

WLAN Compliance, Security and Performance in the U.S. Department of Defense

The explosion of wireless technologies has forced the U.S. Department of Defense (DoD) to implement policies that weigh risk vs. reward. As one of the most mobile organizations in the world, keeping commanders and field operatives in sync with wireless data, voice and video communications brings enormous value and operational benefit. Yet introducing new wireless technologies can be one of the greatest security risks that a network can face. Unsecured devices or rogue access points open the door to data vulnerability, denial-of-service attacks, or worse.

Protect Mobile Operations

The only way to ensure wired-equivalency security and reliability is with tools that proactively identify and quantify threats and performance degradation, before they affect operations.

AirMagnet's commitment to the DoD is to provide a comprehensive solution for managing all risks associated with wireless networks that ensures security, performance and compliance. Innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet WiFi Analyzer — which is known as the “de facto tool for wireless LAN troubleshooting and analysis.” Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over WiFi analysis solution.

Mitigate Risk

Wireless networks have expanded the battle capabilities of the U.S. Military, enabling the communication of critical logistics data to officers in the field. Yet when dealing with real-time battle communications, interruptions of any kind — from interference to denial of service attacks — can cost lives. When dealing with issues of national security or battlefield readiness, DoD staff need to be certain that their applications and communications will work as needed.

Constant changes in physical surroundings, new equipment implementations, interference from wireless security devices and malicious security behavior that could compromise a successful WLAN deployment.

The best practices in securing wireless networks revolve around enforcing a clear set of policies designed to mitigate identified risks to WLANs and the data transmitted over them. Policies should detail incident identification and response and identify strategies for accessing the WLAN, authentication schemes, encryption standards, monitoring and reporting. They should also include a scheme to regularly test wireless devices for policy violations.

AirMagnet tames the complexity and exposure of a government WLAN with a true zero-tolerance approach to wireless security that is tied to the policies and needs of individual organizations. AirMagnet Enterprise detects every threat in the network, worldwide, and then automatically takes action with multiple layers of automated threat response. An intuitive global interface provides full disclosure of all wireless events, making it easy to make the right decisions while cutting through the time required managing your networks. The end result is a system that brings simplicity, accountability and bulletproof defenses to any wireless investment.

AirMagnet empowers the DoD to enforce these critical wireless network policies:

- **No Wireless.** According to DoD Directive 8100.2, the burden of proof is on the IT staff to positively demonstrate that they have no wireless devices or access.
- **Compliant Wireless.** In situations where wireless is permitted, IT staff must validate that the wireless network is in compliance with 8100.2 requirements.
- **Highly Secured Wireless.** Departments that depend on wireless communications must prove the highest levels of security and performance, according to 8100.2.

Detect Rogue Devices and Defend Against Threats

All networks are faced with the issue of rogue devices, but in the case of defense networks, the introduction of unsecured devices is not only a violation of the Directive, it can have devastating effects. Intrusion detection systems, like AirMagnet Enterprise, offer 24/7 active, full-time protection against rogues and hundreds of other wireless threats, including vulnerabilities, denial-of service attacks, MAC spoofing, fragmentation attacks, evil twins, unapproved connections and scores of wireless hacking and reconnaissance tools. Only AirMagnet has advanced technology that can verify that there are no Bluetooth devices accessing the network.

All detected threats and devices can be traced and located, blocked with both wired and wireless suppression methods, and saved for forensic analysis. The enterprise WLAN monitoring solution provides continuous scanning of all WiFi channels including all 200 extended 11a channels to ensure there are no blind spots where rogues can hide and patent-pending WEP Shielding provides additional protection for devices using WEP encryption.

Proactively Manage Network Performance

Dense concentrations of high-tech devices, electrical interference and physical obstructions—especially in urban warfare zones—can disrupt wireless communications with dire consequences. AirMagnet offers the only dedicated sensors to include full spectrum analyzers for troubleshooting non-WiFi sources of interference or security problems.

AirMagnet makes it easy to identify the sources of interference, tracking the problem to a physical location for quick resolution. AirMagnet is designed to provide continuous, stateful analysis of all enterprise WLANs for evolving threats and performance problems and pinpoint the root cause of any issues. The system can proactively alert staff to all types of performance problems, above and beyond RF and interference issues, including overloaded devices and channels, traffic problems, mismatched devices and much more. Threats can be automatically traced, located, blocked and saved for later forensic analysis.

Remote Troubleshooting

In battle, IT specialists can't be on the ground monitoring network performance. Network security specialists rely on AirMagnet Enterprise to secure and manage their wireless networks, streamlining security and support through a centralized system.

Because the reliability and performance of the network is critical to operations, this comprehensive WLAN monitoring solution also provides a full featured remote network analyzer including live drill-down into any device, packet decoding and a suite of connection troubleshooting tools to get clients up and running quickly and remotely.

Compliance Reporting

Compliance reporting is at the heart of all DoD operations, and is nearly as important as the operational infrastructure and capabilities themselves. Departments that have a no-wireless policy require a strong documentation process providing the proof needed to show compliance in a systematic and highly detailed report. For those departments permitted to utilize wireless networking, the Directive requires strong authentication with identity management and non-repudiation capabilities implemented at both the device and network level.

All information must be encrypted — even unclassified data. If the encryption does not meet Federal Information Processing Standards (FIPS), then the wireless capabilities in the device must be disabled, or the device itself must be removed.

AirMagnet's integrated reporting engine arms IT staff with reports that track compliance with Directive regulations. Detailed, customizable reports provide a step-by-step pass/fail assessment of every component of the Directive for any location or date range, with explanations of the standards and the reasons why devices were flagged for non-compliance, when applicable. High-level, easy to read dashboard views, such as pie charts, break down compliance by various categories, highlighting vulnerabilities that require special attention.

Visibility. Control. Security.

AirMagnet protects against every wireless threat by combining the industry's most thorough wireless monitoring with the deepest analysis and threat response available. It enables defense operations to confidently deploy, secure and manage their wireless deployments through innovative planning, troubleshooting and monitoring solutions.

AirMagnet is uniquely able to:

- Proactively detect or stop hundreds of wireless LAN problems and security issues
- Track and record all wireless devices and behavior
- Proactively notify IT teams about evolving problems before users are affected
- Design and deliver WLANs that meet the unique physical and application needs of each department
- Detect and identify sources of interference that can impede network performance and degrade reliability
- Automatically generate detailed DoD Directive 8100.2 compliance reports for all devices and sites
- Ensure that networks are designed from the ground up to meet precise security, performance and compliance needs

Certifications

- First and only WIDS/IPS vendor to receive FIPS 140-2 Certification.
- Officially placed on the Common Criteria "Products under Evaluation" list for AirMagnet Enterprise System 8.0 at Evaluation Assurance Level 2

Corporate Headquarters

830 E. Arques Avenue
Sunnyvale, CA 94085 - USA
Tel: +1.408.400.0200
Fax: +1.408.744.1250

www.airmagnet.com

EMEA Headquarters

St. Mary's Court, The Broadway, Amersham
Buckinghamshire, HP7 OUT - United Kingdom
Tel: +44.1494.582.023
Fax: +44.870.139.5156

 **AIRMAGNET**
Wireless Network Assurance