



**AIRDEFENSE GOVERNMENT SOLUTIONS**

WIRELESS SECURITY SOLUTIONS FOR GOVERNMENT

## AIRDEFENSE WIRELESS SECURITY SOLUTIONS FOR GOVERNMENT

The introduction of wireless technologies has created a new avenue for data breaches, circumventing traditional security architectures. New Department of Defense (DoD) policies have made Wireless Intrusion Detection Systems (WIDS) mandatory for all DoD wired and wireless networks. WIDS must provide 24x7 monitoring of the airwaves, have wireless device location tracking capabilities and must be Common Criteria validated. AirDefense Enterprise meets all the DoD stipulated requirements and has been broadly adopted for deployment throughout the DoD. Current DoD customers include the US Army, Navy, Marine Corps, unified combatant commands, defense agencies and intelligence community organizations. In addition to its large presence in DoD, AirDefense's solutions are utilized by dozens of Federal civilian agencies to protect network data, detect unauthorized devices, mitigate threats and to monitor wireless activity.

### Wireless Risks

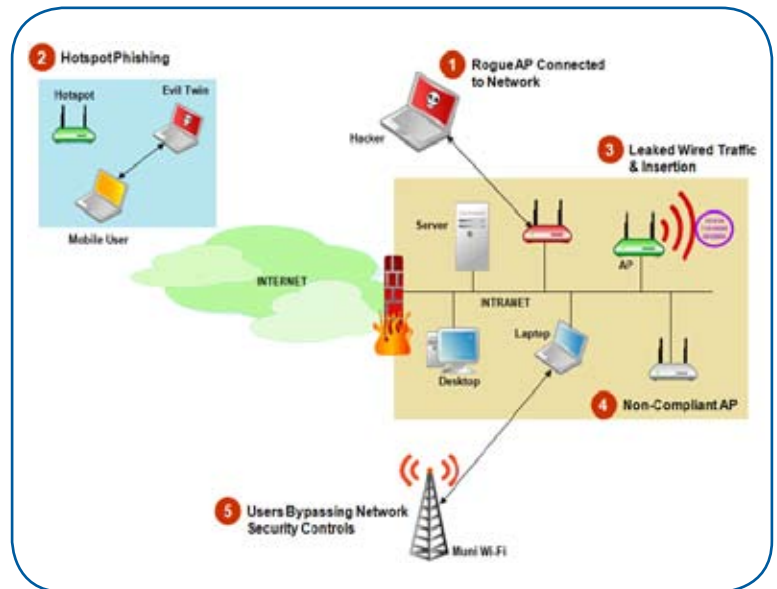
Wireless introduces the following vulnerabilities that traditional security solutions cannot mitigate.

**Rogue Wireless Devices** - A rogue wireless Access Point (AP) is an unauthorized AP physically connected to the wired network. Rogue APs provide attackers with unrestricted access, bypassing firewalls and VPNs, to internal servers just as if they were connected to an internal wired port. Rogue APs can be installed on any network, including networks with no official wireless deployments and networks that have been intentionally segmented from regular wireless networks.

**Identity Thefts** - A hacker can masquerade as an authorized wireless device and connect to an authorized AP. MAC address based filters are useless since wireless MAC addresses are broadcast and hackers can easily change the MAC address of their device. WEP encryption can be cracked in a few minutes. WPA Pre-Shared Key is easy to implement and does not have the vulnerabilities of WEP; however, one common key is used between many devices. Hackers have been known to steal Portable Electronic Devices (PEDs) or use social engineering to obtain passwords. Once a key is stolen or a password compromised, hackers can easily masquerade as an authorized wireless device without having to breach a secure physical perimeter.

**Denial of Service Attacks** - Hackers can easily perform wireless denial of service (DoS) attacks preventing devices from operating properly and stopping mission critical operations. Wireless DoS attacks can cripple a wireless network despite the use of sophisticated wireless security protocols like WPA2. Hackers can insert malicious multicast or broadcast frames via wireless APs that can wreak havoc on the internal wired infrastructure of a high-security network.

**Non-Compliant APs** - Wireless APs and client devices are frequently misconfigured. According to Gartner, a majority of all wireless security incidents will happen as a result of misconfigured devices. Misconfigurations happen for a variety of reasons including human error and bugs in wireless management software. A misconfigured AP at a remote base or central headquarters can be detected and exploited by a hacker to gain access to the network allowing them to attack internal servers and applications. Poorly configured wireless laptops can be phished and compromised very effectively and with relative ease.



Wireless Security Issues in Government

## DoD Wireless Requirements

DoD Directive Number 8100.2 was issued on April 14, 2004. The Directive covers the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG). The Directive spells out policies for deploying secure wireless networks, and requires monitoring of those wireless networks for compliance. On June 2, 2006 the DoD issued a supplemental policy to 8100.2 with the objective of enhancing overall security guidance and to create a foundation and roadmap for increased interoperability that embraces open standards regarding Wireless LAN (WLAN) technologies. This policy applies directly to IEEE 802.11 based WLAN devices, systems and technologies and excludes cellular, Bluetooth, WiMax and proprietary RF communication standards.

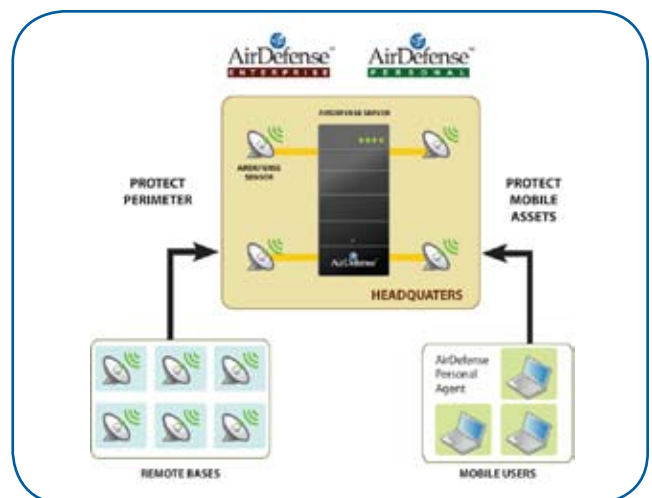
Starting in 2007, DoD Components must implement WLAN solutions that are IEEE 802.11i compliant and WPA2 Enterprise certified that implement 802.1x access control with EAP-TLS mutual authentication and a configuration that ensures exclusive use of FIPS 140-2 (minimum overall Level 1) validated Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) encrypted communications. WIDS was not directly specified in the original 8100.2 Directive. However, the new supplemental policy lays down the following explicit requirements:

1. WIDS is required for all DoD wired and wireless networks.
2. WIDS must continuously scan for and detect authorized and unauthorized devices. Continuous scanning is defined as 24 hours/day, 7 days/week.
3. WIDS must have location sensing capability.
4. WIDS must be National Information Assurance Partnership (NIAP) Common Criteria (CC) validated.

## AirDefense Solution

The AirDefense Enterprise solution was the first industry solution to receive Common Criteria certification and is based on patented technology that incorporates distributed smart IEEE 802.11a/b/g sensors reporting to a central server appliance. The sensors are deployed in remote bases/offices and headquarters. They monitor all WLAN activities 24x7 in their local airspace and communicate with the AirDefense server, which correlates and analyzes the data to provide scalable, centralized management for security and operational support of the WLAN. Administrators access the system via management console software installed on their computer. AirDefense Personal protects mobile laptops from wireless-specific risks that could expose private data and transactions. It allows centralized wireless access policies to be enforced across all wireless laptops. The AirDefense solution addresses three key areas of Federal network security and management.

**Comprehensive Wireless Intrusion Detection/Prevention** – AirDefense Enterprise provides the industry leading solution for rogue wireless detection and containment and 24x7 wireless intrusion prevention. AirDefense Enterprise can accurately distinguish neighboring devices from rogue devices that are connected to the wired network and can be setup to automatically terminate a rogue device over the air. Alternatively, the device can be blocked on the wired side using AirDefense’s switch port suppression feature. To find the location of the rogue device, AirDefense provides accurate map based location tracking using signal strength triangulation. AirDefense Enterprise has the largest wireless attack library with over 200 alarms that can detect a range of attacks such as reconnaissance activity, identity theft, session hijacking or Man-in-the-Middle (MITM) attacks, multiple forms of DoS attacks, wired side leakage, dictionary based attacks, etc. AirDefense reduces false positives by correlating wireless and wired side information in conjunction with rich historical context maintained in its forensic database instead of just looking



