AirTight®
NETWORKS

AirTight
DATA SHEET

- *Automatically classify all wireless devices*
- *Simultaneously detects and prevents threats with alerts to over 150 events including:*
  - *- Rogue Access Points*
  - *- Misconfigured Access Points*
  - *- Ad hoc connections*
  - *- Unauthorized Client connections*
  - *- Client mis-associations*
  - *- Honeypot/evil twin attacks*
  - *- MAC Spoofing*
  - *- Denial of Service attacks*
- *Easily troubleshoot client performance and connectivity issues*
- *Centralized management for end points (SpectraGuard SAFE clients)*
- *Creates compliance reports for Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, DoD Directive 8100.2 and PCI*

# SpectraGuard | Enterprise

## A Comprehensive Wireless IPS and Performance Management Solution

### Protect Your Confidential Business Information

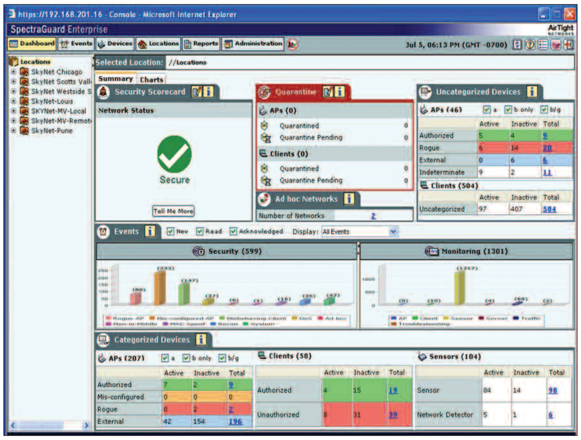
For enterprises with wireless LAN networks, as well as those without, Wi-Fi brings a new set of security threats that cannot be protected against by your current firewall and VPN security systems. Insecure deployments of wireless Access Points (APs) called Rogue APs, often done without malice by your own employees, can open up your network to potential hackers exposing confidential information about your business, customers, products and services. Client mis-associations may lead to additional vulnerabilities. The SpectraGuard® Enterprise Wireless IPS solves these problems by delivering similar protection as a wired firewall, but focused on your corporate airwaves.

- Automatically identify and prevent security risks and attacks
- Provide real-time network audits
- Assist in performance troubleshooting
- Monitor the overall health of the wireless LAN

### Complete the Network Defenses Provided by Your Firewall and VPN

Traditional firewalls only monitor wired traffic and have no visibility into the wireless traffic that is flowing in the air. SpectraGuard Enterprise is a complete wireless intrusion detection and prevention solution comprising a Server and wireless Sensor devices, which continuously scan the airwaves and provide automatic protection against any unauthorized wireless activities.

- Blocks all unauthorized access and rogue traffic without disrupting authorized wireless communication
- Simultaneously prevents multiple threats while continuing to scan for additional problems
- Immediately alarms for clients and APs on banned list
- Compatible with any vendor's wireless Access Points, firewalls and VPNs



Selected Location: //Locations

APs (0)

| | |
|---|---|
| Quarantined | 0 |
| Quarantine Pending | 0 |

Clients (0)

| | |
|---|---|
| Quarantined | 0 |
| Quarantine Pending | 0 |

Number of Networks 2

APs (46) ☑ a ☑ b only ☑ b/g

| | Active | Inactive | Total |
|---|---|---|---|
| Authorized | 5 | 4 | 9 |
| Rogue | 6 | 14 | 20 |
| External | 0 | 6 | 6 |
| Indeterminate | 9 | 2 | 11 |

Clients (504)

| | Active | Inactive | Total |
|---|---|---|---|
| Uncategorized | 97 | 407 | 504 |

☑ New ☑ Read ☑ Acknowledged Display: All Events

APs (207) ☑ a ☑ b only ☑ b/g

| | Active | Inactive | Total |
|---|---|---|---|
| Authorized | 7 | 2 | 9 |
| Mis-configured | 0 | 0 | 0 |
| Rogue | 0 | 2 | 2 |
| External | 42 | 154 | 196 |

