



AirMagnet Enterprise



AirMagnet Enterprise is a centralized system that proactively protects WiFi networks and users from all types of threats, ensures maximum network performance and uptime and arms staff with the tools to solve problems quickly and remotely. AirMagnet Enterprise does this by going to the true source of WiFi threats and problems – the airspace itself. The solution provides full-time automated analysis of all WiFi traffic, channels, devices, their connection state as well as optional spectrum analysis of non-WiFi devices and sources of interference. This full time view lets you get to the root-cause of any problem instead of just seeing the symptoms, while ensuring full visibility and control over the wireless boundary between your network assets and the outside world. AirMagnet Enterprise takes action to defend the wireless environment by automatically blocking, tracing and mapping any threat in addition to an unmatched suite of event alerting, escalation, remote troubleshooting, forensic analysis, and professional PCI and compliance reporting. The end result is a unified system that keeps WiFi under your control – performing safely and meeting the needs of your users and applications.

24x7 WLAN MONITORING AND PROTECTION

- Continuous monitoring of the entire wireless airspace
- Automatic detection and remediation of all of wireless threats
- Trace, locate, map and capture forensics for any WLAN or RF event
- Automated PCI and regulatory compliance reporting
- 11n expertise and troubleshooting to quickly optimize 11n performance
- Automatic threat classification of access points and stations
- Industry standard performance analysis and remote troubleshooting
- Complete fault-tolerance and unmatched scalability

Complete WiFi Security

AirMagnet Enterprise protects against every wireless threat by combining the industry's most thorough wireless monitoring with leading edge research, analysis and threat remediation.

Full Visibility

Unlike other solutions, AirMagnet Enterprise scans all possible 802.11 channels (including the 200 extended channels), ensuring that there are no blind spots where rogue devices can hide. AirMagnet goes beyond WiFi analysis with optional hardware accelerated spectrum analysis to detect RF jamming attacks, Bluetooth devices and unapproved wireless cameras.

Industry Leading Threat Detection

The AirMagnet Intrusion Research Team constantly investigates the latest hacking techniques, trends and potential vulnerabilities in the industry to keep you a step ahead of evolving threats. Their research drives the AirMagnet AirWISE engine which constantly analyzes all wireless devices and traffic using a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis, policy analysis and anomaly detection, enabling AirMagnet to detect hundreds of specific threats, attacks and vulnerabilities such as rogue devices, spoofed devices, DoS attacks, man-in-the-middle attacks, evil twins, as well as the most recent hacking tools and techniques such as MDK3, Karmetasploit and 11n DoS attacks.

Comprehensive Monitoring

- Full-Time Channel Scanning
- All 200+ WiFi Channels
- Spectrum Analysis
- Detection of Hundreds of Threats

Multi-Dimensional Analysis

- Vulnerability Detection
- Intrusion Detection
- DoS Attack Detection
- Rogue AP Detection
- Authentication and Encryption Audit

Response

- Threat Tracing
- Threat Location
- Wired and Wireless Threat Suppression
- Threat Forensics
- Notification and Escalation

Automated Response and Network Protection

AirMagnet provides a full arsenal of remediation and investigation options that can be triggered by policy to ensure that you don't simply know about a problem, but are also protected.

Threat Tracing

All devices are immediately traced using a suite of wired and wireless tracing methods to quickly and reliably determine if a device is connected to your wired network. The system uses a combination of SNMP, automated switch discovery, hardware correlation and traffic analysis to ensure reliable tracing in any network topology.

Threat Blocking and Suppression

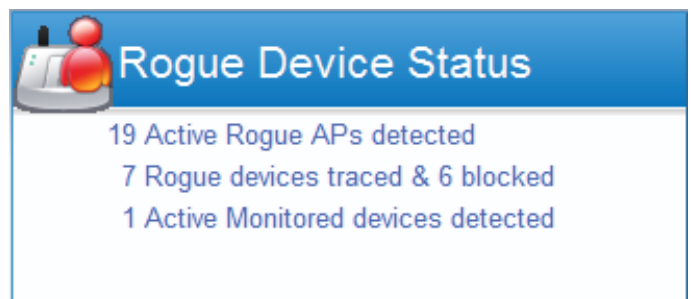
Threats can be manually or automatically remediated with a combination of both wired and wireless threat suppression. Wireless blocking targets a threat at the source and specifically blocks the targeted wireless device from making any wireless connections. Wired blocking automatically closes the wired switch port where a threat has been traced.

