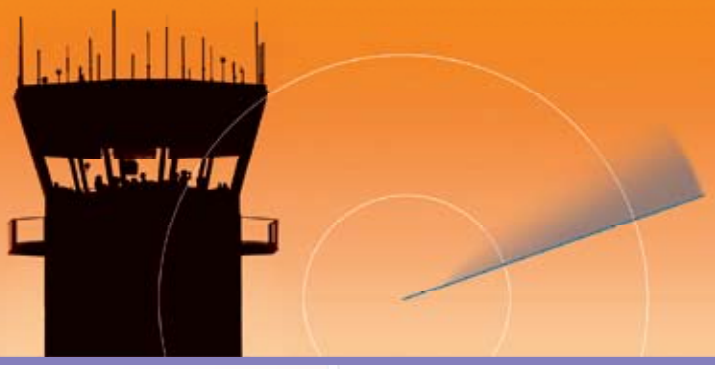
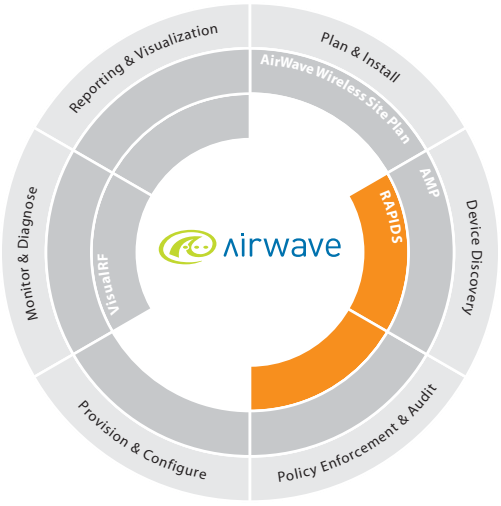


airwave®

FOR WIRELESS **THAT WORKS**

RAPIDS™ ROGUE AP DETECTION MODULE



Unauthorized 'rogue' access points are a critical threat that can expose sensitive data to intruders and may undercut your organization's entire regulatory compliance program (Sarbanes-Oxley, HIPAA, PCI, etc.) Unfortunately, the most likely place for a rogue to be connected to your network is where it is hardest to detect: in remote offices without authorized Wi-Fi networks, hundreds of miles from your headquarters. AirWave's RAPIDS rogue access point detection module lets you sleep easily at night, knowing that there are no unauthorized APs connected anywhere on your network.

Security is Strengthened

AirWave's RAPIDS software solution uses a unique combination of wireless and wired network discovery techniques to detect and locate all rogue APs on your networks, wherever they may be. RAPIDS uses your wireless access points to discover and pinpoint any unknown radios within RF range. It also scans your wired network to locate any other rogues that are not within radio range of your access points. RAPIDS correlates results of the wireless and wired scans, and delivers you a high-priority alert containing all the information you need to locate and remove any rogue devices it has found.

Management is Easy

With RAPIDS' simple web-based user interface, you can launch a global wired and wireless network rogue AP scan from a single console, plus set a schedule for regular, automatic scans.

Visibility – See Where They Are

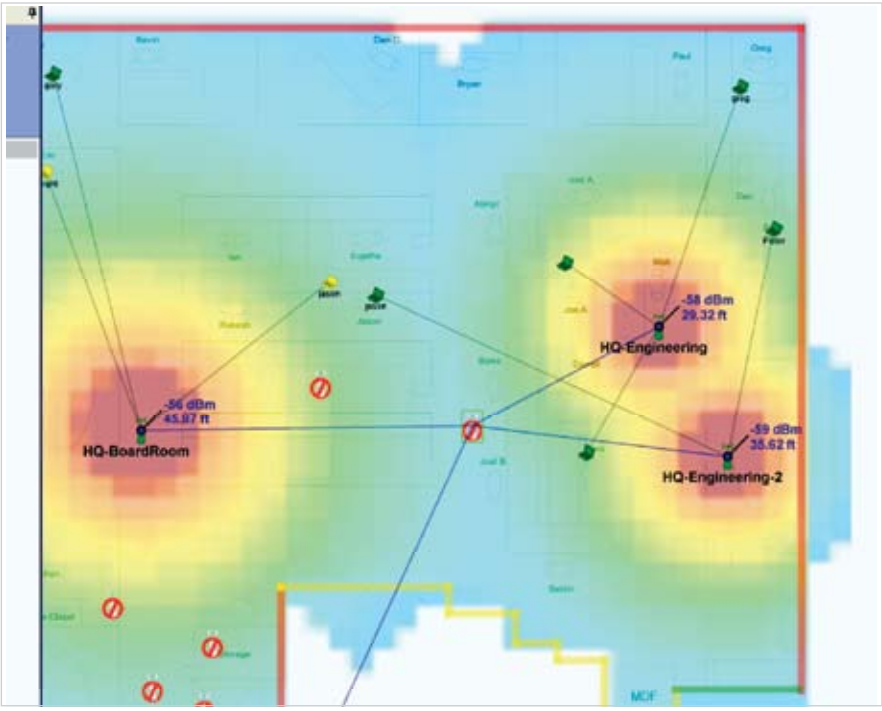
RAPIDS integrates with AirWave's VisualRF module to calculate and display on-screen the physical location of any rogue access points.

