



Unprecedented Visibility into Wireless Vulnerabilities

AirTight[®] Networks enables enterprises to protect both wired and wireless networks and mobile client security from wireless vulnerabilities. AirTight delivers around-the-clock threat monitoring and automatic intrusion prevention and manages wireless network performance for maximum capacity and uptime. With continuous scanning of the airwaves, your company is automatically protected against data leakage through the wireless network. Within minutes, you can proactively detect and eliminate threats with the industry's most accurate and robust automated classification technology. Simplified Regulatory Compliance Reporting SpectraGuard simplifies the task of both internal and regulatory audits with easy to use auditing and reporting tools. SpectraGuard Enterprise provides predefined reports that map wireless vulnerabilities to specific data security compliance standards such as PCI, Sarbanes-Oxley (SOX), HIPAA, Gramm-Leach-Bliley (GLBA), and DoD Directive 8100.2. Accurate on-wire/off-wire classification filters neighbouring devices from the reports, eliminating the guesswork and time needed to validate the results of your vulnerability scans. Automated report generation and delivery make complex wireless audits a "hands off" process. Unsurpassed Threat Detection and Remediation, SpectraGuard Enterprise, protects your organization from emerging threats including comprehensive 802.11n rogue APs, Multi-Pot threats, Denial of Service, and WEP cracking attacks. AirTight's unique DoS prevention disrupts malicious behaviour and reclaims bandwidth for your authorized APs and clients keeping your mission critical applications running at optimal efficiency. AirTight's location tracking technology is the most precise solution that accurately locates any unauthorized access point or client on your floor map for quick removal.

Cisco WLAN Integration

SpectraGuard lowers deployment and operational costs by leveraging customers' Cisco WLAN environment to automatically synchronize device inventory, automatically detect and classify managed devices and by leveraging the background scanning of Cisco APs. By using Cisco APs as RF data sources, AirTight can reduce sensor density by up to 30% while providing higher accuracy live RF views of the Cisco WLAN infrastructure.

Designed for Manageability and Scalability

Distributed WLAN deployments are difficult to administer. Organizations need enhanced security while minimizing the cost and administrative burden associated with a comprehensive wireless security policy. With SpectraGuard, enterprises can design their WLAN management hierarchy in the optimal fashion for their deployment—segmenting their WLAN network and security operations functions just as they do for their wired network.

Location-Based Policy Management

SpectraGuard Enterprise simplifies the security and administration of a distributed WLAN deployment through granular, customizable policies localized on a site by site, region by region or even floor by floor basis.

Remote Management and Troubleshooting

Wireless network performance and operational issues can happen at any remote location in your global enterprise. SpectraGuard Enterprise provides performance management and knowledge-based troubleshooting features that allow analysis and resolution of remote wireless network issues from a central location and delegation of management to local administrators.

Interoperability

SpectraGuard interoperates with standard enterprise management and reporting platforms including ArcSight ESM, Check Point Suite, Cisco WLSE, and Cisco WLC. Integration with network management systems via SNMP and Syslog interfaces consolidates wireless vulnerability management with your existing tools.

SpectraGuard[®] SAFE (Laptop Security)

Wireless Security Agent For Endpoints (SAFE) Protect mobile clients from wireless threats – 24x7

Protect Mobile Clients from Wireless Threats – 24 x 7, wherever they are!

Business today requires network and email connectivity around the clock and around the globe. Laptops and their users are mobile. They require connectivity in the office, on the road, and at home – and more than half the time when they are mobile, they are on wireless connections. WLAN connectivity while convenient and easy to use, also creates a number of security risks for the laptop as well as the network. While the laptop is in a corporate facility – it can be protected by a wireless intrusion prevention system (WIPS). However, when it's out of the office, the only protection that can work is software on the laptop itself. To provide this functionality, AirTight Networks provides SpectraGuard SAFE (Security Agent For Endpoints).

- Lightweight software agent that runs on mobile devices
- Prevents use of open wireless networks even when away from the office, if desired by the administrator
- Protects against common wireless threats such as ad hoc networking, Evil Twin/Honeypot access points and WiPhishing
- Enhances security provided by mobile device firewall, anti-virus and VPN software