Threat Mapping

All threats and devices can be located on a map or floorplan and set to trigger rogue alarms based on the device's location.

Connection History

Staff can easily view all devices an attacker has connected to over time and even see how much data was passed.



Event Forensics

The system can also capture a complete packet or RF forensic record of any network event, allowing staff to investigate any issue in depth even if they didn't see it live. By leveraging its unique intelligent sensors, AirMagnet provides the only solution in the industry to capture forensic information from before, during and after the event.

Notification and Integration

Managers have access to over a dozen notification and escalation mechanisms, making it easy to alert specific staff members of issues or integrate wireless event data into larger enterprise management systems and operations.

Best of Breed Security Architecture

AirMagnet Enterprise offers the only solution in the industry to meet the established standards of a mission critical security application. Only AirMagnet designs fault-tolerance into each component with fail-over boot images in every sensor and automatic server fail-over licenses that come standard with the system. Additionally, AirMagnet Sensors can operate as fully independent IDS/IPS nodes detecting and remediating threats without losing information even if the network connection to the server is lost for days. Additional unique benefits of the AirMagnet architecture include:

Massive Scalability

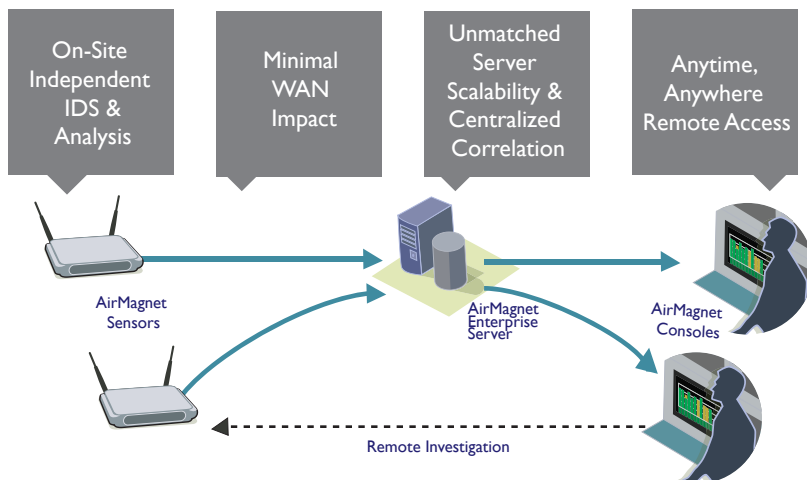
Distributing analysis at the Sensors reduces the need for expensive hardware servers found in solutions that forward information to a central server for analysis.

Minimal Network Impact

Processing at the Sensor also vastly reduces the amount of data each Sensor sends to the Server, thus minimizing bandwidth and ensuring minimal impact to normal network operations.

Designed for Correlation

The AirMagnet Server continuously correlates analysis from all sensors, ensuring that intelligence is always coordinated across the entire enterprise.



Performance Optimization and Troubleshooting

The performance and reliability of the WLAN are directly tied to the return on investment that an organization will derive from wireless. As a result, AirMagnet consistently leads the way in wireless network monitoring to help engineers catch evolving problems before users are impacted, dig to the root-cause of any issue and arm them with the critical tools needed to resolve problems when they happen.

Find Emerging Problems Before Users are Affected

AirMagnet proactively identifies performance issues such as traffic congestion, overloaded devices and channels, device misconfigurations, collisions, roaming problems, QoS issues as well as complications between 11a, 11b, 11g and 11n gear. This allows network staff to quickly get to the root cause of a problem and respond before it spreads and impacts users.