Clients (58)

| | Active | Inactive | Total |
|---|---|---|---|
| Authorized | 4 | 15 | 19 |
| Unauthorized | 8 | 31 | 39 |

Sensors (104)

| | Active | Inactive | Total |
|---|---|---|---|
| Sensor | 84 | 14 | 98 |
| Network Detector | 5 | 1 | 6 |

*Quickly view current security and performance status with a high-level dashboard.*

THE LEADER IN WIRELESS INTRUSION PREVENTION

### Eliminate Time Consuming False Positives

Other solutions claim rogue AP detection, but don't tell you whether the discovered AP is on your network, or a neighbor's network. Sorting through false alarms about neighboring wireless networks is the last thing you need to worry about. Using patented auto-classification techniques, external devices are accurately classified and ignored while those that pose a threat to the network are immediately blocked.

- Automatic device classification of both APs and clients
- True rogue AP detection
  - Clearly identifies APs on your network versus external APs
- Proper identification of external APs

### Most Robust Wireless Threat Prevention

Full visibility of both the air space and the wired network is required to ensure bullet proof detection and prevention. Only AirTight provides Network Detector capability enabling full visibility of your wired network without requiring a Sensor on each subnet.

- Patented technology prevents all major categories of threats from compromising your network
- Unique Network Detector mode lowers costs
- Prevent over 20 threats simultaneously from a single sensor

### Simple Wizard Interface Enables Deployment in Three Easy Steps

SpectraGuard Enterprise can be set up in less than half an hour. A simple Wizard interface guides you through the appropriate steps to quickly defend your network.

- Set security policies based on encryption, AP vendor, 802.11 protocol or any combination
- User-definable classification rules to match your security risk profile
- Comprehensive dashboard view for updates at a glance

### Enterprise Level Integration Capabilities

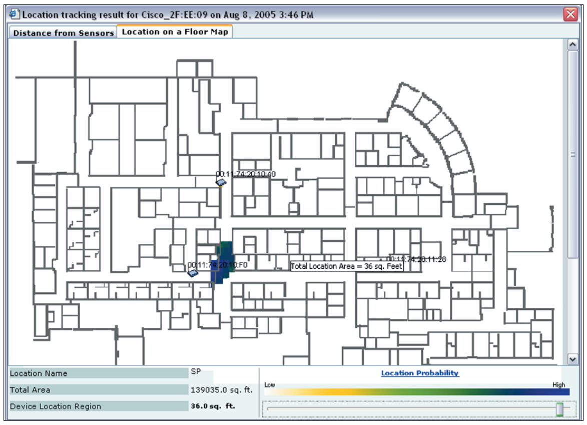
SpectraGaurd Enterprise is interoperable with other enterprise management and reporting platforms

- ArcSight ESM
- Check Point Eventia Suite
- Cisco WLSE
- Syslog

### Find Rogues Quickly with Precise Location Tracking

SpectraGuard Enterprise automatically shuts down unauthorized wireless communication to protect your network immediately. To permanently remove the security threat, precise location tracking quickly pinpoints both rogue APs and Clients.

- Display rogue devices on your floor plans for quick removal
- Unique probability graph shows the most likely location
- Optional integration with floor plans from SpectraGuard Planner



Location tracking result for Cisco_2F:EE:09 on Aug 8, 2005 3:46 PM

| | |
|---|---|
| Location Name | SP |
| Total Area | 139035.0 sq. ft. |
| Device Location Region | 36.0 sq. ft. |

*Precisely locate any access point or client.*

### Troubleshoot Network Performance Issues Easily

Low throughput or intermittent connectivity problems can plague network administrators responsible for wireless networks. Knowledge-based Troubleshooting provides step by step instructions that help desk personnel can use. Suggested remedies get your users up and running quickly.

