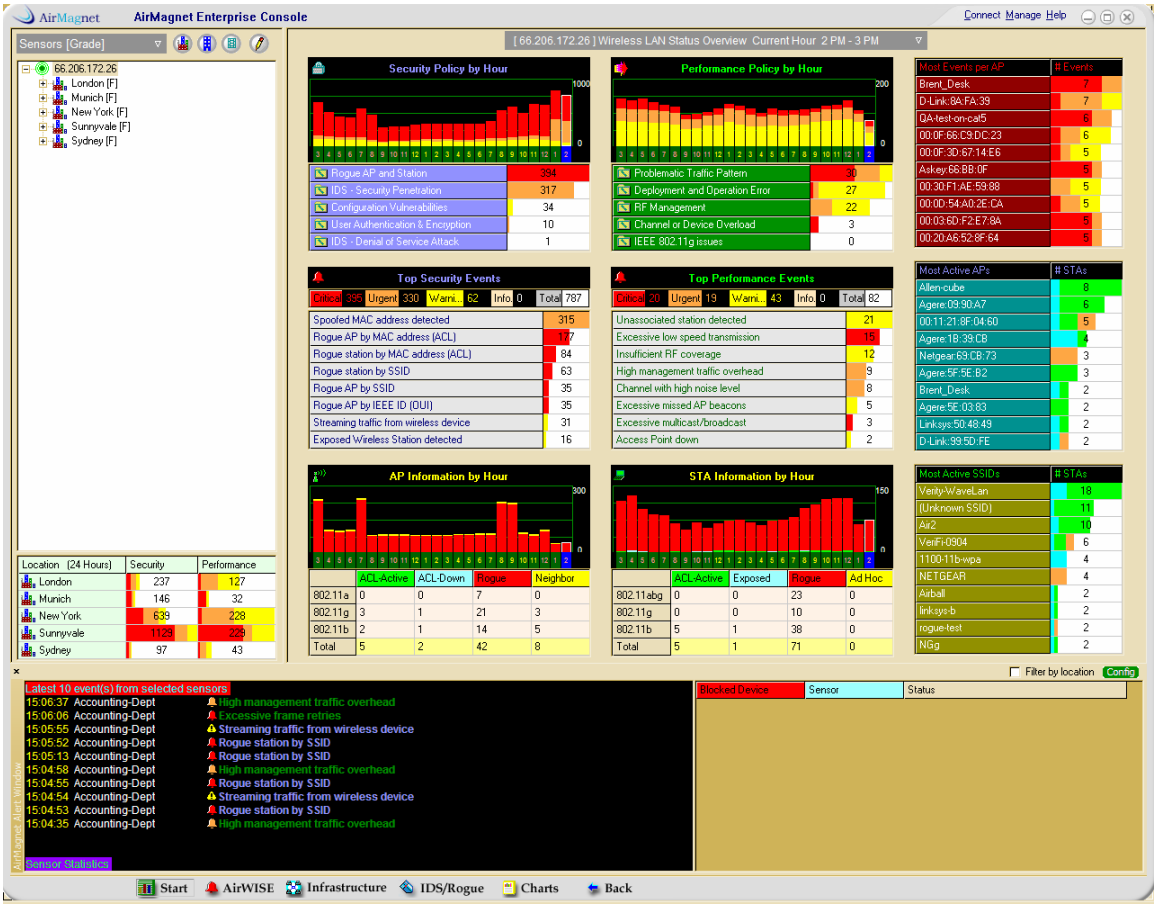


Figure 6: ***24/7 Monitoring.*** *The AirMagnet Enterprise™ console shows WLAN activity at any given point in time. The system administrator can see at a glance which alarms have been given and when they occurred, traffic patterns, network performance and more. The system's granulation is very fine, allowing the administrator to analyze network activity and performance at many different levels.*

Intrusion prevention is enhanced if the system has mobile detection ability. Wireless LANs are in a constant state of flux by their very nature. Users move around from location to location. New devices can introduce RF signals that didn't

