



KEY FEATURES

- World's best wireless intrusion prevention technology

- Automatically detects, blocks and locates rogue APs & other Wi-Fi threats

- Blocks unapproved smartphones and tablets

- Off-line sensor mode for fault-tolerant continuous policy enforcement

- Detects and locates 'non Wi-Fi' interference & RF jamming

- Smart Forensics™ for quick resolution of wireless incidents

- Remote troubleshooting including remote "live packet capture"

- Also available on VMware



SpectraGuard Enterprise

Industry's Top Ranked Wireless Intrusion Prevention System

Wireless LAN (WLAN) infrastructure attacks are today one of the most critical and immediate threats to enterprise networks. To make matters worse, the consumerization of Wi-Fi is flooding enterprises with personal Wi-Fi enabled smartphones and tablets, which are inadvertently tearing down the network security perimeter; organizations without an officially deployed WLAN are also at risk.

AirTight's SpectraGuard Enterprise wireless intrusion prevention system (WIPS) provides enterprises with continuous and the most comprehensive protection against current and emerging wireless threats.

Unmatched Wireless Protection

Powered by AirTight's portfolio of patented wireless intrusion detection and prevention techniques, SpectraGuard provides 24/7 visibility into and complete control over enterprise airspace.

Automatic device classification: Using AirTight's patented Marker Packet™ techniques, SpectraGuard automatically and quickly classifies wireless devices detected in the airspace as Authorized, Rogue and External. As a result it eliminates false alarms and saves you the effort of defining complex rules to identify rogue wireless devices or manually inspecting devices. This is unlike the error-prone device classification integrated into most WLAN infrastructure, which relies on slow and inconclusive CAM table lookups and passive wired network sniffing.

Automatic threat prevention: Automatic over-the-air prevention is a must for effective wireless security as it allows enterprises to respond immediately in the wake of a wireless security incident. But most wireless IDS/IPS solutions do not encourage automatic over-the-air prevention for fear of disrupting own or

neighboring Wi-Fi networks. Because of SpectraGuard's accuracy in distinguishing genuine wireless threats from neighboring Wi-Fi devices, it effectively and confidently uses over-the-air prevention in addition to wire-side prevention for blocking any misuse of Wi-Fi or violation of enterprise security policies.

Protection from unapproved smart devices:

In today's "BYOD" (bring your own device) culture, the rapid adoption of smartphones and tablets poses an immediate threat to your network. Authorized users need only their enterprise login credentials to connect unapproved personal devices to WPA2/802.1x secured Wi-Fi networks and access sensitive enterprise assets. Data leakage on unapproved personal devices, malware and viruses, and "tethering" can compromise enterprise data security without the security administrator ever knowing about it. Monitoring and blocking unapproved Wi-Fi devices, including smartphones and tablets, is an integral part of SpectraGuard Enterprise.

Accurate location tracking: SpectraGuard can pinpoint the physical location of a vulnerable or threat-posing device allowing security administrators to track down and physically remove the device in question. It can provide both real-time and historical location details for a device. AirTight's self-calibrating sensors enable accurate location tracking without the need to conduct RF site surveys.

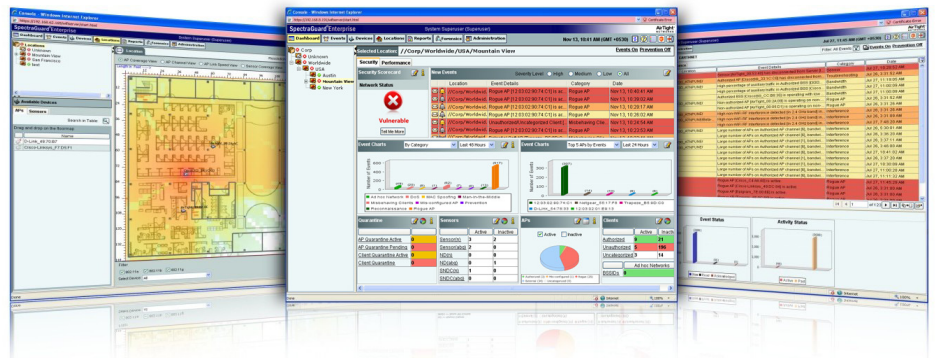
Location-based Policy Management

SpectraGuard Enterprise simplifies the administration of geographically distributed locations through customizable policies defined on a region-by-region, site-by-site or even floor-by-floor basis. The hierarchical location-based management architecture allows network administrators to manage large number of sites from a single console.

About AirTight Networks

AirTight Networks is the global leader in wireless security and compliance products and services, providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers industry's leading wireless intrusion prevention system (WIPS) and the world's only SaaS based wireless security, compliance and Wi-Fi access branded as AirTight Cloud Services™. AirTight's award-winning solutions are used by customers globally in the financial, government, retail and hospitality, manufacturing, transportation, education, health care, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 24 U.S. and international (Australia, Japan and UK) patents granted, and more than 20 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit: www.airtightnetworks.com.

AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. AirTight Networks, AirTight Networks logo, AirTight Cloud Services and AirTight Secure Wi-Fi are trademarks. All other trademarks are the property of their respective owners.



Smart Forensics™

AirTight's Smart Forensics simplifies wireless forensics by filtering out useless data and presenting only relevant and accurate forensics information in an easy to understand and actionable format. Smart Forensics summarizes all relevant information without the need for cumbersome trace collection and packet-level analysis.

Integration and Interoperability

With the broadest integration of any WIPS solution, SpectraGuard lowers deployment and operational costs by integrating with most major WLAN infrastructure vendors. This integration creates a seamless workflow and eliminates inefficiencies, making it easier to manage WLAN security and performance.

SpectraGuard also interoperates with standard enterprise management and reporting platforms including ArcSight, CheckPoint, McAfee ePO and Qualys. SNMP and Syslog interfaces provide the flexibility to integrate SpectraGuard's wireless events with virtually any centralized event management tools.

Simplified Regulatory Compliance

SpectraGuard simplifies compliance with regulatory wireless security requirements

via automated wireless scanning, consolidated analysis of scan data from multiple locations and ready-to-use compliance reporting.

SpectraGuard Enterprise provides predefined reports that map wireless vulnerabilities to specific data security compliance standards such as PCI DSS, Sarbanes-Oxley (SOX), HIPAA, Gramm-Leach-Bliley (GLBA), and DoD Directive 8100.2. Network administrators have the option to schedule reports to be automatically generated and delivered to them by email.

Predictive Wireless Performance

SpectraGuard Enterprise can also alert administrators of wireless LAN performance problems before they impact end users. It classifies performance issues into various categories such as configuration (e.g., incorrect channel allocation, sub-optimal 802.11n protocol settings), bandwidth (e.g., poor utilization, low average data rate, excessive overhead), and RF (e.g., non Wi-Fi interference, channel crowding).

Remote troubleshooting including remote "live packet capture" from a central console allows network administrators to resolve problems at remote sites quickly without sending IT staff to those locations.

The Global Leader in Wireless Security Solutions

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 www.airtightnetworks.com info@airtightnetworks.com

© 2011 AirTight Networks, Inc. All rights reserved. AirTight Networks and the AirTight Networks logo are trademarks, and AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. All other trademarks mentioned herein are properties of their respective owners. Specifications are subject to change without notice.

