



FOR WIRELESS THAT WORKS

RAPIDS™ ROGUE AP DETECTION MODULE

Unauthorized 'rogue' access points are a critical threat that can expose sensitive corporate data to intruders, and may undercut an organization's entire regulatory compliance program (Sarbanes-Oxley, HIPAA, Visa's CISP, etc.). Unfortunately, the most likely location 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 will help you sleep at night, knowing that no unauthorized APs have been connected anywhere without your knowledge.

Security

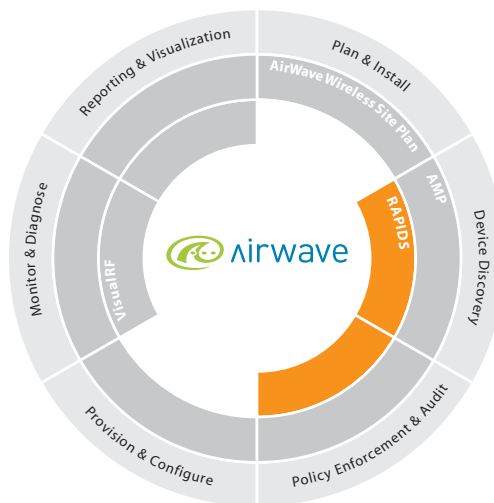
The RAPIDS software solution uses a unique combination of wireless and wired network discovery techniques to detect and locate all rogue APs, wherever they may be. RAPIDS uses your existing, authorized wireless access points to locate any unknown radios within RF range. RAPIDS then scans your wired network to locate any other rogues that may not be within 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 the rogue device.

Management

Using RAPIDS simple web-based user interface, you can initiate a global wired and wireless network rogue AP scan from a single console, as well as schedule ongoing automatic scans.

Visibility

RAPIDS integrates with AirWave's VisualRF module to calculate and display the physical location of any rogue access points, using RF data from your existing APs and the AirWave Management Client.



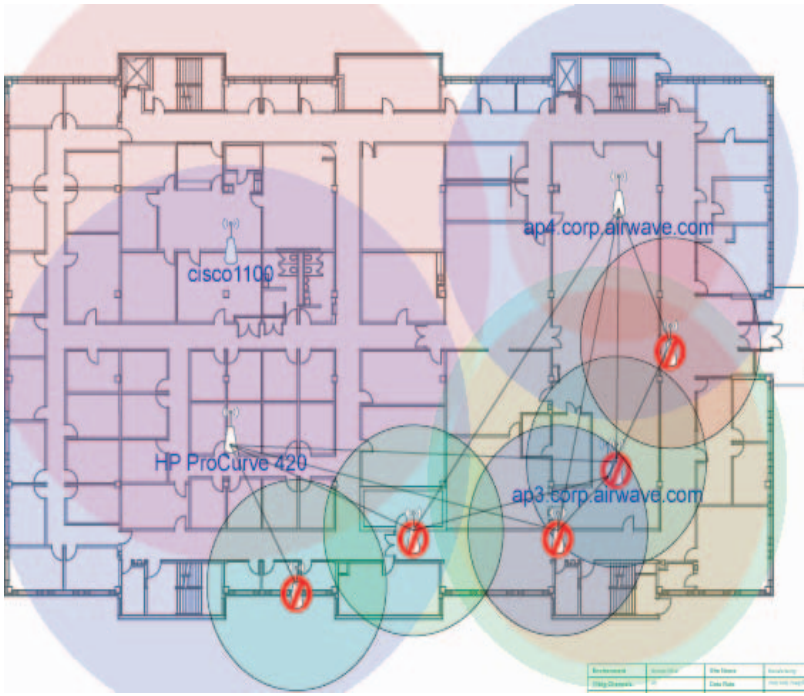
FEATURES + FUNCTIONALITY

- Wired network discovery to locate wireless access points anywhere on the network
- Wireless detection of rogues within range of authorized, managed access points
- Integrated AirWave Management Client for supplemental RF scanning data from Windows devices
- Correlated alerts containing all data from both wired and wireless scans
- Triangulation of rogue location through 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

WiFi ROI

RAPIDS leverages your existing wired and wireless network infrastructure and requires no proprietary sensors. It fully automates rogue AP detection, eliminating the cost of manual scans.





Wired Network Scans

- 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 attempt to definitively “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 devices with a Windows OS.)

Wireless Network Scans

- Instructs authorized access points to scan the airwaves for other wireless APs (NOTE: Most enterprise-grade access

points now provide this functionality, but some older models and SOHO access points do not)

- Uses Windows devices with the AirWave Management Client application to supplement RF data from existing APs. (NOTE: 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 Positive Results

- Correlates rogue detection data from both wireless and wired network scans
- Assigns each device on the network a score (from 1-5) 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 (scores of 5 or 4)

“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

Alerts & Reports

- Assigns alert priority (Critical vs. Major vs. Warning) depending on the rogue score
- Generates automated email alerts containing all known information about the rogue device, 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 physical location of the rogue device
- Triangulates location based on signal level data 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 Inc.
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-001



for wireless that works