- Resolves AP and client performance and connectivity problems
  - Packet or event-based data capture
  - Step-by-step flow charts simplify troubleshooting

### Simplified Compliance Reporting

Many IT organizations now face regular compliance reporting requirements whether it be Sarbanes-Oxley, HIPAA, GLBA and many others. Pre-defined reports simplify this task. Interactive drill-down features as well as customizable reporting and delivery frequency provide the information you need, when you need it.

- Predefined reports for Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, DoD Directive 8100.2, and PCI
- Security violation summary for each section of the regulation
- Drill-down feature to see detail on each event

## Designed for Scalability and Manageability

SpectraGuard Enterprise provides the management capabilities needed for today's enterprise. For remote management as well as monitoring, SpectraGuard Enterprise delivers the protection and performance you need across the nation, or around the globe.

- SpectraGuard Managed Network Console (Manager of Manager) functionality provided to aggregate multiple SpectraGuard Enterprise servers
- Granular administrator management for large enterprise deployments
- Scalable up to tens of thousands of sensors and millions of devices
- At-a-glance dashboard provides comprehensive information for all sites
- Central policy deployment to Sensors in remote and branch offices over any WAN link
- Centralized policy management and auditing for SpectraGuard SAFE clients

SpectraGuard Enterprise includes capabilities for multiple tiered levels of management, as well as scalability and performance enhancements that will support the requirements of the largest enterprises. SpectraGuard also has the ability to manage tens of thousands of SpectraGuard SAFE clients from a single server/appliance, providing a new level of wireless security management to the enterprise.

The SpectraGuard Enterprise server/appliance also provides support for thousands of sensors and millions of WLAN devices, enterprises can now 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.

## Architecture

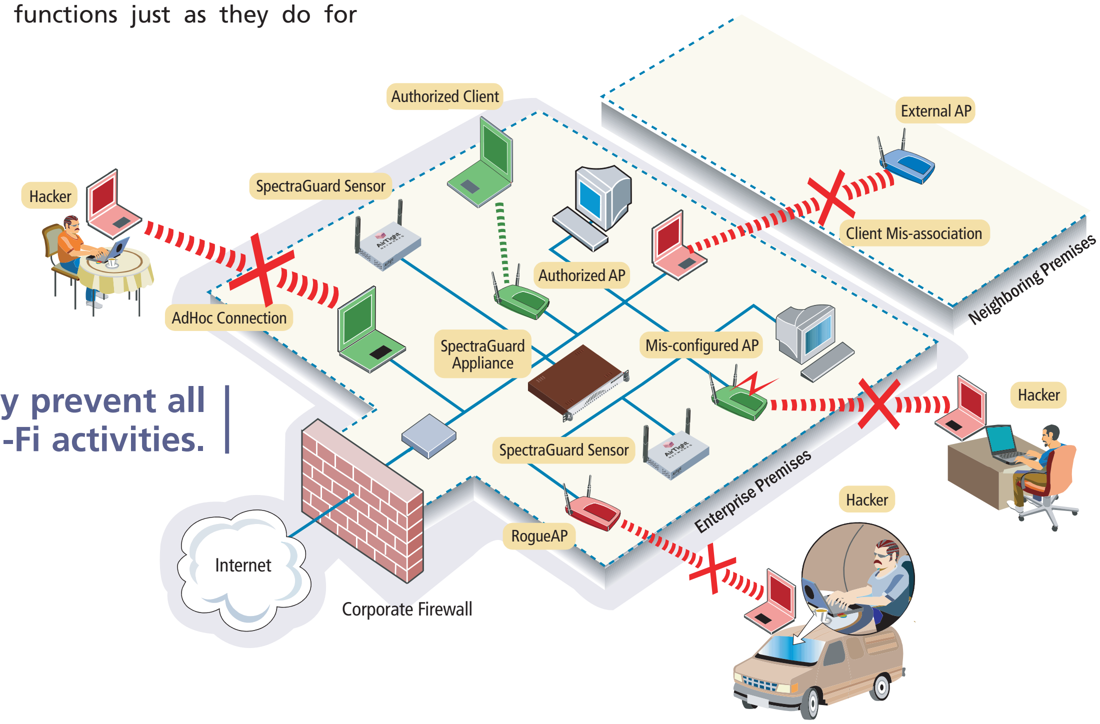
SpectraGuard Enterprise is based on AirTight Networks' Wireless Intrusion Prevention and Performance Management (WIPPM) architecture.

