



September 2008

## AirDefense Enterprise 7.3

[http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14\\_gci1327763\\_idx1,00.html](http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1327763_idx1,00.html)

By Sandra Kay Miller

### WIRELESS NETWORK SECURITY

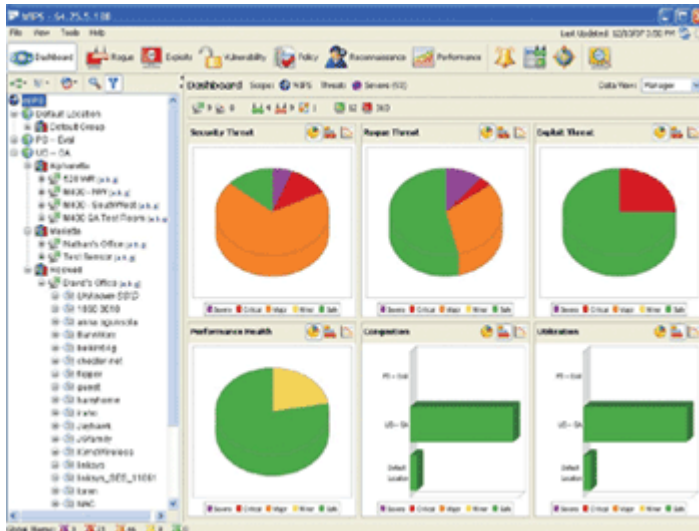


AirDefense Enterprise 7.3

REVIEWED BY SANDRA KAY MILLER

AirDefense

Price: Starts at \$7,995



There have been numerous updates since we last examined AirDefense Enterprise in March 2006 (Motorola recently announced it will acquire AirDefense). Notable improvements for this wireless intrusion detection/ prevention tool include support for

Power over Ethernet (PoE) for its sensors, an improved user interface, overhauled reporting and new features such as WEP cloaking, advanced forensics, spectrum analysis and a centralized console to manage appliances.

## Installation/Configuration

A-

The startup wizard led us through system settings, network structure, user account creation, policy definition, configuring alarms, automated event classification, notification and identifying access points. This was the easiest deployment method, as the documentation for the server and administrator is weak.

You can also restore a saved configuration or perform manual configuration.

Administration is much improved, thanks to distinct management roles. We created administrators, who handle configuration/management; managers, who have administrator rights except for editing logs and adding users; network operators, who deal specifically with network operations, including alerts and alarms; and guests, with limited manager/network operator functions.

Administration roles can be limited through domain-based partitioning, which restricts access to different networks, groups and devices. Users can be authenticated locally through the AirDefense server or through remote RADIUS or LDAP servers.

## Policy

A

AirDefense Enterprise includes a comprehensive set of default policies. Custom policies are easily configured through the Policy Manager, from which we could quickly view the associations, behaviors and protocols (a, b, g) of all locations, groups and devices.

There are four basic policy types: configuration, performance, vendor and channel. The first three apply to access points and the fourth to the sensors. The channel policies are the most powerful, offering granular control over when specific channels are allowed on the network.

## Logging and Reporting

A

Extensive logging and reporting provides access to real-time information and historical data in syslog format.

Web Reporting is suitable for the manager role, with access to standard report templates, previously published reports and frequently run reports.

Administrator and network operator roles have much greater control over content with the Report Builder, which can be used to create reports from scratch or templates.

## Effectiveness

A

Three new features (optional modules) stand out.

Advanced Forensics covers troubleshooting network anomalies and digs deeper into security-related events.

The Spectrum Analysis tool provides background and dedicated spectrum scanning through the sensors. We were able to locate and identify sources of interference from other wireless networks, as well as non-network devices such as microwave ovens.

Live View offers a real-time observation of sensors, APs and users--data, connections, devices and frames--as well as graphical charts for at-a-glance analysis.

WEP cloaking protects organizations that still use that vulnerable encryption protocol. WEP cloaking generates "chaff" frames to confuse common sniffing and WEP-cracking applications.

The wireless traffic detection sensors are a huge improvement, as the model we tested solely utilizes PoE.

## Verdict

AirDefense is a comprehensive, cost-effective solution for protecting and troubleshooting WLANs.

---

**Testing methodology:** We tested the product by deploying the appliance and wireless sensor on an 802.11 network utilizing 802.11a, b and g devices.