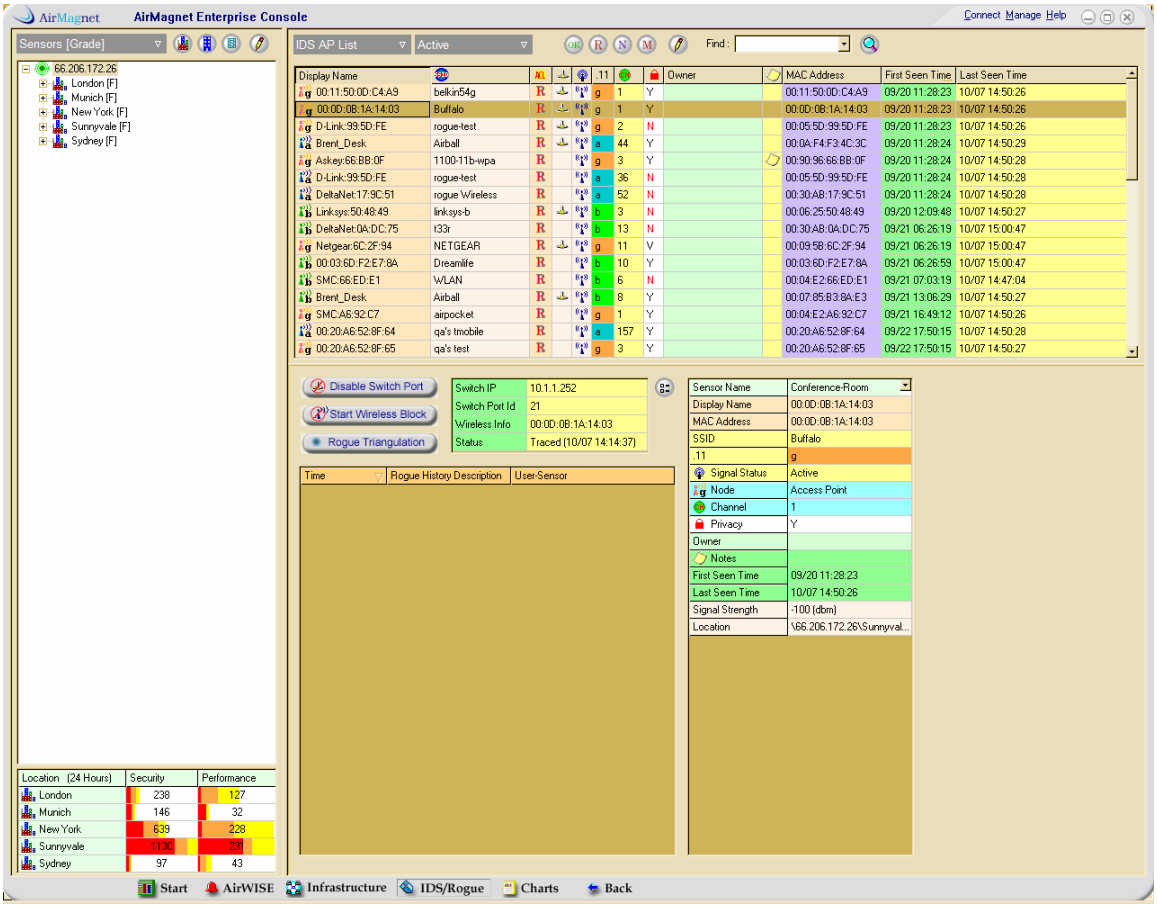


Figure 7: ***The Three D's of Intrusion Prevention.*** *Any wireless network, no matter how well protected, can be threatened by rogue devices. The key to preventing intrusion by rogues is the ability to Detect, Disable, and Document every rogue before it can cause any damage. AirMagnet Enterprise provides a complete approach to rogue management including: multiple detection mechanisms that immediately expose every rogue; an active blocking suite that disables the rogue both on the wireless and wired side; and a dedicated rogue page that provides consolidated details on every device, including its physical location on a map, wired trace analysis, event history and more.*

exist the day before. Users can create dead spots in the network without realizing it. For all these reasons, it is sometimes necessary to be able to make an on-the-spot investigation with a handheld extension of the intrusion prevention system that can perform real time readings and analysis.

AirMagnet Enterprise: A Complete Security System for the Enterprise WLANAirMagnet Enterprise tames the complexity and exposure of a wireless LAN with a true zero-tolerance approach to wireless security that is tied to the policies and needs of your business. AirMagnet Enterprise detects every threat in the network, worldwide, and then automatically takes action with multiple layers of automated threat response. An intuitive global interface provides full disclosure of all wireless events, making it easy to make the right decisions while cutting through the time required to manage your network. The end result is a system that brings simplicity, accountability, and bulletproof defenses to any wireless investment.

Detection

AirMagnet Enterprise automatically detects and alarms dozens of types of wireless intrusions, including rogue APs, DoS attacks, spoofed MAC addresses, the use of freeware probing tools and much more.

Prevention

AirMagnet Enterprise gives an alarm appropriate to the detected problem, but automatically moves to isolate and cut off rogue APs and rogue devices before the network is successfully penetrated. Multiple detection mechanisms identify rogues on the basis of MAC address, vendor type, wireless band or SSID. When the system operator arrives on the scene, AirMagnet Enterprise provides tools to physically locate suspect devices so they can be physically removed.

Vulnerability Assessment

WLANs are never static. Because they change from day to day, AirMagnet Enterprise performs a continuous vulnerability assessment of the network, detecting a host of subtle weaknesses that could result in network penetration. The system alerts IT immediately when it detects a vulnerability.

Control Over Security Policy

Even one AP or station that does not adhere to security policies puts the entire WLAN at risk. AirMagnet allows you to deploy different security strategies for different individuals or different locations, and monitor for 100% compliance. AirMagnet Enterprise offers 130+ security and performance alerts organized into a logical hierarchy, allowing managers to create and manage a coordinated policy. Each policy level and alarm comes with expert explanation and advice. Alarm notifications can be set to escalate in urgency if a problem gets worse.

About AirMagnet

Founded in 2001, AirMagnet, Inc., provides the most trusted WLAN management and security software systems for the enterprise in handheld, laptop and distributed configurations. Used by IT professionals at more than 3,000 companies worldwide in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available on the Web at http://www.AirMagnet.com