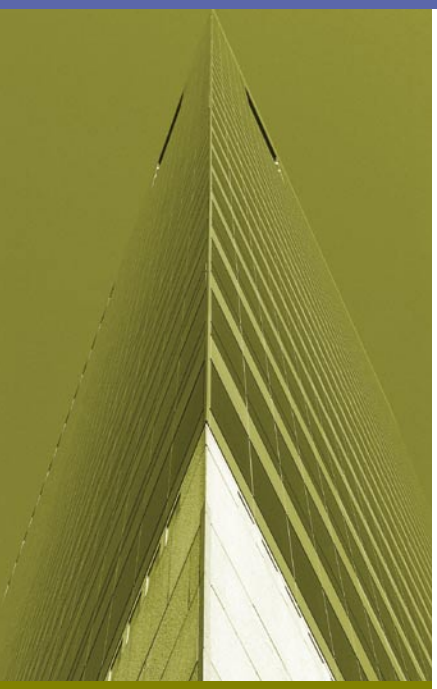
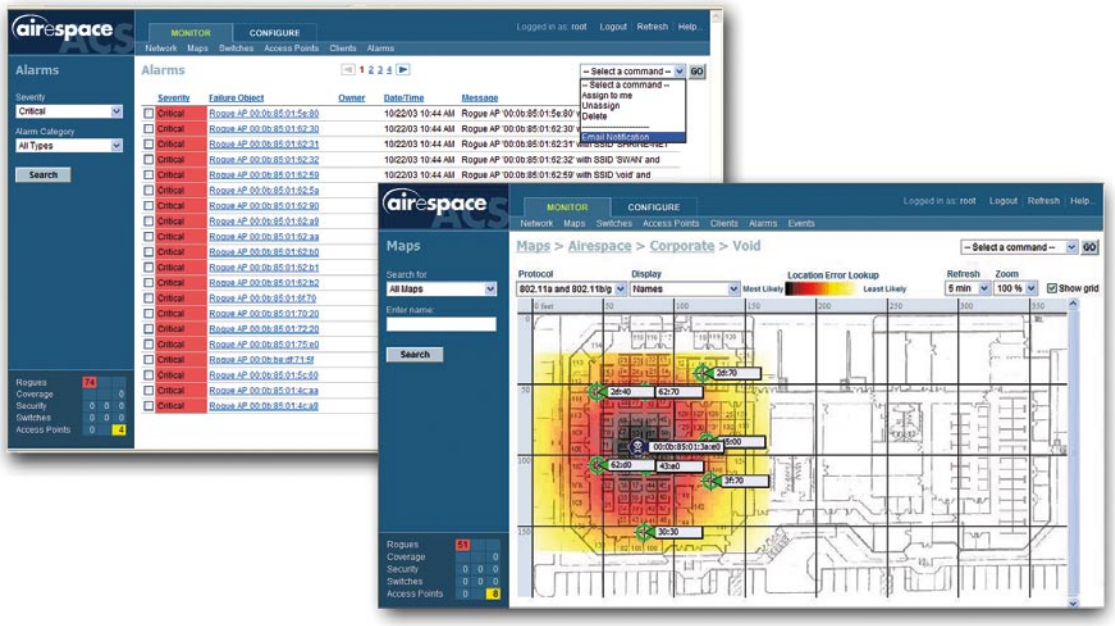
Airespace Wireless Protection System





Features and Benefits

Wireless prevention
Locking down the air space lets IT staff control the deployment of WLAN services

Rogue detection, containment, and location
Enables IT managers to control wireless within their networks. Ensures there are no unknown security risks

WLAN attack signatures
Detect and address malicious attacks in real-time with no system reboot

Client-level visibility
Allows IT managers to see what individual users are doing and control how the WLAN is being used

Integrated wireless protection and data services
Reduced capital expenditures; excellent investment protection

Intuitive centralized management
Reduces the time and training associated with deploying a Wireless Protection System

Multi-layer protection from attacks
Ensures the wireless network provides reliable and secure performance

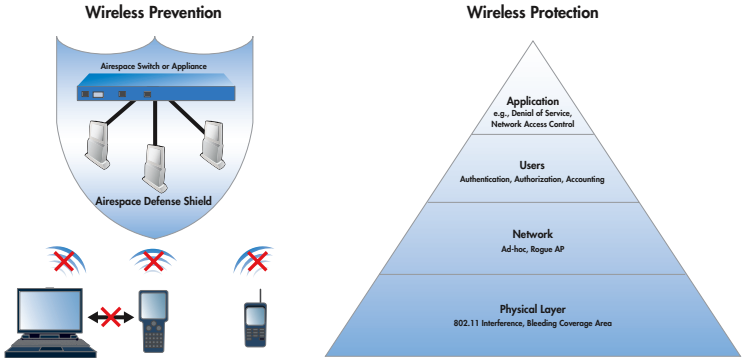
Integrated location
Allows managers to quickly locate devices and malicious activity

Airespace Wireless Protection System

Airespace combines real-time monitoring functionality with advanced analysis capabilities to provide the industry's most advanced and effective Wireless Protection System (WPS). Whether protecting an existing wireless network from unauthorized activity, or preventing the deployment of wireless networks altogether, Airespace's Wireless Protection System is a vital component in protecting business critical networks.

