Air Marshal

Real-Time Wireless Intrusion Prevention System (WIPS) and Forensics

Securing Your Wireless Airspace

Meraki's cloud managed wireless access points (APs) come equipped with Air Marshal, a built-in wireless intrusion detection and prevention system (WIDS/WIPS) for threat detection and attack remediation. APs configured in Air Marshal mode will scan their environment in real-time and take preemptive action based on intuitive user-defined preferences. Air Marshal triggers alarms and automatically contains malicious rogue APs. Intuitive cloud based management with flexible remediation policies makes Air Marshal ideal for security-conscious distributed networks.

Key Benefits:

- Security policy enforcement at the network edge
- Real-time scanning across channels on 2.4GHz and 5GHz bands
- Attack signatures continually updated from cloud
- Granular detection, attack and remediation policies
- Policy-driven real-time alarms via e-mail and SMS
- Works with all Meraki MR-series access points
- Included with the Meraki Enterprise license at no additional cost

Turnkey Setup

With Meraki's Air Marshal, you can deploy a state-of-the-art real-time scanning system without requiring any additional software, hardware or licenses. By default, all APs will opportunistically monitor their surroundings. With a simple click, an AP is marked as an Air Marshal, converting it to a dedicated WIPS scanner.

Centralized Management

Deploy and manage multiple sites from a single-pane of glass, eliminating the need for large IT teams and on-site truck rolls for any security troubleshooting or WIPS-related events. Air Marshal seamlessly scales to thousands of sites.

Heuristic Threat Classification Engine

Air Marshal comes equipped with an intelligent cloud-based heuristics engine, designed to detect and advise on the most sophisticated attacks. APs will monitor management frames and inspect wireless traffic such as probe requests and disassociation packets to identify deviation from normal behavior. Attack profiles are organized into categories such as rogue SSIDs, AP spoofs, and packet floods, facilitating rapid classification and response by a network administrator.

Real-Time Visibility

Gain unparalleled insights into your wired and wireless infrastructure, identifying wired rogues on your LAN, interfering SSIDs, and malicious clients sending packet floods or attempting to hack your wireless network.

Intuitive Rogue Remediation Policies

Meraki's cloud-based management includes the ability to configure auto-containment policies, facilitating pre-emptive action against rogue devices. For example, Air Marshal can be configured to auto-contain APs spoofing your network's SSID, ensuring your employees and customers are not lured into connecting to a malicious rogue device.

Deep Forensics and Granular Tracking

Built-in forensics tools enable thorough analysis following Air Marshal's initial threat assessments. Live tools including over-the-web packet capture enable administrators to run packet scans across one or more APs, while historic event logs give granular information on client associations, RADIUS authentications, roaming events, and much more - with all historic data stored in perpetuity.

Customizable Security Alarms

Administrators may be immediately notified of potential wireless threats with highly customizable real time alerts. Alerts may be enabled for a variety of threat categories, and are delivered via email or SMS.

Recommended Markets & Use Cases

Retail

- Provide a secure wireless LAN for inventory scanning devices or POS systems
- Ensure PCI compliance and security for the Cardholder Data Environment
- Detect and mitigate attempts to steal information via rogue access points

Financial services, government

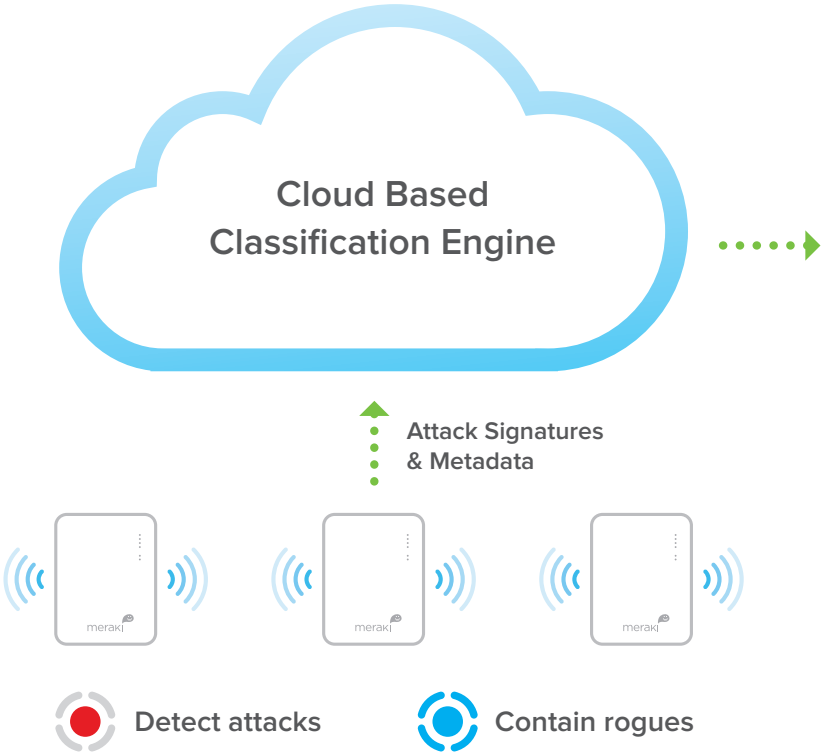
- Detect and contain insecure devices introduced by employees, and malicious rogues introduced by attackers
- Mitigate interfering APs to maximize performance on your wired and wireless network
- Monitor ad-hoc rogues to prevent back-door access to your network

