

Wireless security

AirDefense Enterprise

Version	4.0
Supplier	AirDefense Inc.
Price	Starter kit begins at \$10,000, inclusive of five sensors and a server with database. Further sensors are priced at \$495
Contact	www.airdefense.net



As wireless networks grow in popularity, many security professionals are justly worried about the ease in which non-technical users can set up and operate wireless networks. Also securing wireless infrastructures can be tricky, because the set up of wireless networks can be problematical and not as secure as one might think.

This appliance offers a complete monitoring solution for wireless LANs which allows administrators to secure and monitor the health of their wireless networks.

The package consists of a central AirDefense server housed in a large 1U rack mountable unit, and two or more AirDefense sensors, which should be located on the network close to wireless access points (APs). The sensors can be set to passively monitor all wireless traffic across 802.11a, 802.11b and 802.11g networks, and report back to the central server. Traffic between sensors and the server can be encrypted by SSL, if required.

Initial configuration of the server is quick and straightforward. A keyboard and monitor are attached to the server, and after logging in to the command line interface (CLI) the administrative interface is launched. Initial setup was restricted to setting the IP address of the server, its hostname and other details of the network to which it was attached. On exiting from the CLI, the unit rebooted and came up on the network.

It is possible to run the CLI over SSH and to restrict the management stations that can connect by SSH to the server. After the initial setup, though, most administration and all of the operational tasks are done through the web-based GUI.

Once the server was up and running, we configured the sensors. Initial con-

figuration was done by attaching the sensor and our laptop to a hub, resetting the IP address of the laptop and connecting to the GUI of the sensor. (This is the recommended method – there have apparently been some difficulties in using a cross-over cable). The GUI has a quick setup page where the sensor name, IP address and network details can be entered, as well as the address of the AirDefense server. After saving this configuration, the sensor was plugged in to the network.

Once again, after initial configuration, further management can be done from within the AirDefense GUI using the Sensor Manager.

The main GUI is a Java application, so it requires installation of the JRE plug-in from Sun. Connecting to the AirDefense server on the specified port (which is user configurable) brings up a login screen – on logging in, the GUI loads, showing the main Dashboard. The Dashboard gives information about all aspects of the wireless network, with sections for system activity, alarms, discovered APs, policy violations and suspicious devices. Graphs also show sensor-collected information such as signal strength and traffic levels.

The system worked straight away. As the sensors discovered APs, they appeared in the main Dashboard. The devices from our test network were all found and correctly identified. A number of other APs were found, presumably from nearby offices. As each sensor has a range of 40,000 to 60,000 square feet, this is hardly surprising. We were able to select the APs on our network and focus on them.

It is a simple matter to define policies that are to be applied to the monitoring of the wireless network. They fall under four headings – configuration,

performance, vendor and channel. All the policy thresholds are configurable, and policies can be set per AP if you need to.

And because the AirDefense system has behavioral profiles from all the major wireless product vendors, you can quickly identify equipment that does not conform to network policy. If you run an all-Cisco shop, for example, the system will immediately flag up someone connecting with a card from a different manufacturer. We defined a policy restricting certain stations to a particular AP. Connecting to that AP with a new laptop immediately triggered an alert.

The sensors report on the traffic flow from each wireless station and on the direction of flow. You can enable packet capturing if required, in order to sniff traffic passing to a particular station, although this required enabling capturing on the server for the particular sensor, disabling it, and then retrieving the file from the server for analysis.

The combination of attack signatures and policy compliance monitoring meant that the system worked well as an intrusion detection system. Because the server collates information from different sensors, it will easily detect suspicious traffic like a laptop connecting to a large number of APs.

We fired up NetStumbler on a laptop to scan for APs, and were immediately detected. Attacks with FakeAP and some AirJack tools were also detected and reported on the Dashboard. AirDefense can interact with Cisco APs to disconnect intruders – unfortunately, we were not able to test this facility.

As a management tool, the system provides network administrators with all the data they need to plan, manage



and revise their wireless infrastructure to optimal effect. As the system continuously monitors the network, it would be easy to see on a long-term basis which APs were being over-used and which were carrying little traffic.

Reporting facilities are excellent. Information can be exported in a variety of formats, and alerts can be propagated via SNMP, syslog or email.

Finally, there is extensive online help and detailed PDF documentation covering all aspects of setup and operation.

Jon Stearn

SC MAGAZINE RATING

Features	★★★★☆
Ease of use	★★★★★
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★☆☆
OVERALL RATING	★★★★★

FOR Very easy to get up and running with an excellent and management tool.
AGAINST Interaction currently limited to Cisco APs.
VERDICT Worthy of consideration to monitor proliferating wireless access points.

Contact details: