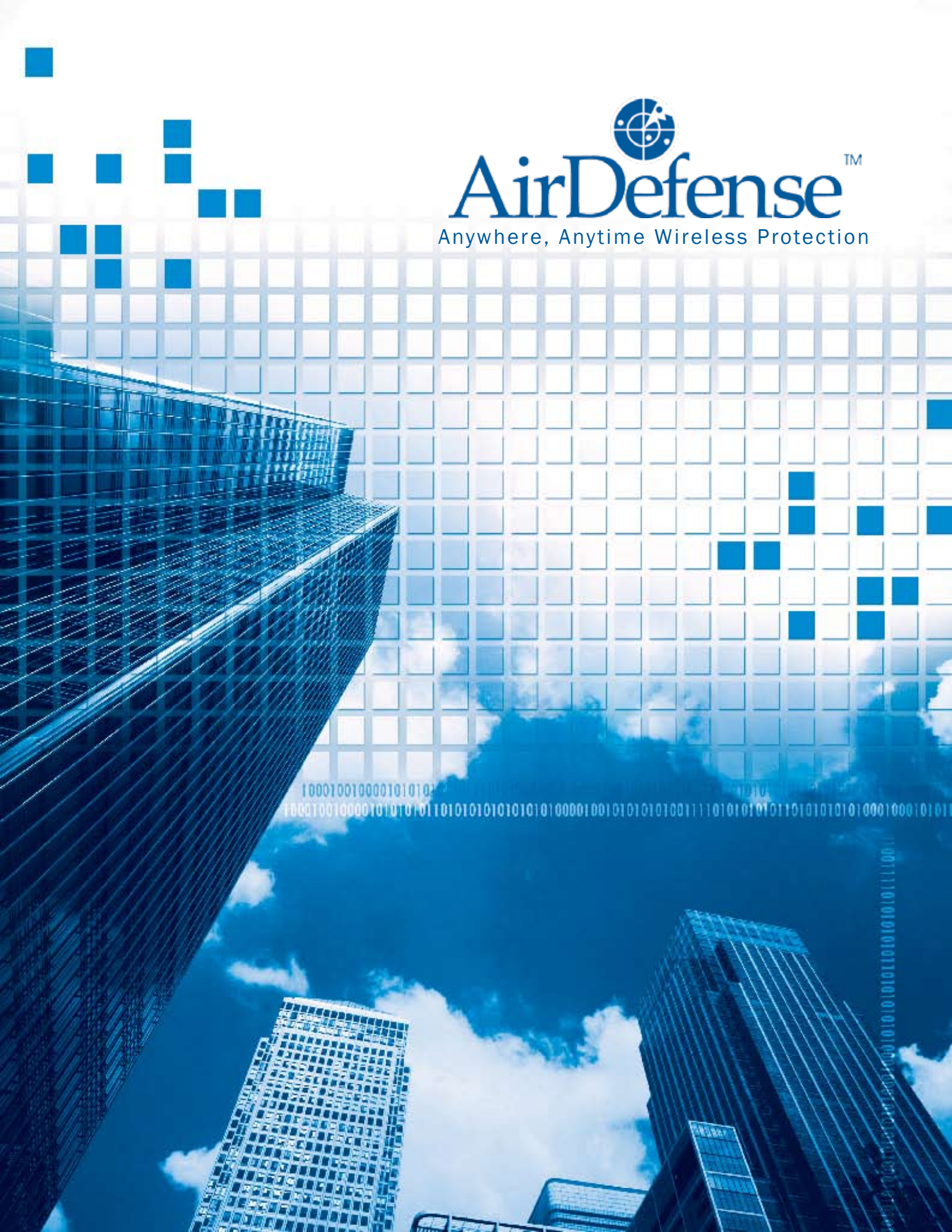




AirDefense™

Anywhere, Anytime Wireless Protection



EXECUTIVE SUMMARY

AirDefense Enterprise™ is the most powerful Wireless Intrusion Prevention System (IPS) available. Having pioneered the field of wireless IPS, AirDefense continues to lead in innovation with 27 patents pending or granted. The AirDefense Enterprise solution provides complete protection against wireless threats, policy compliance monitoring, robust performance monitoring and troubleshooting, and location tracking in an appliance that can scale to meet the largest global organizations' needs. AirDefense uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g) wireless traffic in real time for the highest level of security, rogue mitigation and policy enforcement.

