



CMP

United Business Media

Network Computing

6.232005 | WWW.NWC.COM

For IT By IT

TIME TO

TIGHTEN

THE WIRELESS NET

BY FRANK BULK

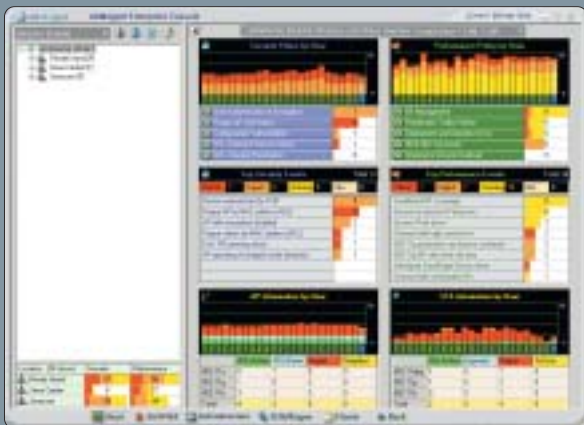
DISTRIBUTED WIRELESS SECURITY MONITORS PROVIDE THE RICHEST SET OF FEATURES FOR LOCKING DOWN YOUR WLAN. AIRMAGNET HELD ON TO OUR EDITOR'S CHOICE BY A HAIR, WHILE NETWORK CHEMISTRY SNAGGED A BEST VALUE AWARD



Remember those warm summer evenings, when you'd try to catch fireflies buzzing around the yard? Remember the frustration when you were just about to grab one, and as you lunged the firefly stopped glowing, so that all you had to show for your effort was an empty hand?

Distributed wireless security monitoring is a little like that, minus the squashed lampyridae. Unlike wired IDSs (intrusion detection systems), where you can put a wired probe on each network segment and your Internet uplink and depend on a well-defined signature set to find the bad guys, wireless security monitoring requires time-sliced behavior. Time-sliced because a wireless sensor or probe can listen to only one channel at a time, which means that if the sensor is set to scan 14 channels in the 2.4-GHz range, it will see only one-fourteenth of your wireless activity at any one time. A single snapshot of wireless traffic might be symptomatic of any number of attacks, which longer-term monitoring will identify.

This time out, we limited our distributed wireless security monitoring review to overlay products. Our recent review of enterprise WLAN vendors (see "Wireless LAN Battle Plan," at ID# 1603f2) demonstrated that though some enterprise players, including Airespace and Aruba, have enhanced their offerings' security functionality in the past year, they don't offer the breadth of features found in point-



AirMagnet Enterprise's dashboard displays colorful graphs and a table describing the wireless network's key trends and stats.

specific products. Most integrated devices can find rogues, some have a few dozen alerts or alarms, some perform rogue mitigation, and all provide insight into performance and their own configuration policies, but the integrative approach is problematic: Wireless client performance will drop if the access point spends too much time listening to other channels. If you're worried that dedicated overlay products aren't looking at the RF enough, how can access points (APs) performing double duty do better? Additionally, enterprise security and network monitoring groups might balk at having an inline system performing airspace analysis. An overlay system that's not dependent on the WLAN and that can be securely segmented, perhaps over VLANs, and controlled by a security operations or enterprise networking group will be more palatable. We're not completely dissing integrated systems—many IT managers swear by them. But very security-conscious organizations, highly regulated companies such as those in financial services and health care, and government facilities dealing with sensitive information should consider an overlay approach.

We put out a call for distributed WLAN monitoring systems that are WAN-optimized for geographical and distributed operation and provide, at minimum, wire-side and wireless rogue-device detection, intrusion detection, RF interference detection, user and group traffic monitoring, and performance monitoring in the 2.4-GHz and 5-GHz ranges.

Of the 11 vendors invited, five took on the challenge. Industry veterans AirDefense and AirMagnet, newcomers AirTight Networks and Highwall Technolo-

gies, and price leader Network Chemistry all supplied gear to our three testing sites: our Syracuse University Real-World Labs® and partner labs in Iowa and Rhode Island. Among the other invitees, BlueSocket and Network Instruments said their latest offerings were not fully baked, and CironD, Newbury Networks, Red-M and WildPackets all said their products did not meet our criteria.