802.11n Intelligence

Much of the massive potential of 802.11n can go unrealized if network managers don't understand how to apply 11n technology in their environment. AirMagnet goes beyond simple 11n support to provide managers with hands-on 11n optimization tools and intelligence focused on real-world performance and network throughput. Tools include live diagnostics of any 11n connection that automatically highlight and explain how performance can be improved. Other tools show how to best configure 11n gear, how to integrate 11n into the current network, and provide guidance on 11n coexistence with legacy 11a/b/g gear, enabling engineers to maximize the power of 11n in their networks.



Interference Analysis

AirMagnet performs a complete interference analysis of the air including interference from WiFi devices, from station collisions as well as optional spectrum analysis of non-WiFi devices such as microwave ovens, cordless phones or legacy wireless equipment.

Active, Remote Troubleshooting

AirMagnet Enterprise lets managers troubleshoot wireless problems remotely to fix problems faster and without costly "truck rolls". Every AirMagnet Sensor contains a full instance of the reknown AirMagnet Analyzer which staff can use to track utilization and bandwidth, packet statistics, view real-time decodes, troubleshoot user connectivity problems and even perform active link tests of any segment of the network.

Simple Policy-Driven Management

As WiFi adoption continues to expand it is increasingly important for network managers to easily cut through the flood of WiFi data and devices to find the point that matters to the network. AirMagnet tackles this challenge with the tools to easily classify new WiFi devices, score and prioritize issues in the network and share timely information with network staff and management systems.

Automatic Device Classification

The AirMagnet device classification engine lets you easily and accurately identify WiFi devices as rogue, neighbors, monitored or approved devices. Classification rules are built using simple straightforward sentences and Boolean rules to classify devices based on their wired traced status, the device vendor, security settings, signal level, association history and variety of other factors. Just as importantly, the system then allows managers to preview the new rule, seeing which devices will be reclassified so that problems can be caught before the policy is pushed live.

Finding the Point That Matters

The AirMagnet Overview Page shows key headline information for all major job roles including the top security issues, performance issues, problem devices and compliance issues. All threats are correlated and scored according to user controlled policies. This allows staff to quickly see prioritize important events and see devices that are at the root of multiple problems.

Focus on Users

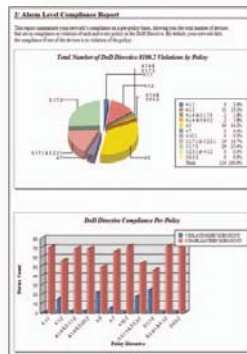
The system also includes a concept of VIP users or devices, allowing staff to prioritize alarms affecting key resources. Similarly, events are scored on their impact to the network, letting staff prioritize issues that are affecting many users versus issues with a lower impact.



Reporting and Compliance

Integrated Reporting

AirMagnet's integrated reporting engine makes it easy to generate professional customized reports for any location or date range. Reports cover all areas of management including RF statistics, device reports, security and performance reports. Reports can be scheduled to be run at regular intervals and delivered to key managers via email.



Compliance Reports

AirMagnet provides detailed compliance reports covering a variety of regulatory standards including Sarbanes-Oxley, HIPAA, PCI, GLBA, DoD 8100.2, ISO 27001, BASEL 2 and CAD3. Reports provide a step-by-step pass/fail assessment of each section of the standard. As a result, IT staff can take the guess work out of compliance audits and complete their work in a fraction of the time.

For More Information

SALES: info@airmagnet.com

PRODUCT INFO: <http://www.airmagnet.com/products/enterprise/>



Corporate Headquarters:
830 E. Arques Ave
Sunnyvale, CA 94085 - United States
Tel: +1 408.400.1200 / Fax: +1 408.744.1250

EMEA Headquarters
6-9 The Square, Stockley Park, Uxbridge
Middlesex, UB11 1FW - United Kingdom
Tel: +44.203.178.7926 / Fax: +44.870.139.5156