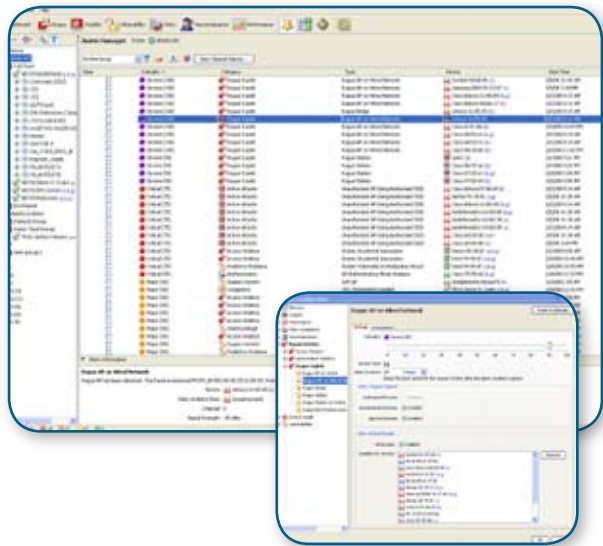
COMPREHENSIVE INTRUSION DETECTION

AirDefense Enterprise provides the most comprehensive detection of wireless intrusion attempts. By analyzing existing and day-zero threats in real-time against historical data, AirDefense Enterprise is able to accurately detect all wireless attacks and anomalous behavior. With context-aware detection, correlation and multi-dimensional detection engines, AirDefense detects only meaningful security events and maintains the lowest rate of false positive alarms. This next-generation wireless protection platform offers the industry's most extensive event library, with more than 200 security and performance events.

Wireless vulnerabilities detected include reconnaissance (ad hoc stations, rogue APs, open/misconfigured APs), sniffing (dictionary attacks, leaky APs, WEP/WPA/LEAP cracking), masquerade (MAC spoofing, evil twin attacks/Wi-Phishing attacks), insertion (man-in-the-middle attack, multicast/broadcast injection) and denial-of-service attacks (disassociation, duration field spoofing, RF jamming).

AirDefense allows administrators to easily distribute and process alarms in enterprise deployments:

- Customized alarm views, notifications and priorities
- Flexible querying and filtering
- Third-party integration



AUTOMATED PROTECTION

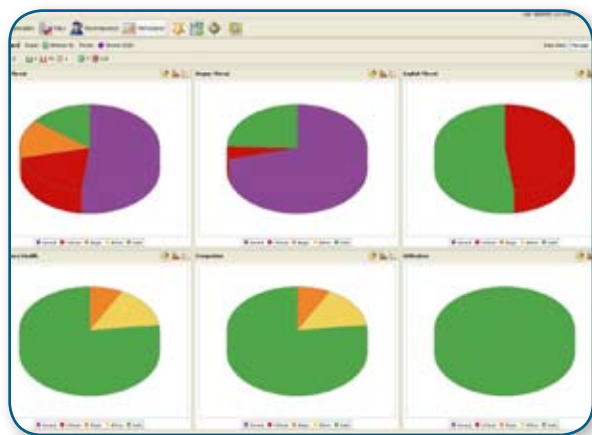
AirDefense responds automatically to wireless threats by stopping the device involved before it is able to cause damage to the network. By responding on both the wireless and wired networks, AirDefense is the industry's most secure wireless intrusion prevention solution. AirDefense performs targeted terminations ensuring that only the correct intruders and rogue devices are disconnected. The system maintains a record of termination actions to allow for a reliable audit trail. AirDefense also complies with FCC regulations and eliminates the liability that could be associated with stopping a device wirelessly.

