

Mojo AirTight

World's Top Ranked Wireless Intrusion Prevention System

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

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

Unmatched Wireless Protection

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



Automatic device classification:

Using Mojo's patented Marker Packet™ techniques, Mojo AirTight 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 contrasts the error-prone device classification integrated into most other WLAN solutions, which rely on slow and inconclusive CAM table lookups and MAC correlation, signatures, or passive wired network sniffing.

Comprehensive Wireless Threat

Mojo AirTight provides the most comprehensive protection from all types of wireless threats, including Rogue APs, Soft APs, Honeypots, WiFi 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. Mojo AirTight takes a fundamentally different approach by focusing on the primary threat vectors and vulnerabilities that form the building blocks for all known and emerging WiFi 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 WiFi networks.

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 WiFi' interference & RF jamming
- Smart Forensics™ for quick resolution of wireless incidents
- Remote troubleshooting including remote "live packet capture"
- Management options include virtual server or cloud

Because of Mojo's accuracy in distinguishing genuine wireless threats from neighboring WiFi devices, Mojo customers effectively and confidently use its automatic prevention capability to block any misuse of WiFi or violation of enterprise security policies.

Mojo AirTight intelligently chooses from various patented over-the-air and on-wire

Demo

Want to learn more? Of course you do! An intimate demo is the best way to learn more about Mojo Networks and what we can do to bring you the best wireless security platform for every need.

Evaluation

After we show you what Mojo AirTight is all about, we want you to see it for yourself. Be sure to ask your rep about our no obligation 30-Day trial.

Contact us

877-930-6394
myrep@mojonetworks.com
www.mojonetworks.com

Federal agencies can contact:
federsales@mojonetworks.com



C-60

High Flexibility

Dual radio, dual concurrent device that can operate as:

- Overlay WIPS sensor (802.11n)
- Combination AP/Sensor mode (each dedicated to single radio)
- DISA UC ACL Approved for WIPS



C-75

High Performance

Dual radio, dual concurrent device that can operate as:

- Overlay WIPS sensor (802.11ac)
- Dual 3x3 802.11ac Wave 1 AP with background scanning
- DISA UC ACL Approved for WIPS

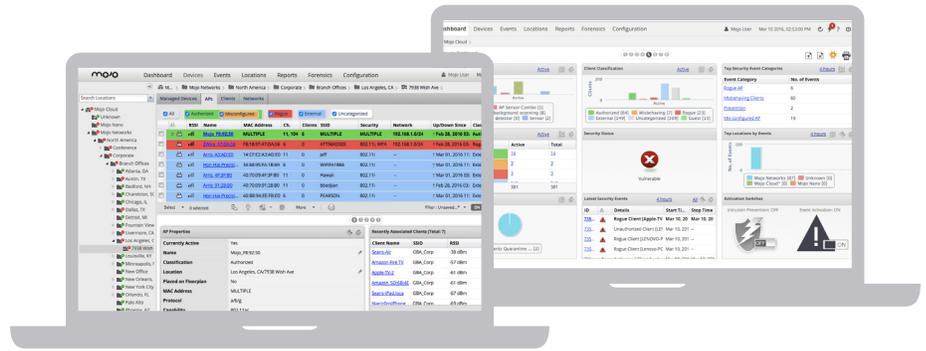


C-75-E

Extended Coverage

Dual radio, dual concurrent device that can operate as:

- Overlay WIPS sensor
- Dual 3x3 802.11ac Wave 1 AP with background scanning
- 6x External Antenna slots
- DISA UC ACL Approved for WIPS



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 WiFi 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. Mojo AirTight 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:

Mojo AirTight can pinpoint the physical location of any detected WiFi 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. Mojo's self-calibrating sensors and sophisticated stochastic models go beyond simplistic RF triangulation to enable accurate location tracking

without the need for RF site surveys.



Location-based Policy Management

Mojo AirTight 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™

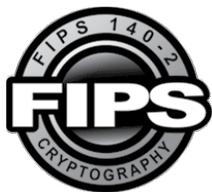
Mojo's Smart Forensics simplifies wireless forensics by filtering out useless data and presenting only relevant and accurate forensics information in an easy to understand and actionable format. Smart Forensics summarizes all relevant information without the need for cumbersome trace collection and packet-level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

Simplified Regulatory Compliance

Mojo 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.

About Mojo Networks, Inc.

Mojo Networks is redefining the modern WiFi platform. Imagine the scalability to set up millions of access points with a few clicks, all from your smartphone. Envision an Internet experience that engages users with your business to drive results. Stay secure on the same WiFi cloud powering major brands and the highest levels of government. And enjoy the cost savings of a cloud-first solution without the pricey markup of proprietary hardware. Welcome to the era of prolific connectivity. Founded in 2003, Mojo Networks (formerly known as AirTight Networks), serves customers in the Fortune 500, Global 2000 and large carriers around the world. Request a free demo of Mojo Cloud Managed WiFi Platform at www.mojonetworks.com



Mojo AirTight provides predefined reports that map wireless vulnerabilities to specific data security compliance standards such as DoD Directive 8100.2, PCI DSS, SOX, HIPAA, and GLBA. Network administrators have the option to schedule reports to be automatically generated and delivered to them by email.

Predictive Wireless Performance

Mojo AirTight 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 WiFi 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

Mojo AirTight 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 WiFi” policy in highly security

sensitive environments where use of WiFi is prohibited. Mojo AirTight is also built into the Mojo WiFi solution. It can be used in an integrated mode in Mojo APs through background scanning.

Integration and Interoperability

With the broadest integration of any WIPS solution, Mojo 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.

Mojo also interoperates with standard enterprise management and reporting platforms including ArcSight, SNMP and Syslog interfaces provide the flexibility to integrate Mojo’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. Mojo AirTight, offered as a part of Mojo cloud managed platform, can be hosted and managed from Mojo’s public or private cloud. Or enterprises can choose to host and manage Mojo AirTight from a VMware server installed on-premise. Regardless of the deployment model, Mojo AirTight sensors at any number of geographically distributed sites can be managed centrally from a single HTML5 console.