Datasheet: AirMagnet Enterprise

AirMagnet Enterprise provides a scalable 24x7 WLAN security and performance monitoring solution that mitigates all types of wireless security threats, enforces enterprise policies, proactively detects and pinpoints wireless performance problems and audits the regulatory compliance of all Wi-Fi assets.

- *Full-time packet and RF scanning of the air so costly threats aren't missed*
- *24x7 monitoring for connectivity issues such as channel interference, coverage, malformed packets, De-Authorization attacks to ensure optimal and reliable wireless network availability*
- *Automated Health Check (AHC) proactively monitor and notify any wireless AP performance issues*
- *Power to actively test, diagnose and remediate problems remotely in less time*
- *Dynamic Threat Update (DTU) technology ensures the network is always protected as new threats emerge*
- *802.11ac support with 802.11ac compatible Access Points*

AirMagnet Enterprise

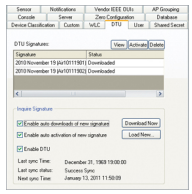
24x7 WIDS/WIPS for proactive enterprise Wi-Fi network security.

AirMagnet Enterprise centralized wireless intrusion detection/prevention system (WIDS/WIPS) defends your wireless environment by automatically detecting, blocking, tracing and locating any threat on all Wi-Fi channels. It contains an unmatched suite of event alerting, escalation, remote troubleshooting, forensic analysis, network health check, and professional PCI and other policy compliance reporting. The end result is a unified system that scans your environment 100% of the time to ensure your WLAN is performing safely and securely and is meeting the needs of your users and applications.

In addition to rich security features, AirMagnet Enterprise constantly monitors the health and performance of the WLAN and RF environment to proactively detect evolving problems that can lead to network interruption. The system detects issues, gives users remediation advice and includes active remote tools to troubleshoot the issue. This allows staff to avoid network downtime and vastly reduces the time-to-fix for any outage, leading to greater uptime, better performance and overall higher end-user satisfaction.

AirMagnet Enterprise — Complete Cellular and Wi-Fi Security

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



Dynamic threat update

Full Visibility

Unlike Access Poins (AP), AirMagnet Enterprise scans all possible 802.11 channels (including the 200 extended channels), and cellular spectrum channels ensuring there are no blind spots where rogue or interfering devices may be hiding. AirMagnet Enterprise also provides cellular spectrum analysis that detects and classifies RF jamming attacks, Bluetooth devices and many other non 802.11 transmitter types, such as wireless cameras and cell phones.

Industry Leading Threat Detection

The AirMagnet Security Research Team constantly investigates the latest hacking techniques, trends and potential vulnerabilities to keep organizations ahead of evolving threats. Our Dynamic Threat Update (DTU)technology speeds the creation, automation and immediate deployment of new threat signatures New DTU signatures can be deployed immediately with no impact to system operation, providing a unique framework for maintaining the most up-to-date WLAN security posture for over 230 threats.

The AME AirWISE® engine constantly analyzes all wireless devices and traffic using a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis and anomaly detection.

Automated Response and Network Protection

AirMagnet Enterprise provides a full arsenal of remediation and investigation options that can be triggered by policy to ensure that WLAN problems are quickly and accurately detected and that appropriate automated protection mechanisms are activated.

Threat Tracing, Blocking/Suppression and Mapping

All devices are traced using a suite of wired and wireless tracing methods to quickly and reliably determine if a device is connected to the network. The system uses a newly enhanced set of sophisticated techniques, including use of SNMP, automated switch discovery, and hardware and traffic analysis, to ensure accurate, fast tracing in any network topology.

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.

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

Event Forensics

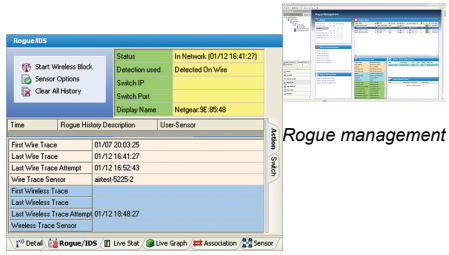
AirMagnet Enterprise captures a complete packet or RF forensic record of any network event, allowing appropriate staff to investigate the issue in depth, at any time.