AirTermination™

AirDefense can mitigate wireless threats via the air by disabling wireless connections between intruders and authorized devices. AirTermination is extremely precise ensuring that only the offending device is prohibited from operating.

Wired-side Termination

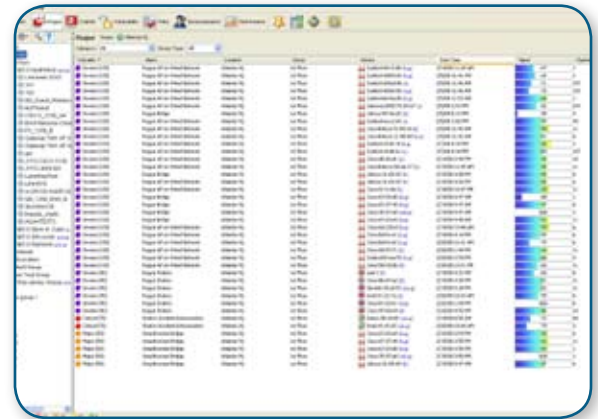
AirDefense identifies the switch port to which offending devices are connected and turns it off thus preventing the rogue device from accessing the network.



ELIMINATE ROGUES CONNECTED TO THE NETWORK

Rogue devices are a serious threat to enterprise security. A single rogue access point can allow an attacker to gain full access to the internal network. AirDefense can identify any rogue device and disable it automatically. AirDefense Enterprise identifies rogue devices and determines if they are connected to the internal network. By analyzing wireless traffic, AirDefense can determine the level of threat that a potential rogue poses to the organization. This allows administrators to ignore neighboring devices and focus only on the rogues that present a serious threat.

This advanced analysis also ensures that neighboring wireless devices are not misclassified as a rogue. Accuracy is essential as less sophisticated Wireless IPS systems can easily disable a neighboring access point by mistake opening the organization to unwanted liability.



Device Name	IP	MAC	Status
AP-001	192.168.1.1	AA-BB-CC-DD-EE-FF	Authorized
AP-002	192.168.1.2	AA-BB-CC-DD-EE-FF	Authorized
AP-003	192.168.1.3	AA-BB-CC-DD-EE-FF	Unauthorized
AP-004	192.168.1.4	AA-BB-CC-DD-EE-FF	Unauthorized
AP-005	192.168.1.5	AA-BB-CC-DD-EE-FF	Unauthorized
AP-006	192.168.1.6	AA-BB-CC-DD-EE-FF	Unauthorized
AP-007	192.168.1.7	AA-BB-CC-DD-EE-FF	Unauthorized
AP-008	192.168.1.8	AA-BB-CC-DD-EE-FF	Unauthorized
AP-009	192.168.1.9	AA-BB-CC-DD-EE-FF	Unauthorized
AP-010	192.168.1.10	AA-BB-CC-DD-EE-FF	Unauthorized
AP-011	192.168.1.11	AA-BB-CC-DD-EE-FF	Unauthorized
AP-012	192.168.1.12	AA-BB-CC-DD-EE-FF	Unauthorized
AP-013	192.168.1.13	AA-BB-CC-DD-EE-FF	Unauthorized
AP-014	192.168.1.14	AA-BB-CC-DD-EE-FF	Unauthorized
AP-015	192.168.1.15	AA-BB-CC-DD-EE-FF	Unauthorized
AP-016	192.168.1.16	AA-BB-CC-DD-EE-FF	Unauthorized
AP-017	192.168.1.17	AA-BB-CC-DD-EE-FF	Unauthorized
AP-018	192.168.1.18	AA-BB-CC-DD-EE-FF	Unauthorized
AP-019	192.168.1.19	AA-BB-CC-DD-EE-FF	Unauthorized
AP-020	192.168.1.20	AA-BB-CC-DD-EE-FF	Unauthorized



