



February 2008

## GroupTest: Wireless security

Vendors are promoting wireless connectivity very heavily as a replacement – not an alternative – to wired networks, and this is driving growth in the market, says [Peter Stephenson](#).

### PICK OF THE LITTER

**AirDefense Enterprise** provides protection against wireless threats, policy compliance monitoring, robust performance monitoring and troubleshooting, and location tracking in an appliance that is scalable for most size organizations. For its excellent value, ease of use and performance we rate this our Best Buy.

**AirMagnet Enterprise** delivers active full-time protection against the entire spectrum of wireless threats. For its ease of use and good value, we rate this product Recommended.



Back in January of 2005, Dell'Oro Group predicted that the wireless LAN (WLAN) market would grow to \$4.3 billion by 2009. In early 2007, CRN reported that the market had surpassed \$3.6 billion in 2006. If all that is true, the 2009 numbers will be reached by the beginning of 2008 or a little after. The vendors are promoting wireless connectivity very heavily as a replacement – not an alternative – to wired networks. Cisco has made huge investments in development and acquisition as an example of this market growth.

The new 802.11n standard, though hotly debated, is likely to play a major part in driving the WLAN market as well. Virtually all of the products we tested support 802.11n one way or another.

The products we looked at are a somewhat reduced batch from those we reviewed last year. However, what is interesting about these is that three of the five products are new to our labs. The products all are part of larger integrated systems. In one case, endpoint security can be added. And, one product, especially, appears in different guises in both our Group Test reviews. This points to a convergence of functionality that includes both wired and wireless security.

*What 802.11n will mean* — The key advantage of 802.11n is speed. The top speed is 248Mbit/s, as opposed to 54Mbit/s for 802.11g. This gives an average expected throughput of 74Mbit/s, far faster than 802.11g's average 19Mbit/s. One way 802.11n achieves higher throughput is via the use of multiple input/multiple output (MIMO) technology. This requires multiple transmitter and receiver antennas. It also requires aggregation in the medium access controller in the physical layer. Range for 802.11n access points also improves to about double that of 802.11g. The standard is not without problems, however.

The problem with 802.11n has nothing to do with technology. Rather, it rests in a patent battle. The Commonwealth Scientific and Industrial Research Organization (CSIRO) holds the patent and has so far refused to provide the Institute of Electrical and Electronics Engineers (IEEE) with a letter of assurance that they won't sue over patent infringement. This has not stopped most vendors from betting on an eventual solution to the apparent impasse.

*How to buy wireless security products* — One major difference between last year's review and this year's is the improved forensics availability. Tracing wireless events with forensic certainty is beginning to reach maturity. Be sure that the product you are considering has solid tracing and reporting capability and supports emerging wireless security requirements.

Most of the products we looked at do most of the things you'll need. The devil is in the details.

*Testing a wireless security system* — Testing a wireless security system is not much different from testing any intrusion detection/prevention system (IDS/IPS). Use the usual vulnerability assessment and penetration tools and treat it exactly as you would a wired network. However, once those tests are complete, the next set of tests is unique to a wireless network. These include rogue access point detection, attempting to break encryption, and attempting to reconfigure access points. Rogue access point detection has two important facets. First, can the system detect the existence of a rogue access point (AP)? Second, can it detect the location of the AP?

Testing wireless security systems is critical and should be done regularly. A wireless security product that cannot detect a rogue access point, for example, is not particularly useful. However, just because the AP can be detected, you still don't know where it is. Thus, a good wireless security product should be able to tell if the AP is on your network and where it is.

*What we found in this batch of products* — Overall, this was a good bunch of wireless security tools. Generally, they all provided core functionality. However, not all have robust AP location capability, and some product's reporting is better than others. These products tend not to be expensive, so cost should not be a factor in deciding to implement wireless security. The differences between having exactly what you need and "making do," however, are not large enough to prevent you from buying exactly the product that will support your infrastructure.

Remember, as your enterprise approaches the 80 percent wireless predicted by some mavens, what you spend on protection is trivial compared to the potential risk of opening up your company network to enterprising attackers.

---

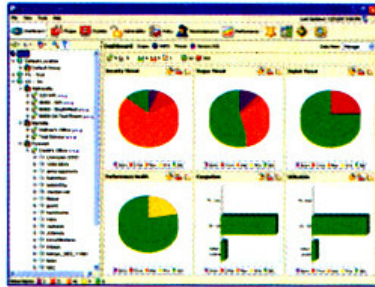
*Mike Stephenson and John Aitken contributed to these reviews.*

Specifications for wireless security tools

●=yes ○=no

Company	AdventNet	AirDefense	AirMagnet	AirTight Networks	ZENworks
<b>Product name/model</b>	WiFi Manager	Enterprise	Enterprise	SpectraGuard	Endpoint Security Mgmt.
<b>(A)ppliance or (S)oftware</b>	A&S	A	A or S	A	S
<b>Wireless access point configuration management (centralized)</b>	●	○	●	○	○
<b>Wireless access point configuration audit (centralized)</b>	●	●	●	●	●
<b>Wireless access point configuration reset (centralized)</b>	●	○	●	●	○
<b>Rogue wireless access point detection</b>	●	●	●	●	●
<b>Centralized logging capabilities</b>	●	●	●	●	●
<b>Ability to detect admin access to wireless access point</b>	●	●	●	○	○
<b>Rogue wireless client location detection</b>	●	●	●	●	●
<b>Rogue wireless client detection</b>	●	●	●	●	●
<b>System support of 802.11 (n)</b>	○	●	●	●	●

# Enterprise v7.3



**Vendor** AirDefense  
**Price** starts at \$7,995  
**Contact** [www.airdefense.net](http://www.airdefense.net)

**A**irDefense Enterprise provides protection against wireless threats, policy compliance monitoring, robust performance monitoring and troubleshooting, as well as location tracking in an appliance that is scalable for most size organizations. The AirDefense Enterprise offers comprehensive detection of wireless intrusion attempts by analyzing threats in real time against historical data. This allows accurate detection of various wireless attacks and anomalous behavior.

Automated protection works by stopping any attempted connection by a rogue device before access is gained to the network. This ensures that unauthorized users and rogue devices are disconnected. The system then generates and maintains a log of termination actions for audit records.

The product allows administrators to define, monitor and enforce policy in the areas of security, performance, usage and vendor types. AirDefense Enterprise includes a variety of regulatory compliance reports that administrators can generate. The AirDefense product

provides forensic data to retrace any device's activity down to the minute.

We found this product the easiest to set up of any product we tested. It is true plug-and-play. Within seconds of completing the installation, it discovered its sensor and immediately began to report rogue access points. The user interface is excellent and navigation is intuitive.

The documentation for this product is accurate and well-structured, providing the reader with the necessary information for deployment and administration.

AirDefense has two support options for the enterprise product: option one includes hardware support, all software upgrades and telephone support from 8 a.m. to 8 p.m. ET, Monday through Friday. Option two includes hardware support, all software upgrades and telephone support 24/7. The AirDefense website is also a valuable resource for support.

Pricing starts at \$7,995 for a starter kit with server, five sensors and licenses, which, given the rich feature set and ease of use, provides an excellent total cost of ownership value.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>Strengths</b>	Solid product with excellent ease of use and performance.
<b>Weakness</b>	None.
<b>Verdict</b>	For its excellent value, ease of use and performance, we rate this our Best Buy.