Notification and Integration

Managers have access to more than 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.

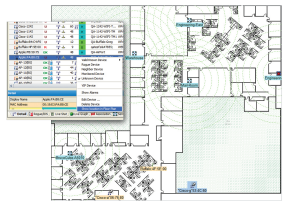
Flexible Sensor Architecture

The SmartEdge Sensor, Series 4, supports a tri-radio design, including two 802.11n 3x3 MIMO Wi-Fi radios and dedicated Wi-Fi or cellular spectrum analysis. This design enables a wireless connection from the sensor, eliminating the need for costly Ethernet cabling, or simultaneous security monitoring and performance testing.



Rogue management

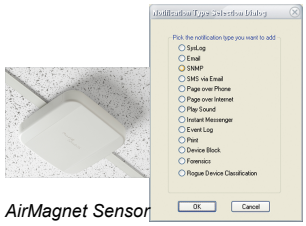
Rogue device detected and traced



Locate rogue device on a floor map

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. It is the only system to build 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 Enterprise 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 Enterprise architecture include:



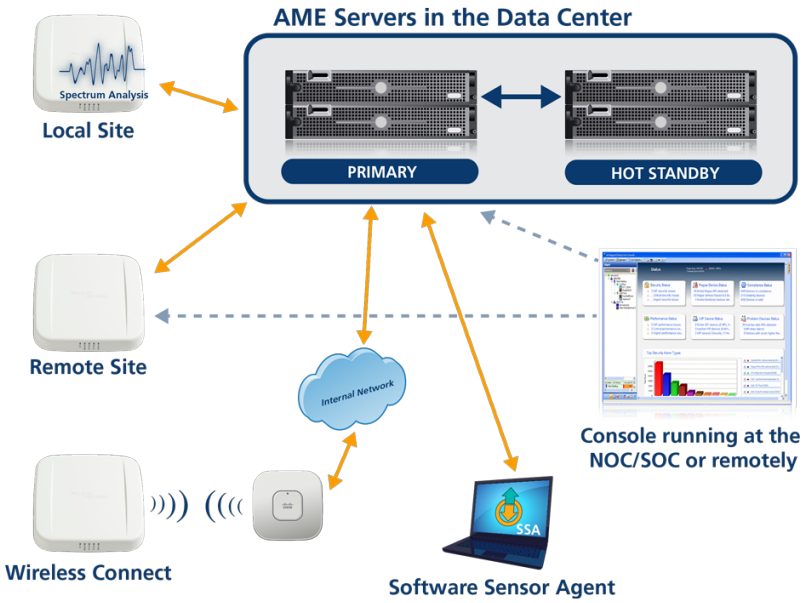
AirMagnet Sensor

Notification options

Massive Scalability
With intelligent sensors that locally analyze Wi-Fi, cellular and RF conditions, more than 1,000 sensors can be supported through a single centralized server in the data center, requiring minimal network bandwidth.

Highest System Resilience
Processing at the sensor level means that each sensor continues to enforce the security policy even if connection to the server is lost for more than 24 hours. Hot standby server software (included) enables fully redundant datacenter operations for maximum wireless security protection.

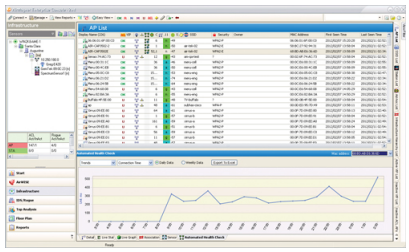
Designed for Correlation
The AirMagnet Enterprise server continuously correlates analysis from all sensors, ensuring that intelligence is always coordinated across the entire enterprise.



