



## AirMagnet Enterprise



AirMagnet Enterprise provides a simple, scalable solution that enables any enterprise to ensure the security, performance and compliance of their wireless LANs matches their wired networks. The solution provides continuous, stateful analysis of all wireless channels, devices, traffic and RF spectrum to proactively identify all possible wireless threats, including hundreds that would be missed by the part-time security found in access points, which “bolt on” security as an afterthought. All threats can be automatically traced, located, blocked and saved for forensic analysis. AirMagnet Enterprise also delivers proactive performance analysis, spectrum and interference analysis and includes a suite of remote troubleshooting tools to help keep the WLAN running at peak levels. All events are correlated and scored by severity and impact for simple prioritization, and an integrated reporting engine provides on-demand access to detailed internal and regulatory compliance reports. The end result is an enterprise WLAN with no blind spots and ready for any challenge.

### 24x7 WLAN MONITORING AND PROTECTION

Continuous monitoring of the entire wireless airspace

Automatic detection and remediation of hundreds of wireless threats

Trace, locate and capture forensics for any WLAN or RF event

Industry standard performance analysis and remote troubleshooting

The industry's only on-premises WIDS/WIPS

Complete fault-tolerance and unmatched scalability



## The Only WIDS/WIPS Designed for the Enterprise

AirMagnet Enterprise provides the only WIDS architecture to align with established industry best practices for network security and IDS. Unlike other solutions, AirMagnet performs intrusion detection in real-time and at the traffic source by building a full wireless analysis engine into every sensor. This approach, while unique in wireless security, is precisely the model used in wired network security where IDS is always performed as close to the ingress/egress points as possible, and always on-site. This guarantees that AirMagnet always retains reliable, direct access to all wireless traffic without being dependent on remote systems or public networks. Other key benefits of the AirMagnet architecture include:

### Massive Scalability

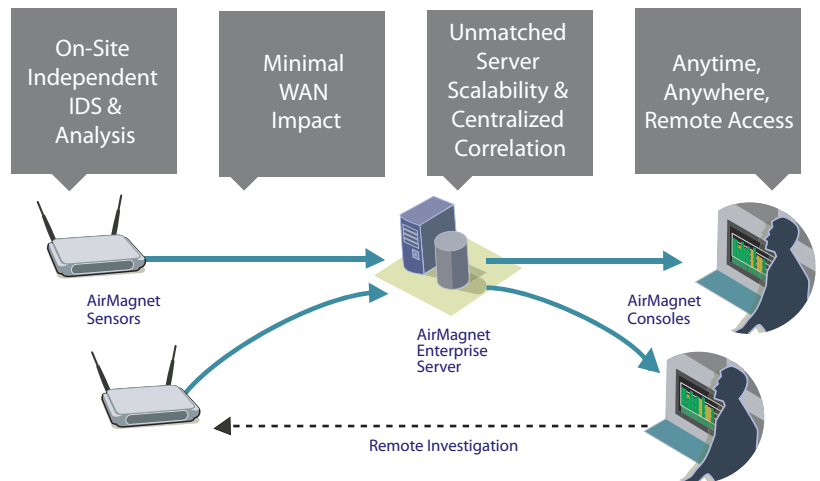
Distributing analysis at the sensors removes the server as a processing choke-point, thus enabling each AirMagnet Server to scale to thousands of sensors.

### 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.

### Continuous Correlation

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



## Complete WLAN Security

AirMagnet Enterprise protects against every wireless threat by combining the industry's most thorough wireless monitoring with the most deepest analysis and threat response.

### Full Visibility

As the only dedicated WIDS solution to scan all 802.11 channels (including the 200 extended 11a channels), AirMagnet ensures that there are no blind spots where rogue devices can hide. In addition to traditional traffic analysis, AirMagnet Enterprise also includes the option to perform spectrum analysis to detect Layer 1 threats such as jamming attacks and potential non-WiFi threats, such as Bluetooth devices or unapproved wireless cameras.

### Multi-Dimensional Threat Detection

The AirMagnet AirWISE engine automatically analyzes all wireless devices and traffic using multiple methods to detect all types of wireless threats. All traffic undergoes a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis, policy analysis and anomaly detection, enabling AirMagnet to detect all types of threats. The solution automatically identifies hundreds of specific threats, attacks and devices such as rogue devices, spoofed devices, DoS attacks, man-in-the-middle attacks, evil twins, penetration tools, fragmentation attacks, reconnaissance and cracking tools and much more.

### Comprehensive Monitoring

- Full-Time Channel Scanning
- All 200+ WiFi Channels
- Spectrum Analysis

### 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
- WEP Shielding
- Threat Forensics
- Notification and Escalation

# Automated Threat Response

Detecting a threat is only the first step in protecting wireless LANs and AirMagnet provides a full arsenal of responses that can be tied to and triggered by enterprise policies.

## Threat Tracing

All threats and devices are automatically traced using both wired and wireless methods to accurately determine if a threat is connected to the wired network, helping to quickly prioritize and differentiate threatening devices.