FEATURES + FUNCTIONALITY

- Wired network discovery to locate wireless access points anywhere on the network
- Wireless detection of rogues within range of authorized, managed access points
- AirWave Management Client provides supplemental RF scanning data from Windows devices on which it is installed
- Correlated alerts containing all data from both wired and wireless scans
- Locates rogues by triangulaton of radio data and displays on-screen by integration with the VisualRF module
- High accuracy and low false positive rate through rogue scoring and OS interrogation
- No proprietary sensors or hardware required for accurate rogue detection

Wi-Fi ROI is Enhanced

RAPIDS uses your existing wired and wireless network infrastructure. It does not require proprietary sensors. It fully automates rogue AP detection efforts, eliminating the cost of manual scans.



"We calculated that it would take us two years to install wireless sensors in 3,000+ retail stores. Two years without a true security solution in place is far too long."

IT Security Manager,
Fortune 500 Retailer

Wired Network Scans and AP Identification

- Uses SNMP, HTTP, CDP, and other discovery protocols to identify all devices on your wired network
- Interrogates devices with manufacturer default and configurable passwords to 'fingerprint' a wireless AP
- Examines the MAC address of each device on the network and compares it to RAPIDS' database of 9,000+ known MAC address ranges to identify devices with MAC addresses commonly used by wireless hardware manufacturers
- Uses RAPIDS' database of 1,700+ OS types to identify the device operating system to help you eliminate 'false positive' results (i.e., a device with an embedded OS is far more likely to be a rogue access point than a device with a Windows OS)

Wireless Network Scans

- Instructs authorized access points to scan the airwaves for other wireless APs
- Uses Windows devices loaded with the AirWave Management Client application to provide supplemental RF data. (AMC is an AirWave-developed client application available to all RAPIDS users)
- Compares results of RF scans to the list of known access points to create a rogue list
- Allows you to distinguish between 'true rogues' & 'neighboring APs' that are in RF range but not connected to your network

Rogue Scoring & Elimination of False Positives

- Correlates rogue detection data from both wireless and wired network scans
- Assigns each device on the network a score reflecting the likelihood that the device is a rogue access point
- Provides filters so you can see lists of the highest priority devices that are most likely to be rogues

Alerts & Reports

- Assigns varying alert priority to each discovered AP (Critical vs. Major vs. Warning) depending on its rogue score
- Generates automated email alerts containing all known information about rogue devices, including:
  - Radio MAC address
  - LAN MAC address
  - Discovery method
  - SSID
  - Channel
  - Security settings
  - Switch port
  - IP address
- Rogue summary screens display real-time, up-to-date information on all suspected rogues

Visualization

- Integrates with AirWave's VisualRF module to display the likely location of each rogue device on an office map
- Triangulates location using signal level data collection from APs and the AirWave Management Client
- Location accuracy increases when the rogue device is discovered by more RF scanning agents

Product Information

- Linux-based server platform
- Web-based user interface
- Does not require proprietary sensors or other hardware
- Includes a license to multiple copies of the AirWave Management Client
- May be licensed independently of other AirWave software applications

AirWave Wireless
1700 South El Camino Real
Suite 500
San Mateo, CA 94402

Phone: (650) 286-6100
Fax: (650) 286-6101

www.airwave.com
General information: info@airwave.com
Sales: sales@airwave.com
Technical support: support@airwave.com

RAPIDS-53 03/08

airwave®

for wireless that works