Evolution

We last reviewed WLAN security products 15 months ago. This time, we took our testing to the next level by evaluating some sophisticated features as well as WAN and other performance metrics. Fortunately, the vendors whose products we tested have also moved ahead: Rather than rest on their laurels, they're working to help companies wring extra value out of their overlay systems. Features such as security-policy templates and detailed forensic-traffic reporting can save harried IT staffs hundreds of hours. Given that most security initiatives defy obtaining a hard return on investment, features that boost compliance with GLBA (Gramm-Leach-Bliley Act), HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley and other regulations can only help, and this is one area where point-specific products shine.

To get a better feel for what it's like to manage a truly distributed wireless security monitoring system, we stationed sensors at our labs and with SANS Institute wireless security researcher Joshua Wright, best known for creating the *asleep* attack. Our partnership with Wright yielded some very interesting findings, which we summarize in "Doctrine of Containment" on

REAL-WORLD
LABS®

REPORT CARD

Wireless Security Suites

	AirMagnet Enterprise	AirDefense Enterprise 6.2	Network Chemistry RFprotect System 4	AirTight Networks SpectraGuard Enterprise 3.0	Highwall Technologies Enterprise 3.0
SECURITY POLICY MONITORING & ENFORCEMENT (40%)	4	4	3.5	3.5	2.5
INSTALLATION, ARCHITECTURE & DESIGN (20%)	4.5	4.5	4	3.5	2.5
COST OF OWNERSHIP (15%)	4	3	5	3.5	4
PERFORMANCE & CONFIGURATION POLICY MONITORING (10%)	4.5	4.5	3.5	2.5	2.5
SENSOR/PROBE DESIGN & IMPLEMENTATION (10%)	4	4	4.5	3.5	3
LOCATION CAPABILITIES (5%)	4	3.5	3.5	4.5	3
TOTAL SCORE (100%)	4.15	3.98	3.93	3.45	2.80

A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5 A-C GRADES INCLUDE + OR - IN THEIR RANGES. TOTAL SCORES AND WEIGHTED SCORES ARE BASED ON A SCALE OF 0-5.



SECURITY POLICY MONITORING & ENFORCEMENT rates alarms, rogue discovery and rogue containment.

INSTALLATION, ARCHITECTURE & DESIGN rates the complexity of installation and configuration as well as quality of design and GUI, scalability, reporting and ability to handle link failure.

COST OF OWNERSHIP scores are based on our three pricing scenarios.

PERFORMANCE & CONFIGURATION POLICY MONITORING rates the accuracy and detail of performance metrics as well as ability to define a variety of security policies.

LOCATION CAPABILITIES rates how accurately the products could pinpoint the whereabouts of rogue wireless devices.

Customize the results of this report card using the Interactive Report Card®, a Java applet, at www.nwc.com.

page 6. Our experience with a mixture of public and NAT connections made us incredibly sympathetic toward our comrades who've deployed wireless to hundreds of remote locations, but we learned that given a solid understanding of your network and adequate preparation, it is possible to "unplug and play."

AirMagnet Enterprise 5.2 Last time around, we

B+ evaluated the beta 4.0 release; now, just 15 months later, Enterprise has been upped to version 5.2. At first glance, the product looks

and acts much the same: It still runs a Win32-based system using Microsoft SQL server as its back end; its stand-alone laptop version inherits a Win32 interface similar to that of the appliance; and it uses the same Senao sensor, which still doesn't support standards-based PoE natively. But once we delved deeper, the improvements became apparent: Automated intrusion response, both on the wired side using switched port disabling and on the wireless side with RF-containment, is now included. Compliance reporting covered DoDD (Department of Defense Directive) 8100.2, GLBA, HIPAA and SOX. Also new are map-based location services, a time-based ACL (access-control list), and the ability to add notes and assign owners to devices.

AirMagnet didn't send us an appliance for testing. Rather, we performed a fresh install of the product on the laptop the company had supplied for our last review; the PC had Microsoft Windows 2000, SQL and IIS pre-installed. A wizard asked us to choose a system policy that best matched our desired configuration; examples included enterprise, government and no wireless. After we completed a few initial steps, AirMagnet's dashboard opened up and displayed a colorful grouping of graphs and tables providing key statistics relating to the health of our wireless network.



To set up the sensors, we had to attach a serial cable and configure the device's IP network information, management server and secret key that is used to encrypt the communication flow between the sensor and server. In contrast to AirDefense, which performs most analysis on the server, AirMagnet accomplishes most of its analysis on the edge device, the sensor. Although there's much debate in the vendor community about which approach works best, it's never an either-or implementation. In AirMagnet's case, patches and feature enhancements will almost always necessitate a software upgrade of the sensor, something we experienced during our tests. While upgrading our two remote sites, a local Internet link failure threw us for a loop. We recovered one sensor with some late-night technical assistance; by the time we had it working, the AirMagnet sensor at the other site had restarted and successfully completed the download!

Having provided integration with AP management vendor AirWave for some time, AirMagnet recently added data exchange with Cisco's WLSE and a generic XML interface and support for Cisco's RDEP (Remote Data Exchange Protocol), also based on XML. AirMagnet provides account integration with Microsoft's Active Directory and OpenLDAP to allow for a single password store.

Port detection of rogue APs outperformed Network Chemistry, the only other vendor that uses its sensors as wireless clients to assist in evaluating whether rogues were on or off the network. Although AirMagnet Enterprise had trouble identifying the switched port for two of the four wireless routers in our test bed, some of the other products tested required third-party assistance or didn't support the feature at all. While the system's wireless rogue AP and client containment were effective, it transmitted the most packets of the systems tested, consuming much more bandwidth than the others.

AirMagnet was first known for its PDA analyzer,

GET HIP TO FIPS 140-2

Wireless IDSs regularly monitor data that could be very valuable to attackers: SSIDs (Service Set IDs), device MAC addresses, channel usage and sometimes even packet captures. Encrypting data flow between the sensor and server is one way to hamper man-in-the-middle attacks. But not all cryptographic implementations are secure, so government agencies and contractors that deal with information categorized as sensitive but unclassified must certify their IT products with FIPS 140-2 (per OMB circular A-130). Focusing mostly on the devices' cryptographic modules, there are four lev-

els of security ranging from no physical security mechanisms to requirements for the device to be tamper-resistant and to include physical protection around the cryptographic module. Just because a product claims FIPS 140-2 certification doesn't mean the whole system has been evaluated. Areas within the management platform, such as identification (who are they?), authentication (is the user who he says he is?) and access control (what functions can the user perform?), may not have been examined.

AirMagnet is the only wireless IDS vendor that has submitted its

sensor and the sensor's version 5.2 software load for FIPS 140-2 certification. It's in the second of five stages required for final and full certification (of 143 devices submitted, only eight had completed all five stages at press time). AirMagnet says submitting its sensor for review was required for a recent deal with the military. The details of FIPS 140-2 and surrounding regulations seem to exempt most wireless IDS vendors from required certification, but verticals such as the military and financial services will appreciate a system that has gone through a formal examination process.

which it followed up with a standalone laptop device. Those strong analytical roots let AirMagnet provide more live detail on what was going on in our wireless space than its competitors. Once we drilled down to the sensor of interest, we could view the live RF surrounding that sensor, including what portion of the air is used up with 1-Mbps, 2-Mbps and 5.5-Mbps traffic. We also enjoyed specialized tools to assist in troubleshooting client-AP negotiations, packet capture and decoding, as well DHCP, ping and trace.

AirMagnet supports more than 130 security and policy violation alarms, and it had the best success identifying the more advanced attacks. On the other hand, we felt the system was a little trigger-happy: A client that was incorrectly configured to access a Cisco AP configured for WPA-LEAP was labeled as possibly running the *asleep* attack because of all the failed access attempts. And while we performing our wireless attacks, AirMagnet Enterprise complained that the attacker wasn't using TKIP or PEAP—who

cares! There are options to tune alarms for only certain SSIDs, but a more advanced system would filter out the noise and present the most relevant data to the wireless administrator, something that the setups from AirDefense and AirTight could do.

AirMagnet's pricing was reasonable. Organizations looking for a strong wireless IDS with some diagnostic capabilities will want to evaluate AirMagnet, and government facilities with higher security needs might rest easier knowing that AirMagnet is the only vendor in the beginning stages of FIPS 140-2 certification.

AirMagnet Enterprise 5.2. AirMagnet,
(877) MAGNET-5, (408) 400-0200.
www.airmagnet.com