AirMagnet Enterprise System

Performance Optimization and Troubleshooting

Performance and reliability of a WLAN are often directly tied to the value a wireless network delivers to an organization. AirMagnet Enterprise technology has consistently been at the forefront of innovation, developing into wireless network monitoring solutions that help IT professionals identify and mitigate WLAN problems before they impact users. By digging into the root-cause of any issue and arming users with the critical tools needed to resolve problems when they happen, AirMagnet Enterprise ensures wireless networks can reliably support business critical applications.



Automated Health Check performance test results

AirMagnet Enterprise provides a 24x7 spectrum security solution empowering customers to enforce unified no wireless (cellular and Wi-Fi) zones. It offers detection, monitoring, and remediation of spectrum activity in a broad frequency range that includes 3G, 4G LTE, and CDMA. Activity by cellular devices like cell phones and jammers is tracked and reported. Further AirMagnet Enterprise monitors and reports on 4 types of cellular security violation events:

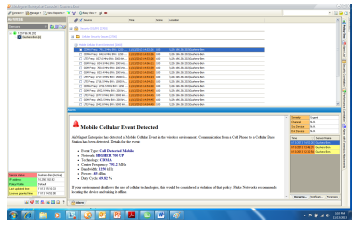
Cellular Location monitor

- Mobile cellular events, e.g., calls made from a specific cellular network
- Cellular interference events, e.g., cellular jammers
- Non-cellular energy events, e.g., events taking place outside of the country's allocated cellular bandwidth
- Base station cellular events, e.g., base station beacons
- Location of cellular event
- Provide Cellular Operator information

For further analysis, users can access sensor's built-in cellular spectrum analyzer. This avoids costly truck-rolls and reduce time to resolution.

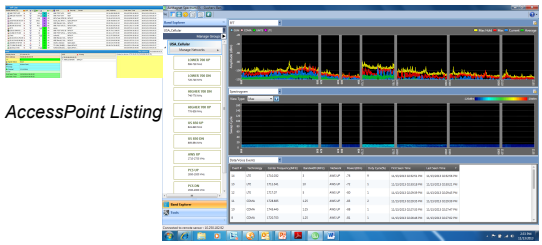
Find Outages and Emerging Problems Before Users are Affected
Powered by the Automated Health Check (AHC), AirMagnet Enterprise sensors and Software Sensor Agents actively test and verify complete WLAN connectivity from the wireless link all the way through to application servers or the Internet, automatically detecting critical outages or network degradation while pinpointing the exact source of trouble. Sensors running AHC tests provide a true client perspective, as they fully authenticate to the network and proactively probe for problems, which can be related to WLAN issues or other network resources. This provides network staff with immediate and specific information on the root cause, so they can respond often before users are impacted.

Comprehensive Wireless Analysis
AirMagnet Enterprise identifies and generates AirWISE alarms for performance issues such as traffic congestion, overloaded devices and channels, device misconfigurations, collisions, roaming problems, QoS issues, as well as complications between 802.11a/b/g/n devices. Tools for 802.11n optimization enable network staff to ensure that their WLAN investment is delivering the expected real world performance to users.



AirWISE alarm with cellular security events

Extensive RF Interference Analysis
AirMagnet Enterprise is the only WLAN monitoring system supporting dedicated spectrum analysis hardware in the sensor for the most accurate and complete RF interference detection and remote real-time analysis. The environment is scanned 100 percent of the time over both 2.4 GHz and 5 GHz Wi-Fi bands, and specifically classifies interference sources like video cameras, cordless phones and microwave ovens which can seriously impact the performance of the WLAN.



AccessPoint Listing

Cellular spectrum analyzer with security events

Real-time Remote Troubleshooting
AirMagnet Enterprise allows IT professionals to troubleshoot wireless problems remotely to fix problems faster and without costly "truck rolls". AirMagnet Enterprise sensors contain a real-time analysis interface based on AirMagnet Wi-Fi Analyzer and Spectrum XT, enabling staff to track utilization and bandwidth, view real-time decodes, troubleshoot user connectivity and RF interference problems without leaving their desks.

