

Refense VMS™

Ensuring Compliance with DoD Directive 8100.2

Overview

DoD computer networks are frequent targets of attack and as such require proactive security measures to maintain the highest level of security. Maintaining a secure network has become increasingly difficult, considering the explosive amount of new vulnerabilities and the rapid adoption of wireless technology. The DoD Directive Number 8100.2 defines the security policies for the usage of wireless technologies within the DoD Global Information Grid (GIG).

The main purpose of this policy is to protect DoD computer networks from the security vulnerabilities introduced via wireless networks. Some of the requirements of Directive 8100.2 include:

- 4.1.1 – Implementing strong identification and authentication measures for wireless users
- 4.1.2 – Encryption of data, to and from wireless devices
- 4.1.5 – Introduction of wireless technologies requires a security review and documentation
- 4.10 – Must disseminate information on wireless vulnerability assessments, best practices, and procedures for wireless device configurations
- 5.2.3.1 – Implement a capability to assess the risks and vulnerabilities associated with wireless technologies

DoD Directive 8100.2 applies to all wireless devices and technologies, specifically including widely used 802.11 standard, also known as Wi-Fi. Additionally, the scope of this directive is applicable not only to all DoD employees, but also all contractors and visitors that enter DoD facilities or that have access to DoD information.

The Most Effective Solution for Complying with DoD Directive 8100.2

Manually performing periodic vulnerability assessments of wireless devices, is labor intensive, expensive and when considering the enormous scope and the diverse network of an enterprise, it is nearly impossible. Attempting to manually detect a single misconfigured vulnerable wireless network among thousands is a great example of the proverbial “needle in a haystack” and the key reason why many large enterprises have suffered from wireless attacks. Refense VMS™ effectively solves this problem by easily and proactively identifying the threats and vulnerabilities within wireless networks.

Refense VMS™ specifically assists in complying with Directive 8100.2 by:

- Detecting vulnerabilities such as lack of wireless encryption and access control
- Providing a scalable, enterprise solution for determining the risks and vulnerabilities within networks
- Providing an efficient, automated solution to perform security reviews and fully document the security posture
- Enabling the enterprise to quickly disseminate security reports, policies and best practices via the built in capabilities of the product



About Refense

Refense Technologies is a leading provider of vulnerability management solutions for network devices. The company develops solutions that address security concerns within network devices, the foundation of an IT infrastructure. With Refense VMS™, organizations can proactively identify and mitigate threats and vulnerabilities within wireless and wired network devices.



Refense Technologies, Inc
105 Brooks Ave
Raleigh, NC 27607
Phone 1.800.432.6187
sales@refense.com
www.refense.com