INFORMATION SECURITY®

Even if you don't have an unauthorized WLAN, you need protection now that your users are...

unplugged

There are two kinds of wireless networks: those you know about and those you don't. Wireless adapters have become commodities, embedded in every laptop moving in and out of your organization. Whether you are trying to enforce strict no-wireless policies or protecting your growing wireless infrastructure as an essential part of your business, you can't afford to allow unsecured Wi-Fi connections on your network.

Wireless security products have rapidly evolved and matured to meet the rigorous security demands of the enterprise. When wireless IDSes/IPSes first hit the market, they were little more than RF scanners designed to identify 802.11 traffic within close proximity to their sensors. Now, they are overlay solutions integrated into existing WLAN infrastructure and mobile or hand-held devices. They sport a multitude of rich features such as compliance reporting and site assessment for sensor placement, in addition to accurately detecting and blocking numerous wireless attacks.

In this review, *Information Security* evaluates four standalone wireless IDS/IPS products in the lab and in a live testing environment. These products are AirDefense Enterprise 7.0 from AirDefense; AirMagnet Enterprise 6.5 from AirMagnet; AirTight Networks' SpectraGuard Enterprise 4.0; and Network Chemistry's RFprotect 5.0.

We then graded each product based on its ability to identify and thwart common wireless attacks, as well as its features, such as policy enforcement, tracking and blocking, response automation, reporting, installation and ease-of-use (*see "Making the Grade"*).

Total Coverage

A comprehensive site survey is absolutely critical to planning a successful wireless IDS/IPS deployment. Even the most sophisticated tools won't protect you if there are gaps in your defenses.

Each of these products includes site survey tools to determine the best locations for RF reception, helping you place not only the sensors but the wireless access points (APs) to best advantage. Although wireless IDS/IPS vendors can tell you the basic coverage of their sensors, building materials and conditions impact bit and error rates--and the same goes for APs. Metal shelves, microwave ovens, window blinds, doors, HVAC systems and power/network distribution closets, etc. can impact 802.11 signals.

AirTight's SpectraGuard Planner, AirMagnet's Surveyor and Network Chemistry's RFprotect Survey (all tools included with their base products) provide detailed planning for WLAN IDS/IPS deployment. AirTight goes a step further by offering professional services to create a sensor placement blueprint based on floor plan/coverage area. AirDefense Mobile only offers limited RF planning tools in the form of real-time discovery with capture file playback for later analysis.

AirTight's tool was the easiest to use and was much more granular than the others, accounting for factors such as construction materials and an extensive list of wireless equipment. AirTight and AirMagnet also provide the ability to simulate WLAN deployments for best RF coverage. AirMagnet Surveyor has a nicer interface than Network Chemistry, but their functionality is about the same–delivering important

information such as coverage area, RF signal strength, data rates and packet loss.

A relatively new feature that simplifies sensor deployment is power over Ethernet (PoE), which eliminates the need for an additional power adapter for each sensor. That translates into significant cost savings and performance enhancement; sensor placement isn't limited to nearby power sources or installing electrical outlets. All but AirDefense are PoE-compliant.

Deploying the Sentinels

AirTight presented a painless and secure installation and excellent configuration options. Each of the others had some "gotcha" that hindered installation and configuration.

We were particularly pleased that AirTight forces the use of a strong administrative password. It can also enforce policy on individual subnets; for example, there could be a subnet for employees, one for vendors/partners, one for contractors and one for guests.

The AirTight and AirDefense appliances were initialized with basic network settings using a command-line interface through a serial connection; the administrative consoles were accessed through a Java-based GUI using a secure browser connection. Setup wizards took us through the basics of access point and client classifications, 802.11 security and intrusion detection/prevention policies. AirMagnet and Network Chemistry are both software-based, so the configuration wizards start from the moment of installation.

Deciding what to monitor and effectively managing all RF signals in an enterprise environment are daunting tasks.

Overall, we found both AirDefense and AirMagnet more complex and time-consuming than AirTight to install and configure. (AirDefense bills itself as a plug-and-play configuration, but we didn't find this to be the case.) Instant network device synchronization was also supposed to be an AirDefense feature; however, during our testing several of the APs from less common vendors had to be reset in order for AirDefense to identify them.

The configuration choices were pretty much the same across the board for security policies, letting us limit access based on security settings (WPA, WEP, AES), protocol (802.11a/b/g), SSID and AP vendors. Since the practical testing environment had multiple AP vendors and mobile users with older equipment capable of only 802.11b and WEP, our security settings were set to SSID and the use of WEP--the bare minimum for wireless security.

AirMagnet suggests installing its Enterprise Server on a machine solely dedicated to running only its services; if you use Microsoft SQL Server with AirMagnet Enterprise Reporter, it needs to be installed on another machine. We'd prefer one hardened, rack-mounted appliance.