COMPLY WITH ENTERPRISE & REGULATORY POLICIES

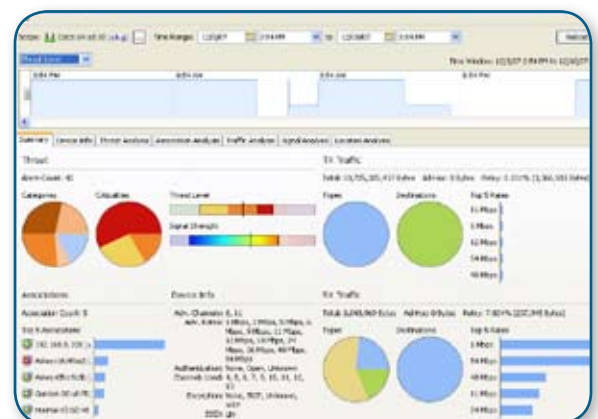
AirDefense Enterprise allows administrators to define, monitor and enforce wireless LAN policies in the areas of security, performance, usage and vendor types. Organizations can minimize vulnerability by ensuring that wireless devices are using the proper security protocols. Mis-configuration is one of the most common causes for wireless security breaches. When a device is found to be non-compliant, AirDefense notifies the administrator of the exact discrepancy.

AirDefense includes a variety of regulatory compliance reports for retail establishments, healthcare organizations, financial service providers and government agencies. There are specific compliance reports for the Payment Card Industry (PCI) Standard, Sarbanes-Oxley (SOX), HIPAA, GLBA, and the Department of Defense 8100.2 Directive. AirDefense administrators can simply print the applicable report to demonstrate the wireless network's compliance.

INVESTIGATE INCIDENTS WITH FORENSIC DATA

AirDefense Enterprise provides forensic data that allows administrators to retrace any one device's steps down to the minute. With forensic research, investigating an event takes minutes instead of potentially hours. Cases that normally would have required administrators to physically visit sites can now be investigated remotely.

Administrators can rewind and review minute-by-minute records of connectivity and communication with the network. By storing more than 325 data points per wireless device, per connection, per minute, AirDefense Enterprise allows organizations to view months of historical data on a wireless device that was recently discovered to be suspicious. AirDefense stores important information such as channel activity, signal characteristics, device activity and traffic flow. AirDefense can display time of attack/breach, entry point used, length of exposure, transfers of data and systems compromised.



TROUBLESHOOT NETWORK PERFORMANCE

With a real-time view of all WLAN traffic, AirDefense enables network administrators to remotely troubleshoot problems, identify and respond to network mis-configurations, and monitor the network's availability. AirDefense analyzes traffic flow to interpret WLAN performance and identify usage characteristics, interference from neighboring WLANs, channel overlap, and performance degradation.

AirDefense can help measure network usage & performance by determining over-utilized APs & channels, pinpointing network congestion, finding bandwidth hogs & analyzing utilization & congestion trends.