The WIPPM architecture is comprised of four tiers: the wireless devices or clients, wireless sensors which see and protect the clients, the WIPPM server(s) which manages the sensors, and a Management Console which provides visibility, intrusion prevention, and management capabilities across multiple WIPPM servers and millions of wireless devices.

AirTight's WIPPM architecture delivers lower capital and operations costs for a wireless network infrastructure, as well as higher performance, higher reliability, and higher security on that wireless infrastructure.

- Capital cost savings stem from enhanced placement and utilization of the wireless infrastructure – through better planning and management visibility.
- Operational cost savings are driven by the need for fewer people as well as management and compliance reporting, improved diagnostics, and tools that allow for faster and more accurate and effective response to wireless problems that occur.
- Higher performance on the wireless network is provided through more efficient management and protection of the spectrum, both proactive and reactive.
- Higher security is the cornerstone deliverable – of SpectraGuard Enterprise – through intrusion detection, prevention, and location of wireless threats – automatically, accurately, and robustly – no matter how they occur, across tens of thousands of sensors and millions of devices.

**Automatically prevent all unauthorized Wi-Fi activities.**



## *About AirTight Networks*

*Founded in 2002, AirTight Networks is the leader in wireless intrusion prevention and performance management (WIPPM) solutions. AirTight Networks' SpectraGuard® family of WIPPM performance products and services provides enterprises and service providers with around-the-clock wireless monitoring and automatic intrusion prevention, while managing wireless LAN network performance for maximum performance, capacity and uptime. The SpectraGuard family of products is the industry's only solution that correctly classifies wireless devices and events; and automatically identifies, automatically stops, and accurately locates wireless security risks and attacks. AirTight Networks' solutions scale from a single laptop to networks with millions of wireless devices. AirTight Networks is a privately held company based in Mountain View, CA. For more information, visit the company's Web site at www.airtightnetworks.net.*