Network Chemistry's initial installation and configuration was somewhat confusing. There are multiple choices on wizard windows that use inconsistent terminology (client vs. console). Auto-provisioning the sensors through either DNS or DHCP required additional steps such as auto-generating Encrypted Transport Layer keys, DNS addressing schemes and vendor-specific DHCP tags.

For large, distributed installations, this functionality is probably worth the effort to figure out, but for our practical testing, we manually configured each sensor through the console by simply clicking the "Add Sensor" button. The configuration from there was similar to setting a network adapter on any Windows-based system using DHCP or by inputting static IP settings. The template settings, which let us set up a single sensor and then load those settings on to the other sensors, made the job fairly painless.

There is a lot of neat technology in Network Chemistry's software, but the details will challenge anyone except an RF engineer to set it up.

On the Radar

Deciding what to monitor and effectively managing every RF signal in an enterprise environment are daunting tasks. Given the proliferation of wireless devices, this includes tracking both authorized and unauthorized RF signals in your airspace, and investigating and halting potential attacks.

AirTight's dashboard stood out for its ability to give you a quick assessment of your network security, and then easily drill down for details. For example, if you want to see APs using WEP, you can click on the appropriate column for a list of all the devices according to type of encryption.

AirTight's dashboard displays quarantined, known and unknown devices, as well as a security scorecard that rates the WLAN as either secure or vulnerable. Security scorecard settings can be customized so that if sensors pick up a neighboring WLAN that isn't a threat, the scorecard won't display your network as vulnerable. In the quarantine section on the dashboard, there's a button that pops you directly into the IPS policy editor for quick changes–such as when the boss arrives with a new wireless PDA and is shut out of the network. A colored bar graph gives a real-time view of what is taking place on the WLAN. Within seconds of launching our DoS attack, for example, we saw the scorecard change from green to red and the bar for DoS attacks rise. We didn't have to read any numbers or descriptions to know we had trouble.

AirMagnet's console cleanly displays all deployed sensors and policies in a tree format on the left side of the console, with one-click access to editing tools at the top of the display. However, we really had to concentrate to wade through the wealth of information–statistics displayed through both numbers and bar graphs of security events, policy violations and WLAN performance–to figure out what was happening on our network.

We had to use the menu options at the bottom of the console to access a listing on rogues, infrastructure details and AirWISE, which displays current alarms and policy violations, and their location, along with the policy and infrastructure tree similar to the console page. We actually preferred the AirWISE display to the main console.

making the grade

Vendor	AirDefense AirDefense Enterprise 7.0 www.airdefense.net Starts at $8,975	AirMagnet AirMagnet Enterprise 6.5 www.airmagnet.com Starts at $8,995	AirTight Networks SpectraGuard Enterprise 4.0 www.airtightnetworks.net Starts at $7,500	Network Chemistry RFprotect 5.0 www.networkchemistry.net Starts at $4,398
Ease of Installation & Configuration (how easily the product can be deployed and configured) 10%	B	B	A	B
Policy Configuration & Enforcement (effort required to create an enterprise wireless policy, and the granularity with which it could be enforced) 20%	A	A	A	C
Automatic Classification & Blocking (how effectively threats are classified and/or blocked; false positives were considered) 20%	A	A	A	B
Overall Security Features (how many wireless threats and vulnerabilities are effectively mitigated) 30%	A	A	A	A
Monitoring, Alerting & Reporting (how well product presents real-time information, sends alerts of suspected issues and generates useful reports) 20%	A-	A-	A	B+
The Verdict	**A-** Brings mature security features and offers extensive regulatory compliance reporting capabilities.	**A-** Significant improvement over previous version with better rogue reporting and triangulation.	**A** Best tool on the market for real-time RF management and sensor placement planning for full coverage.	**B+** An affordable solution, delivering rich security features; weak on policy configuration.

AirMagnet's Rogue View screen lists all detected rogue devices with detailed information about them in a single view. AirMagnet showed significant improvement in triangulating the location of rogue devices compared to an earlier review, almost matching the accuracy of the other three products, all of which tracked offending devices to within a few feet of their actual location.

AirDefense's console was the easiest to navigate, despite the incredible amount of information displayed, but was visually overwhelming. AirDefense provided an extensive overview of the entire WLAN, with individual statistic areas for associations, APs and clients, signal strengths and traffic (by channel and amount transferred). We would have preferred less information up front, with the ability to drill down as needed.

Network Chemistry's console lacked the polish of the competition, but we liked the simple display that instantly showed the critical security factors of our WLAN, including a summary of security alerts (intrusions, threats, vulnerabilities and attacks), the most active devices, a summary of operational alerts (new clients and APs), number and status of sensors, an inventory of connections and their status, and a graphical breakdown of the spectrum (802.11a/b/g). More detailed information was available with a single click on a tab.

