DATASHEET

AirTight® WIPS

World'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 official WLAN are also at risk.

AirTight WIPS provides enterprises with continuous and the most comprehensive protection against current and emerging wireless threats.

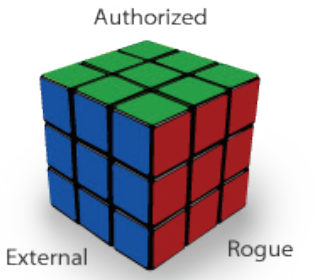
Gartner Rated "Strong Positive"

Consistently rated as the industry's best wireless intrusion prevention system (WIPS), AirTight is the only vendor to receive the highest "Strong Positive" rating from Gartner two years in a row in its annual MarketScope Report on Wireless LAN IPS. AirTight is also the only vendor to be rated at the top in all Gartner MarketScopes for Wireless LAN IPS till date. Ease of use, automatic device classification and accurate threat detection, and reliable threat prevention differentiate AirTight WIPS from other competing WIDS/WIPS solutions.

Unmatched Wireless Protection

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

Automatic device classification:



Using AirTight's patented Marker Packet™ techniques, AirTight WIPS automatically and quickly classifies wireless devices detected in the airspace as Authorized, Rogue and External. As a result it eliminates false alarms and saves security administrators 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 solutions, which rely on slow and inconclusive CAM table lookups and MAC correlation, signatures, or passive wired network sniffing.

Comprehensive Wireless Threat Detection

AirTight WIPS provides the most comprehensive protection from all types of wireless threats, including Rogue APs, Soft APs, Honeypots, Wi-Fi DoS, Ad-hoc networks, Client misassociations, and Mobile hotspots. Security administrators are not required to define complex signatures for threat detection, which is the case with other WIDS/WIPS solutions. AirTight WIPS takes a fundamentally different approach by focusing on the fundamental threat vectors and

Key Features

- Automatically detects, blocks and locates all types of wireless threats
- Patented Marker Packet™ techniques eliminate false alarms in 'on wire' Rogue AP detection
- Secure BYOD policy enforcement
- Off-line sensor mode for fault-tolerant continuous policy enforcement
- 24/7 Spectrum analysis
- Detects and locates 'non Wi-Fi' interference & RF jamming
- Smart Forensics™ for quick resolution of wireless incidents
- Remote troubleshooting including remote "live packet capture"
- Management options include hardware appliance, virtual server, or cloud

Common Criteria

FIPS

DISA UC APL

C-10

DoD Approved

Dual radio, dual band overlay WIPS sensor:

- Certified for Common Criteria EAL2+, FIPS 140-2 and U.S. DoD UC APL
- Cannot be converted to an AP – an industry first

C-60

Maximum Flexibility

Dual radio, dual concurrent device that can operate as:

- Overlay WIPS sensor
- Concurrent 3x3 AP and dedicated sensor – an industry first
- Dual APs with background scanning

C-55

High Performance

Dual radio, dual concurrent 2x2 device that can operate as:

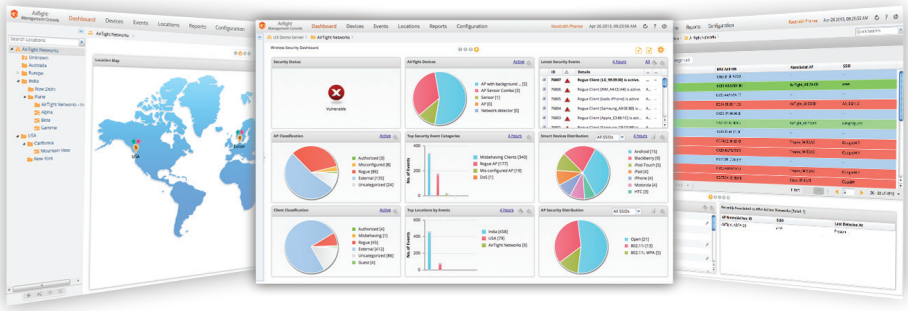
- Overlay WIPS sensor
- Dual APs with background scanning

C-50

Most Affordable

Single radio, dual band device that can operate as:

- Overlay WIPS sensor
- AP with background scanning



vulnerabilities that form the building blocks for all known and emerging Wi-Fi hacking attacks and tools.

Automatic threat prevention:

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 AirTight's accuracy in distinguishing genuine wireless threats from neighboring Wi-Fi devices, AirTight customers effectively and confidently use its prevention capability to block any misuse of Wi-Fi or violation of enterprise security policies.

AirTight WIPS intelligently chooses from various patented over-the-air and on-wire prevention techniques depending on the type of wireless threat, and is capable of simultaneously blocking multiple threats across multiple channels in 2.4 GHz and 5 GHz frequency bands.

Secure BYOD policy enforcement:

In today's Bring Your Own Device (BYOD) culture, the omnipresence of smartphones and tablets poses an immediate threat to enterprise networks. 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" Soft APs and Mobile hotspots can compromise enterprise data security.

AirTight WIPS can automatically fingerprint all types of smartphones and tablets, and enforce a secure BYOD policy by blocking unapproved devices from getting onto the enterprise network.

Accurate location tracking:

AirTight WIPS can pinpoint the physical location of any detected Wi-Fi device or interference source. As a result security administrators can readily track down such devices and take action.

Both real-time locations (for devices currently active) and historic locations (for devices which may have participated in a security incident in the past) are available. AirTight's self-calibrating sensors and sophisticated stochastic models that go beyond simplistic RF triangulation enable accurate location tracking without the need to conduct RF site surveys.

Location-based Policy Management

AirTight WIPS 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.

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.

Simplified Regulatory Compliance

AirTight 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.

AirTight WIPS provides predefined reports that map wireless vulnerabilities to specific data security compliance standards such as PCI DSS, SOX, HIPAA, 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

AirTight WIPS provides 24/7 spectrum analysis capability and alerts 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).

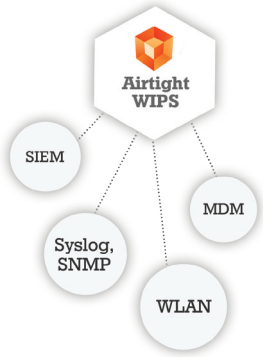
Remote troubleshooting including remote "live packet capture" from a central console allows network administrators to resolve problems at remote sites quickly without sending IT staff to those locations.

Meets Any Security Need

AirTight WIPS can be deployed in different configurations to meet any security need. It can be installed as an overlay security solution on top of your existing WLAN infrastructure or to enforce "No Wi-Fi" policy in highly security sensitive environments where use of Wi-Fi is prohibited. AirTight WIPS is also built into the AirTight Wi-Fi solution. It can be used in an integrated mode in AirTight APs for part time or background scanning or using the innovative software-configurable dual radio AirTight C60 AP, enterprises can concurrently have 3x3:3 Wi-Fi access with dedicated WIPS for 24/7 protection in a single device -- an industry first.

Integration and Interoperability

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



AirTight 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 AirTight's wireless events with virtually any centralized event management tools.

Flexible Delivery Models

A variety of deployment and pricing options cater to enterprises of every industry and size. AirTight WIPS, offered as a part of AirTight Cloud Services™, can be hosted and managed from AirTight's public cloud or private cloud. Or enterprises can choose to host and manage AirTight WIPS from a VMware server or an AirTight appliance installed on-premise. Regardless of the deployment model, AirTight WIPS sensors at any number of geographically distributed sites can be managed centrally from a single HTML5 console.

AirTight® NETWORKS

Comprehensive Cloud-Managed Wi-Fi

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