**AirTight Networks**

339 N. Bernardo Avenue
Suite 200
Mountain View, CA 94043

Tel: +1 877 424 7844
Tel: +1 650 961 1111
Fax: +1 650 961 1169

www.airtightnetworks.net
info@airtightnetworks.net

## Specifications

| | |
|---|---|
| **Wireless IPS** | |
| Wireless Protocols Supported | 802.11b, 802.11b/g, 802.11a, 802.11 pre-n, 802.11 draft-n, Turbo a/b/g |
| Protocol Inspection for Security and Authentication Method | Encryption: WEP, TKIP, CCMP<br>Authentication: 802.1x, WPA, WPA2, 802.11i |
| AP Vendors Discovered | 3Com, Cisco, D-Link, Linksys, Netgear, Proxim, Symbol and many others |
| Automatic SSID Discovery | Yes |
| Auto-classification of Devices | APs: Authorized, rogue APs, external APs, insecure (misconfigured)APs, soft APs<br>Clients: any client type embedded or standalone, authorized or unauthorized |
| Automatic Intrusion Prevention | Rogue APs, insecure (misconfigured) APs, authorized clients connecting to external Wi-Fi networks, ad hoc networks, MAC spoofing, Evil Twin/honeypot APs |
| Denial of Service Prevention | Authentication flood, deauthentication flood, association flood, disassociation flood, EAPOL floods and others |
| Wired-side Switch Port Blocking | Yes, via integration with Cisco Systems Wireless LAN Solutions Engine |
| Prevention Level | Selectable; "Deter" to "Complete Blocking" |
| Simultaneous Scanning and Prevention of Attacks | Yes, with protection for over 20 simultaneous attacks per sensor |
| Channels | 62 sense & defend channels |
| **Location Tracking** | |
| Floorplan Mapping | APs and clients; authorized and unauthorized |
| Display Method | Distance from sensors; probability plot on floorplan |
| **Planning** | |
| Input Method | Scanned floorplan, location of APs and sensors (drag and drop) |
| Planning Views | Wi-Fi network: Link speed, capacity, redundancy, RF spillage<br>Security sensor network: Coverage |
| Scenario Analysis | Channel allocation, output power, protocol selection (.11a, .11b or .11g) |
| Calibration | Automatic feedback to improve prediction accuracy |
| **Monitoring and Reporting** | |
| Realtime Coverage Maps | Realtime RF and security sensor coverage maps |
| Realtime Network Monitoring Charts | Dynamic, customizable dashboard of network performance and events. Includes top devices by event, number of associated clients by AP, top devices by bandwidth usage, bandwidth usage for devices, and more. |
| RF Coverage Statistics | Dynamic display of signal strength, channel allocation, link speed at any point |
| Alerts | Over 150 security and performance alerts |
| Alerting Method | Email, SNMP, Syslog |
| Regulatory Compliance Reports | Sarbanes-Oxley, Healthcare Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, DoD Directive 8100.2, PCI and MITS. |
| Standard Report Types | Wireless device inventory, location |
| Customizable Reports | Build custom reports based on query(ies) of database for event type, client type, and many others. |
| Automatic Report Generation Interval | Set specific day, hour and repeating frequency with customizable delivery options. |
| **System Management** | |
| Management Interfaces | Web, SSH, SNMP, and Syslog |
| Rapid Deployment | Setup Wizard Automatic server discovery, Automatic sensor software verification |
| **Network** | |
| Server Interface | Auto-sensing 10/100/1000 Mbps Ethernet |
| Sensor Interface | Auto-sensing 10/100 Mbps Ethernet |
| IP Address Assignment | DHCP or static |
| Server and Sensor Communication | IP |
| Secure communications | FIPS compliant |
| **Environmental** | |
| Standard and Premium Servers: | |
| Operating Temperature | 10 to 35° C |
| Storage Temperature | -40 to 70° C |
| Humidity | Non-Operating: 95%, non-condensing at 30°C |
| Sensor: Operating Temperature | 0 to 55°C |
| Storage Temperature | -20 to 70°C |
| Humidity | Max 95% |
| Safety Certification | UL2043 (plenum), CSA, EN60950, and IEC60950 |
| RoHS | Compliant with Restriction of Hazardous Substances Directive |
| **Power Supply** | |
| Standard Server | Autosensing 100-127/200-240 V, 50/60 Hz, 6/3 A |
| Premium Server | Autosensing 100-127/200-240 V, 50/60 Hz, 5/2.5 A |
| Sensor | Autosensing 100/240 VAC; 50/60 Hz or IEEE 802.3af Power over Ethernet |
| **Physical Specifications** | |
| Standard Server: Dimensions | 17 x 26 3/4 x 1 3/4 in (w x d x h), 432 x 680 x 45 mm |
| Weight | 24 lbs (10.91 kg) |
| Premium Server: Dimensions | 17 x 29 x 1 3/4 in (w x d x h), 432 x 737 x 45 mm |
| Weight | 28.9 lbs (12.73 kg) |
| Sensor: Dimensions | 8.2 x 4.9 x 1.0 in (l x w x d), 20.9 x 12.5 x 2.6 cm |
| Weight | 1.3 lbs (0.59 kg) |
| Antenna Connector Type: | RP-SMA female (Connectorized Sensor only) |