Airespace's WPS is an integral component of the Airespace Wireless Enterprise Platform, which consists of Airespace Access Points (APs), WLAN Switches/Appliances, and Airespace Control System (ACS) Software. Airespace access points act as air monitors, communicating real-time information about the wireless domain to Airespace WLAN Switches and Appliances via the Lightweight Access Point Protocol (LWAPP). All security threats are rapidly identified and presented to network administrators via ACS, where accurate analysis can take place and corrective action taken.

Airespace offers the only WLAN system that offers simultaneous wireless protection and WLAN service delivery. This ensures complete WLAN protection with no unnecessary overlay equipment costs or extra monitoring devices. Or, the Airespace system can be deployed as a standalone Wireless Protection System and upgraded to offer data service in the future. This allows network managers to create a "defense shield" around their RF domain, containing unauthorized wireless activity until they are ready to turn-up WLAN services. Regardless of the deployment method chosen, Airespace provides the highest level of wireless protection functionality for completely secure Wireless LAN operations.

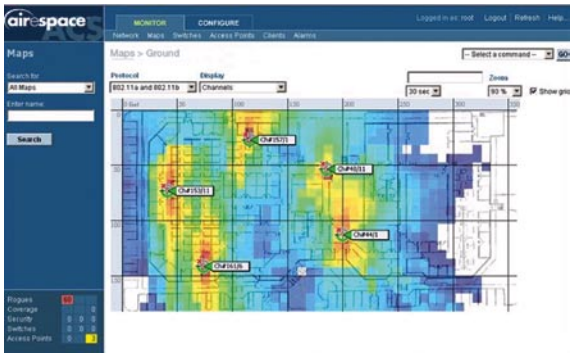


Control Your Air Space

Airespace's Wireless Protection System enables network managers to control how the air space is used – or if it can be used at all. When deployed as a standalone system, WPS prevents all unauthorized 802.11 activity (client and AP), enabling IT staff to deploy WLAN services at their own discretion. This takes wireless service delivery out of the hands of the employee and places it into the hands of the network manager.

When deployed in conjunction with WLAN data services, WPS ensures all corporate resources remain safe from unwanted intrusion and malicious activity. Enterprise-wide policies can be centrally configured and managed to govern how employees and visitors use the RF domain. The Airespace Wireless Protection System also monitors existing access points to make sure they fit pre-defined security policies.

Unsurpassed WLAN Security Features



The Airespace Wireless Protection System is a complete solution designed to address the unique security requirements of RF environments. WPS complements existing LAN security platforms by providing multiple layers of WLAN protection, including:

- **RF:** detect and avoid 802.11 interference; minimize RF bleed
- **Network:** rogue detection, location, containment; ad-hoc prevention; WLAN device certification and protection from address spoofing (e.g., man in the middle attacks)
- **User:** user authentication, authorization, and access control; protection from dictionary and other password attacks; IDS signature detection
- **Application:** data encryption; packet inspection; application protection from Denial of Service (DoS) and other attacks that can debilitate performance; client software integrity checking (i.e. Network Access Control)

Airespace's WPS supports a wide breath of standard security protocols, including:

- X.509 certificates
- Web authentication
- 802.1X (PEAP, TLS, TTLS), WEP, WPA, and 802.11i (WPA2)
- L2TP and IPsec VPNs that roam with wireless clients
- Integration with common backend servers for RADIUS, token authentication, and directory services

Airespace has consistently demonstrated an adherence to the highest levels of security, including HIPAA compliance and FIPS 140-2 level 2 certification. This has enabled the Airespace WLAN System to be deployed in mission critical environments, such as emergency rooms, trading floors, and military sites.

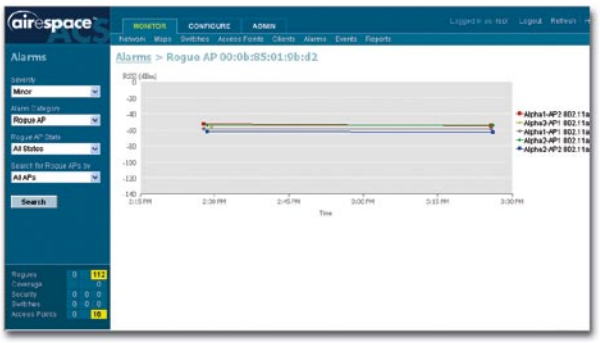
Airespace Wireless Protection System

A Complete Solution for Handling Rogues

Whether deployed maliciously or inadvertently by employees looking to improve mobility and productivity in everyday job functions, rogue access points are an enormous security risk for any enterprise.