## Threat Blocking and Suppression

Threats can be manually or automatically remediated with a combination of both wired and wireless threat suppression, keeping all threats fully quarantined without impacting normal network operations.

## Location

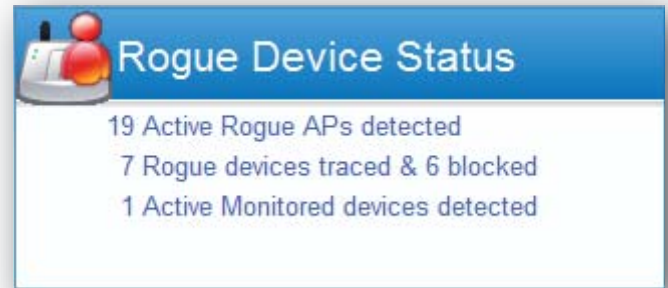
All threats and devices can be located on a map or floorplan and even trigger rogue alarms based on location.

## Event Forensics

The system can capture a complete forensic record for any network or spectrum event, allowing staff to retain hard evidence or save data for detailed post-mortem analysis.

## Connection History

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



## WEP Shielding

AirMagnet Enterprise's new patent-pending WEP Shield feature also includes the option to deploy countermeasures to protect wireless LANs from "WEP cracking" tools designed to recover encryption keys.

## Notification and Integration

Events can also trigger any of a dozen notification and escalation mechanisms, making it easy to alert specific staff members to issues or integrate wireless event data into larger enterprise management systems and operations.

# Performance Analysis and Troubleshooting

How efficiently an enterprise can manage the reliability and performance of the network will have a strong impact on the enterprise's overall return on the investment in wireless. This is why AirMagnet Enterprise provides the same level of insight and analysis for performance issues as it does on security issues.

## Find Emerging Problems Before Users are Affected

AirMagnet tracks all devices, traffic and RF information to proactively identify evolving performance. This includes identifying the causes of traffic congestion, overloaded devices and channels. The solution also identifies a variety of device conflicts, such as 11b devices that may be slowing down faster b/g devices. Staff can see a roaming history for all end-users to identify devices that may be thrashing from AP to AP.

## Interference Analysis

AirMagnet also performs a complete interference analysis that correlates the three unique sources of interference (from WiFi devices, from hidden nodes and from physical environmental noise). The spectrum analysis option also allows users to proactively identify the source of non-WiFi devices that can cause interference such as microwave ovens, cordless phones or legacy wireless equipment.



## Active, Remote Troubleshooting

AirMagnet Enterprise provides network managers with a robust suite of tools to troubleshoot wireless problems remotely, vastly reducing the time to fix and preventing inefficient "truck rolls". Every AirMagnet sensor contains AirMagnet's reknown analyzer capabilities which staff can use to remotely inspect the live behavior of any wireless device or channel. Users can track utilization and bandwidth, track packet statistics and leverage a real-time decode page to inspect any frame. The suite includes a connectivity troubleshooting tool that allows staff to diagnose connection problems between any AP and client. Staff can perform link tests to test various segments of the network, and even test for multipath interference.

# Simple Policy-Driven Management

As with any enterprise-class management system, it is critical for staff to be able to cut through raw data to quickly see the most important devices and events. To this end, AirMagnet Enterprise offers a powerful yet remarkably simple interface to prioritize events based on enterprise policy and the overall impact to the network. This enables staff to immediately triage wireless problems and get the information they need to do their job, quickly and efficiently.

## 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.

## Notification and Escalation

AirMagnet Enterprise delivers targeted, actionable information to network staff and management systems via a comprehensive notification system. Notification methods include SNMP versions 1, 2, and 3, SysLog, EventLog, Email, Pager, Instant Message, SMS, Print, and more. RDEP support allows AirMagnet to seamlessly integrate with other wired IDS systems. All notifications can be configured based on event thresholds and individual alerts can be routed to specific recipients. If problems gets worse, notifications and responses can be automatically escalated based on the severity of the problem.

## Focus on Users

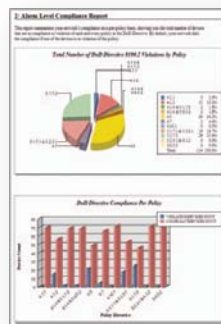
The system incorporates a concept of VIP users or devices, allowing staff to prioritize alarms affecting key resources. Similarly, events are scored on their impact to the network, letting staff prioritize issues that are affecting many users versus issues with a lower impact.



# 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-DSS, GLBA, DoD 8100.2, ISO 27001, BASEL II 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: <http://www.airmagnet.com/company/contact/form/?type=sales>

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

PATENTS: U.S. Patent No. 7,009,957, 7,130,289 and 7,236,460. Additional patents pending



Corporate Headquarters:  
1325 Chesapeake Terrace  
Sunnyvale, CA 94089 - United States  
Tel: +1 408.400.1200 / Fax: +1 408.744.1250



EMEA Headquarters:  
St Mary's Court The Broadway, Amersham  
Buckinghamshire, HP7 0UT - United Kingdom  
Tel: +44 1494 582 023 / Fax: +44 870 139 5156