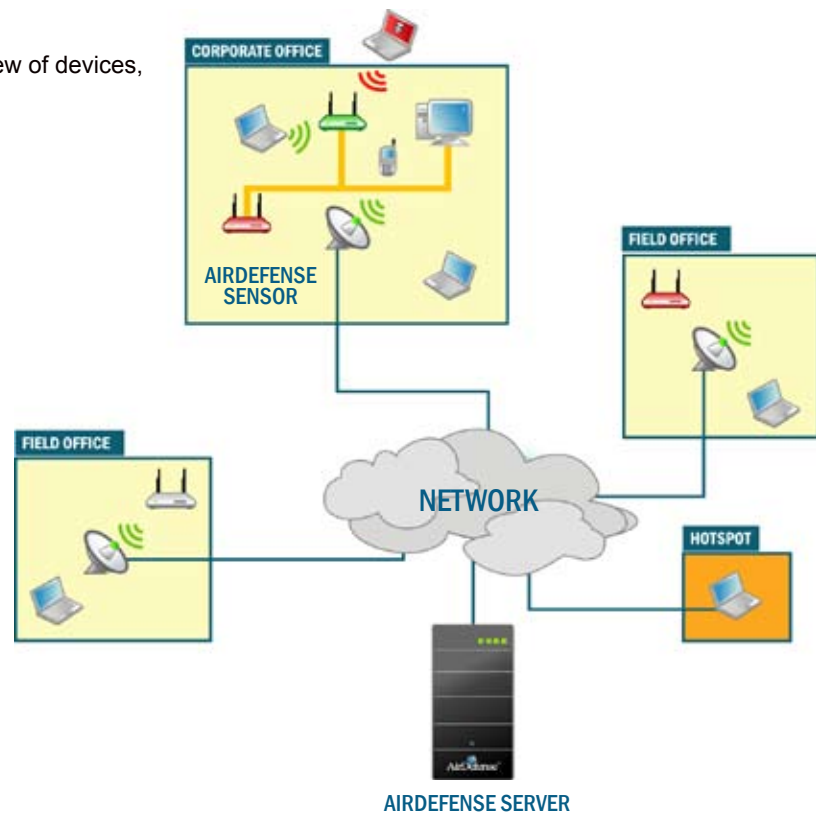
Administrators can drill down into a live, streaming view of devices, BSSIDs, and channels to review:

- Remote frame captures
- Authentication errors
- AP configuration issues
- Network interference

LOCATION TRACKING

AirDefense Enterprise includes powerful location tracking technology that allows administrators to minimize the amount of time required to find a device when visiting a site. After importing images of a floor plan and specifying the characteristics of the building, AirDefense is able to consistently locate devices within four cubicles.

AIRDEFENSE DEPLOYMENT



MOBILE WORKFORCE PROTECTION

AirDefense Personal, an add-on for AirDefense Enterprise, protects end-user laptops when they travel away from the protection of AirDefense sensors. AirDefense Personal is a software agent that enforces wireless policy for remote users. It quietly monitors for malicious or accidental wireless activities and misconfigurations that may cause security exposures or policy violations. AirDefense Personal provides uninterrupted protection for all mobile employees and their enterprise wireless assets - at work, home, airports or other hotspots. Threats detected include risky configuration, insecure communication, suspicious WLAN settings and risky WLAN connectivity.

It integrates with AirDefense Enterprise for:

- Centralized policy definitions and analysis
- Combined alarm management & reporting
- Automated enforcement
- Comprehensive reporting

INNOVATIVE ADD-ON MODULES

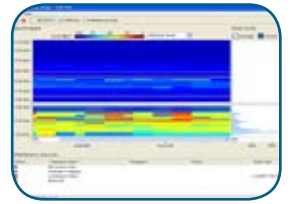
WEP Cloaking

WEP Cloaking provides protection for wireless infrastructure secured by WEP encryption. It helps meet PCI requirements by supplementing WEP encryption and provides protection for WEP networks that would otherwise be extremely vulnerable. It leads to tremendous cost savings by enabling a more orderly process of migrating away from the WEP protocol.



Spectrum Analysis

With Spectrum Analysis, administrators can identify and classify possible sources of non-802.11 interference. Interference types detected include microwaves, cordless phones, wireless cameras and Bluetooth. Administrators can troubleshoot the physical layer of the WLAN in real-time at remote locations without requiring specialized hardware.



Sensor-less Rogue Detection

Sensor-less Rogue Detection allows the administrators to detect and eliminate rogue wireless devices without deploying wireless sensors. It is the most cost-effective and easily deployed solution to identify rogue wireless devices on a large scale and allows for prioritization of sites in need of additional wireless protection.