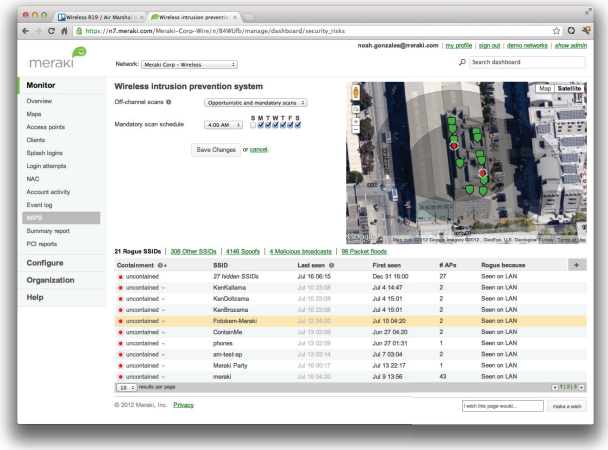
Event Wi-Fi, public spaces, service provider

- Detect and disable copycat SSIDs to provide a secure and consistent user experience
- Protect vendors and guests by maintaining PCI compliance, securing cardholder data

Distributed Enterprise

- Detect and prevent intrusions across thousands of branches, without on-site IT staff





Meraki Dashboard

- Classify and filter attacks
- Shoot down rogue APs
- View forensic data

Meraki, Inc. | 660 Alabama St, San Francsico, CA 94110 | (415) 632-5800 | sales@meraki.com

Specifications

Real-Time Wireless Intrusion Detection and Prevention System (WIDS / WIPS)
Real-time detection of rogue AP and rogue client threat events
Attack classification engine based on threat levels
Policy creation for rogue auto-containment enforcement
Heuristics-driven signatures engine with regular updates
Configurable alarms for administrative visibility
Centrally managed via Meraki's cloud management platform

Attack Signatures & Rogue Reporting
Management frame monitoring
24+ signatures based on packet types and behavior profiles
Attack classification engine based on threat levels
Organization-wide visiblity and reporting for complete WIPS overview
View specifications for each wireless threat: broadcast MAC, channel, first and last seen, manufacturer, SSID, VLAN, and wireless MAC

Security Policies and Alarms
Configure autocontainment based on policy profile matches
SSID keyword/token 'exact' or 'similar' matching profiles
Wired infrastructure rogue AP profiles
E-mail and SMS alarms for rogue events and configuration changes

Packet Capture
Run by AP tags or across entire network
Noise filters for multicast and broadcast traffic
View capture output within dashboard or download as .pcap file for Wireshark analysis
Filter expressions by IP address, port, and protocol type, with operand logic for intelligent searching

Event Log
Search by AP, client device, or time
Per AP: Monitor device boots, AutoRF, dropped frames, stuck beacons, authentication status, administrative state, and WIPS events
Per client: Monitor 802.11 events, WPA associations, 802.1x authentications, DHCP flows and IP address assignment, authentication states, ARP and DNS info
Historic data stored since inception of network

Change Log
Monitor and track time, admin name, network/SSID, and old and updated values per-setting, for all changes across entire network
Track WIPS policy changes and auto-containment and manual containment policy decisions
Historic data stored since inception of network

Access Point Compatibility
Compatible with all MR-series access points

Ordering Information
Included with Meraki Enterprise license
No additional hardware necessary

Meraki, Inc. | 660 Alabama St, San Francsico, CA 94110 | (415) 632-5800 | sales@meraki.com