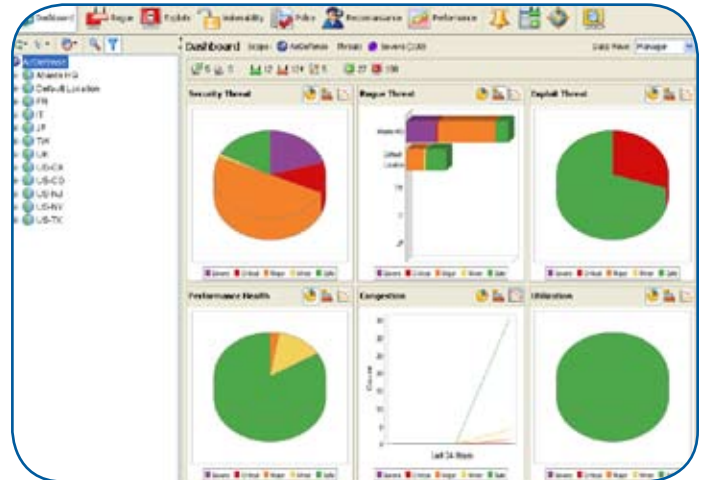
AirDefense Enterprise Solution for Government

## Anywhere, Anytime Wireless Security

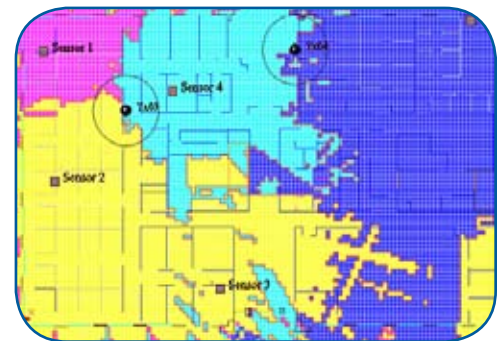
at the present snapshot. AirDefense recognizes documented and undocumented (day-zero) attacks, because it does not rely solely on attack signatures but also on advanced anomalous behavior analysis. Once an accurate assessment of an intrusion is made, AirDefense Enterprise provides wireless and wired termination capabilities to mitigate the threat in real-time.

**Wireless Policy Compliance** – AirDefense provides DoD Components and other Federal agencies the ability to define granular wireless policies for how WLAN devices should be configured and operated and then monitors all WLAN devices 24x7 to identify when any device deviates from that policy. AirDefense can understand and monitor all DoD specific WLAN authentication and encryption policies (WPA2, 802.1x, EAP-TLS, AES-CCMP). Further, AirDefense allows network managers the ability to define WLAN device and roaming policies, WLAN channel policies for approved channels of operation and usage policies such as approved hours of operation. Upon deploying a WLAN, customers have an expectation for how the network should perform. AirDefense allows network managers to define these expectations for performance and audit the wireless network 24x7 for performance compliance. AirDefense Personal allows policy enforcement across laptops when they are outside monitored and secure facilities. By statefully monitoring all WLAN activity, AirDefense Enterprise maintains a historical database that powers robust forensic analysis and historic trending as well as incident investigation. AirDefense stores over 300 statistics for every wireless device on a minute-by-minute basis. With a single click AirDefense can display the time of attack, what entry point was used, the length of the exposure, how much data was transferred, which systems were compromised, etc. DoD policy compliance reports are built into AirDefense Enterprise. The reports are available in several formats and can be automatically scheduled and sent to appropriate personnel or manually generated. In addition, AirDefense allows the creation of fully-customizable reports that leverage the forensic data stored by the system and facilitate compliance management against arbitrary policies.

**Remote Wireless Troubleshooting** – AirDefense Enterprise can significantly reduce the management cost of wireless networks by providing powerful tools for remote troubleshooting. AirDefense can provide the administrator with a live streaming view of all devices, channels, bands and networks to identify hardware failure, RF interference, network misconfigurations, usage and performance problems. AirDefense Enterprise features a LiveRF module that allows Federal network administrators the ability to remotely visualize real-time RF coverage from an application perspective and assess the impact of noise and interference on different applications that are using the WLAN. Given the transient nature of RF interference, LiveRF is indispensable for remote troubleshooting of physical layer wireless problems in real-time.



AirDefense Dashboard



Remote Troubleshooting

## About AirDefense, Inc.

AirDefense, the innovator and market leader of anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection. Ranked among Red Herring's Top 100 Private Companies in North America, AirDefense provides the most advanced solutions for rogue wireless detection, policy enforcement, performance monitoring, troubleshooting and intrusion prevention, both inside and outside an organization's physical locations and wired networks. AirDefense provides protection for all protocols (802.11 a/b/g and Bluetooth), and enterprises and their mobile users. As a key element of wireless LAN security, AirDefense complements wireless VPNs, encryption and authentication. 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.