Advanced Forensics

The Advanced Forensics module provides administrators with the ability to rewind and review detailed records of wireless activity that can assist in forensic investigations or wireless network troubleshooting. It also allows trend analysis for network performance and capacity planning. By storing and managing 325 data points every minute for each wireless device, Advanced Forensics is the ultimate resource for tracking threats and understanding the performance trends of the wireless network.

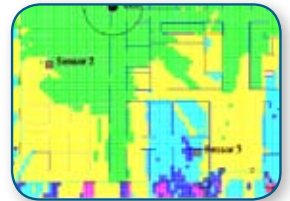


Centralized Management Console

The Centralized Management Console (CMC) manages settings of multiple appliances from one console. Using the CMC, administrators can manage deployments with tens of thousands of sensors from one central console. Settings across multiple appliances can be synchronized to ensure a consistent deployment.

LiveRF

The AirDefense LiveRF module, powered by Motorola technology, provides the industry's only real-time assessment of wireless network performance. Administrators can troubleshoot wireless connectivity, view throughput, capacity, coverage holes and interference issues from a central console. With LiveRF, administrators can visualize the performance of differing wireless applications from simple web browsing to live video without having to go out to remote locations.



ENTERPRISE CLASS SCALABILITY WITH LOWEST TCO

Scalable

AirDefense Enterprise's distributed architecture supports sensors in hundreds of locations reporting back to a centralized appliance.

The high-end appliance supports up to 150,000 devices per appliance with over 35,000 devices concurrently active.

Centrally-managed

Using a single interface for policy enforcement, system/sensor updates & system management, AirDefense Enterprise is easy to use with dashboards and wizards that provide role-based views. Multiple appliances can be managed using the Centralized Management Console.

Easily deployed & reliable

AirDefense Enterprise is an appliance based solution and uses zero-configuration sensors requiring minimal effort to deploy. For redundancy, a secondary appliance can be deployed.

Low bandwidth requirements

Patent-pending optimization algorithms to minimize the amount of wired bandwidth to less than 3 Kbps per sensor, while continuing to maintain full, centralized correlation and complete security.

ABOUT AIRDEFENSE

AirDefense is the market leader in anywhere, anytime wireless security. The company is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other company. AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks.

As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption & authentication. AirDefense Enterprise detects & responds to wireless threats and unauthorized devices on the wireless network using distributed smart sensors (monitoring 802.11 a/b/g) and a secure server appliance. With Common Criteria certification and FIPS compliant cryptography, AirDefense's enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

MARKET LEADER

- 700+ Customers including market leaders in all major industries & government
- More than 35 of Fortune 100 companies depend on AirDefense
- Securing over 10,000,000 wireless devices around the globe

TECHNOLOGY LEADER

- Pioneer of wireless intrusion prevention technology & market
- Most advanced solutions for mobile worker protection regardless of location
- 27 Patents pending covering fundamentals of wireless security
- Common Criteria certified

RECOGNIZED LEADER

- Numerous industry awards for innovation & growth



"After completing an exhaustive search of wireless LAN security and management solutions, DeCA concluded that AirDefense offers the only enterprise-class solution for 24x7, real-time monitoring of the airwaves that scales to support a wireless LAN deployment with more than 1,000 access points around the globe."

Defense Commissary Agency (DeCA)

"(AirDefense) enables us at any one time to graphically depict all over the world what access points are communicating with what (wireless workstations) -- whether there is unauthorized policy set on those devices, whether there are security or performance issues."

News Corp.

"With AirDefense, I sleep well at night knowing that my network is protected from rogue wireless devices."

University of Utah Health Sciences Center

"AirDefense provides the peace of mind from knowing that we can identify and eliminate all unsanctioned wireless laptops, APs, ad hoc networks and application-specific wireless devices as they enter our airspace."

Carilion Health System