Airespace's Wireless Protection System stops rogue devices dead in their tracks. Through real-time monitoring, the Airespace system automatically detects an unauthorized device as soon as it enters a wireless network. Alarms are generated via ACS, allowing IT staff to assess the threat. For example, they can see which clients are attached to the rogue, whether it is physically inside the building, or if it is a known device such as an AP in a neighboring coffee house or business.

Based upon the above analysis, the Airespace Wireless Protection System can be used to contain the rogue device, preventing it from participating in the wireless network. Furthermore, Airespace's integrated location tracking capabilities can be used to pinpoint the precise location of the unauthorized AP, enabling IT staff to take rapid corrective action.



Detailed rogue trending reports can be provided by ACS for historical analysis. This helps enterprises to identify recurring security problems.

Protection from Attacks

The RF is an open medium, making WLANs susceptible to a variety of attacks. The Airespace Wireless Protection System provides multiple levels of security to protect sensitive corporate resources from this type of malicious activity.

The Airespace Wireless Protection System detects excessive interference and unusual user activity and adjusts channel assignments and access control accordingly, protecting legitimate wireless users from DoS, void11, and other attacks. In addition, it prevents address spoofing of wireless devices to avoid FakeAP and similar attacks. The Airespace WLAN system also excludes users who make repeated unsuccessful login attempts, preventing dictionary attacks, and it leverages attack signatures to detect and prevent other common WLAN exploits. Finally, WPS detects and adjusts RF coverage areas to limit the effectiveness of NetStumbler and similar tools. The result is an iron clad RF domain that protects both wireless and wire-line resources from unscrupulous activity.

Investment Protection

Airespace access points provide real-time air monitoring in addition to WLAN service delivery. As a result, the Airespace system appeals to Chief Financial Officers in addition to Chief Security Officers. By eliminating the need for a separate overlay wireless protection system (with specialized appliances and monitoring nodes), the Airespace system dramatically reduces capital equipment costs when deployed as a WLAN infrastructure. When deployed as a standalone Wireless Protection System, the Airespace platform provides a cost-effective solution for containing wireless activity today, and a seamless migration path for the delivery of WLAN services tomorrow. As no new equipment or software is required when wireless services are ready to be delivered, Airespace provides an economical long term strategy for those enterprises not yet ready to deploy business-critical WLAN services.

Airespace Wireless Protection System

Intuitive Management

Airespace Control System Software provides an easy to use interface into the Airespace Wireless Protection System. This enables fast and accurate configuration of security policies and simplified day-to-day management. When coupled with the advanced WLAN capabilities that are inherent only to the Airespace Wireless Enterprise Platform, such as location tracking, enterprises have all the tools necessary for robust WLAN operations that are easy to manage and cost effective to deploy.

Airespace's Wireless Protection System is centrally managed for complete control of an entire enterprise. ACS Software is used to gather information from all of the Airespace access points, switches and appliances that are deployed in the network. It is also used to push out updated attack signatures for maximum WLAN protection with zero network downtime. As APs can be located across a campus, or across a Wide Area Network (WAN), Airespace provides an easy way to centrally administer enterprise-wide wireless protection policies. This improves overall security, and reduces the cost of managing a wireless network.

Integrated Location Tracking

The Airespace Wireless Protection System goes well beyond problem detection by delivering invaluable tools for problem resolution, such as granular location tracking. With this capability, which is unique to the Airespace Wireless Enterprise Platform, IT managers can establish geography-based access control policies that prevent intruders from accessing their wireless network from unauthorized locations. Or, Airespace's location tracking software can be used to pinpoint the exact location of a rogue device or the source of a network attack to expedite problem resolution.

Airespace's location tracking capabilities eliminate one of the hardest problems in securing a wireless network, which is determining the actual location of a security risk. Once the IT staff identifies where a security threat exists, they can easily, and expeditiously, take care of the problem.

airespace®

Worldwide Headquarters
110 Nortech Parkway
San Jose, CA 95134
Tel: 408.635.2000
Fax: 408.635.2020

EMEA Headquarters
3000 Cathedral Hill
Guildford, Surrey GU2 7YB
United Kingdom
Tel: +44 (0) 01483 243632
Fax: +44 (0) 01483 243501

Airespace K.K.
Yurakucho Denki Building
South Tower 10F
1-7-1, Yuraku-cho, Chiyoda-ku,
Tokyo Japan 100-0006
Tel: +81-3-5288-8511
Fax: +81-3-5288-8525

Airespace Wireless Networks Pvt. Ltd.
D08, 8th Floor, Tower D
Diamond District
#150, Airport Road
Bangalore 560 008, India
Tel: +91-80-5694-6777
Fax: +91-80-5125-9741

www.airespace.com

LIT 09-04-04-10-WPS