Powerful Protection

All four products detected everything we threw at them–including a host of common attacks .

The way they process the threats is worth noting. AirMagnet and Network Chemistry perform in-depth analysis at the sensor and then send an aggregate back to the server. There is a distinct advantage to this method because, even if the central server goes down, the sensors continue to protect the WLAN. AirTight and AirDefense perform minimal analysis at the sensor, sending collected data back to the server for more extensive analysis and correlation. AirTight allows users to upload SpectraGuard Sensor software onto other vendors' access points, turning them into SpectraGuard Sensors and saving both time and money.

Given the extensive coverage of enterprise WLANs, creating an access policy can be challenging, especially for organizations using a mix of equipment from multiple vendors. The granularity of policy configuration for the tested products covered a vast array of choices–individual and global settings, channel, encryption method, vendor and behavior. For example, we configured our products to ignore traffic that was not trying to connect to any devices associated with our WLAN.

This is critical for enterprises that operate in areas in which other WLANs can overlap–such as in high-rise office buildings and business parks.

AirTight shone with rapid response time for identification and extensive details of all attacks.

Network Chemistry responded to our attacks faster than AirDefense and AirMagnet, but didn't provide their robust level of detail. Its alerts offered minimal information, such as the alert type (e.g., rogue AP), the offending address, the location of the nearest sensor, a time and date stamp, and some canned information about the type of alert. The rest of the products provided much more information about the their alerts, including the device name, MAC address, amount of data transferred, duration of the event and other devices involved.

All the products block rogues on both the wired and wireless side. Wireless blocking is done by signal jamming and can be quarantined for a specified amount of time or until the alarm is acknowledged. Wired threats, such as rogue APs, can be traced and blocked at the switch port.

Unlike wired IDS systems, wireless IDS/IPS systems don't need an extensive amount of tuning or frequent signature updates to reduce false positives. Their custom-tuning is much more intuitive and GUI-based than, say, writing Snort signatures. In fact, during our testing, the only false positive returned was from AirMagnet on an older, D-Link 802.11b AP.

No Wireless Allowed

One of the strongest business cases for these stand-alone solutions is their ability to identify unauthorized WLANs in organizations with a zero-wireless policy.

Practically every laptop shipped with Windows XP tries to connect with a wireless network from the moment the it is powered on. With a $20 off-the-shelf access point, an employee can punch a hole in your firewall in less than five minutes by simply plugging into the corporate network. Likewise, in high-rise and campus environments, where existing WLANs often overlap, peer-to-peer networks and inadvertent association from your employees' wireless laptops open your organization to many vulnerabilities.

We set up each product to identify all RF traffic detected. Rogue APs, laptops broadcasting in ad hoc mode and other private WLANs in proximity to the sensors were immediately identified by each product. We were particularly impressed when the AirTight sensor picked up a passing delivery truck's barcode scanner.

Considering its accurate detection at such a low cost, Network Chemistry would be a good choice for implementing a no-wireless policy.

Alerting and Reporting

No longer chained to their consoles, managers are demanding more ways to receive critical alerts when their networks are under siege, as well as generating reports for auditors and management.

AirMagnet topped our list with nine different ways to deliver alerts, which can be set based on their individual thresholds of importance. AirDefense and AirTight have similar options, but Network Chemistry trailed the pack.

Logging and reporting has become critical due to strict audit requirements and government regulations. It's no surprise that wireless security measures are subject to increasing scrutiny.

Each of the products provides enterprise-class reporting features. AirDefense has the most robust reporting, offering an exhaustive amount of data (well over 200 data points per device) on a minute-by-minute basis. Its reports include historical analysis and trends, and those based on device, security and policy compliance.

Although Network Chemistry doesn't have such extensive capabilities, its strength lies in the ease at which reports can be set up, and automatically generated and distributed.

AirMagnet's compliance reporting was the most comprehensive, providing reports for auditing requirements associated with DoD 8100.2, HIPAA, SOX and GLBA.

AirTight provides four reports specific to regulatory compliance, in addition to commonly requested reports, such as detailed event and sensor listings. It excels in its flexibility to customize and edit templates, and to create templates from scratch.

Attractive Options

It's hard to go wrong with any of these choices. All of them are close in terms of features in functionality.

AirTight's SpectraGuard was the easiest to deploy, configure and manage. We were instantly alerted to attacks and vulnerabilities. With the maturity of their products, AirDefense and AirMagnet can meet the rigorous demands of the enterprise, but also have developed an air of complexity. Network Chemistry's RFprotect is a no-frills wireless IDS/IPS at a price that makes it a good deal, especially for organizations looking to enforce a zero wireless policy.

AirTight
NETWORKS™