



Network Computing

For IT By IT

March 2, 2006

Sneak PREVIEWS

20 RARITAN COMPUTER COMMANDCENTER NOC
22 AVIDIAN TECHNOLOGIES PROPHET 24 QUICK TAKES

Rogue Hunters

Distributed wireless security monitors help categorize and prioritize threats **BY FRANK BULK**

good

- Well-categorized wizards
- Strong forensic analysis with detailed reporting

bad

- Flawed behavioral trending
- Data consistency issues

Vendors are racing to keep up with escalating security concerns. In recent weeks, two of the vendors represented in our last comparative review of wireless IDS products (see "Time To Tighten the Wireless Net," ID# 1612/2) have introduced significant security upgrades to their products. AirDefense, an established player in the market, has pushed forward with its forensic analysis, which adds insight into the history of your wireless space. AirTight has filled out its feature set and enhanced the auto-classification capability of its relatively young product, SpectraGuard.

AirDefense Enterprise 7.0

The AirDefense Enterprise wireless IDS system provides overlay security for existing Wi-Fi networks and enforces "no-Wi-Fi-allowed" policies in those organizations that have them. Version 7.0 introduces new features such as built-in location tracking, while enhancing existing capabilities like forensic analysis.

The AirDefense Enterprise sys-

tem arrived as a rackmountable server with several sensors, which are powerful APs (access points) coupled with custom software that connect to the server through a serial cable. Initial server configuration is done through a menu-driven text interface, but ongoing management is via a Java-based interface that runs within a Web browser or as a standalone application.

AirDefense has redesigned its dashboard by grouping its core functionality into five analysis wizards. The rogue analysis wizard does a good job prioritizing rogue clients and APs. APs found on the wired network are clearly tagged with a higher threat level than standalone APs. On

the wired side, a switch port lookup finds rogue APs, but you must enter all your switches' IPs and SNMP community strings. When I used a Cisco AP and a wireless router as test rogues, however, the system had limited success, because the wired MAC address is significantly different than the rogue BSSIDs (Basic Service Set Identifiers). Even associating a client to the rogue AP and sending some traffic through didn't help.

On the plus side, it's easy to select and right-click a rogue to contain it, terminate it or find out more information. Termination can be performed wirelessly or by disabling the port. The system also can integrate with Cisco's WLSE (Wireless LAN Solution Engine) to assist with wireless tracing and disabling.

The performance analysis wizard lists problems such as excessive roaming or traffic that crosses defined thresholds, and assigns them threat levels. The compliance



AirDefense Enterprise has redesigned its dashboard by grouping its core functionality into five analysis wizards—rogue, performance, compliance, forensic and intrusion.

analysis wizard lists APs that are out of compliance with predefined or configured policies. The intrusion analysis wizard lists events that warrant further investigation.

The forensic analysis wizard supplies a wealth of detail. AirDefense says it tracks up to 300,000 devices, each with 249 data points using a new database that dramatically increases data-retrieval speeds. This wizard also offers location tracking and threat mitigation. However, the wizard listed both my test clients' WEP (Wired Equivalent Privacy) status as "unknown." But running a report against the same two devices showed WEP as "on," as did a report against the AP. AirDefense says this was a bug. The wizard and reports also listed my laptop's DNS name as "Laptop," using the alias I had assigned to the device rather than performing a reverse lookup of the IP address or leaving it blank.

Another significant feature in this release is statistical base-lining: If an AP or client acts out of character, the system will flag a behavioral alarm. My test system stumbled here, failing to learn the behavior of production traffic and sending me false behavioral alarms. AirDefense was not able to identify why this occurred.

Despite quirks, AirDefense Enterprise easily identified and contained the devices I threw at it. And the forensic analysis added details about

my wireless network and devices that no other product provides.

■ **AIRDEFENSE ENTERPRISE 7.0**, \$8,975, server, four sensors, 25 connection licenses, AirDefense, (770) 663-8115. www.airdefense.net