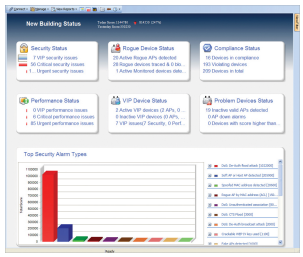
802.11ac Analysis
AirMagnet Enterprise provides 802.11ac analysis capabilities utilizing existing SmartEdge Series 4 sensors. AirMagnet Enterprise integrates with 802.11ac capable AccessPoints to provide:

- Detection of 802.11ac AccessPoints
- 802.11ac Frame Analysis
- Rogue 802.11ac device detection and blocking

NETSCOUT

Simple Policy-Driven Management

As Wi-Fi adoption continues to expand, it is increasingly important for network managers and wireless professionals to leverage tools that allow them to easily cut through the flood of Wi-Fi data and devices, revealing the information that matters most. AirMagnet Enterprise does this with tools that easily classify new Wi-Fi devices, score and prioritize issues in the network and share timely information with network staff and management systems.



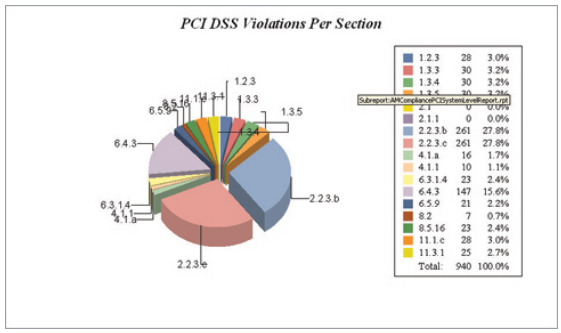
Dashboard view of top WLAN issues

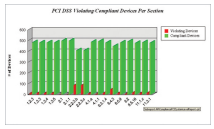
Automatic Device Classification

The AirMagnet Enterprise device classification engine allows a user to easily and accurately identify Wi-Fi 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. The system also allows managers to preview new rules so they can see what devices will be reclassified and catch any problems before the policy is pushed live.

Finding the Information that Matters

The AirMagnet Enterprise dashboard 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 and prioritize important events, and see devices that are at the root of multiple problems.





PCI compliance summary

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 lower impact issues.

Reporting and Compliance

Compliance Reports

AirMagnet Enterprise outputs detailed compliance reports covering a variety of regulatory standards including Sarbanes-Oxley, HIPAA, PCI, DSS 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 guesswork out of compliance audits and complete work in a fraction of the time.

PCI 3.0 report

Integrated Reporting

AirMagnet Enterprise'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 cellular security events, RF statistics, device reports, security and performance reports. Reports can be scheduled to run at regular intervals and delivered to key managers by email.

PCI 3.0 Compliance

AirMagnet Enterprise PCI 3.0 Compliant Reports automatically identifies and provides actionable results and point out the areas to focus on in order to become compliant to the PCI 3.0 standards.

NETSCOUT

Ordering Information	
Model	**Description**
AM/A5505	Enterprise console and server software, unlimited sensors
AM/A5115	Enterprise server license for 802.11n features, unlimited sensors
AM/A5106	Enterprise server license for spectrum analysis features, unlimited sensors
AM/A5311G	AirMagnet Enterprise Server License for Software Sensor Agent (100)
AM/A5630G	AirMagnet Enterprise Server License for AHC
SENSOR4-R1S1W1-E	AirMagnet Sensor, cellular spectrum, 4th Gen, 1 X 11n Radio, External Ant.
SENSOR4-R1S0-I	AirMagnet Sensor, 4th Gen, 1 X 11n Radio, Internal Ant.
SENSOR4-R1S1-I	AirMagnet Spectrum Sensor, 4th Gen, 1 X 11n Radio, Internal Ant.
SENSOR4-R2S0-I	AirMagnet Sensor, 4th Gen, 2 X 11n Radio, Internal Ant.
SENSOR4-R2S1-I	AirMagnet Spectrum, 4th Gen, 2 X 11n Radio, Internal Ant.
SENSOR4-R1S0-E	AirMagnet Sensor, 4th Gen, 1 X 11n Radio, External Ant.
SENSOR4-R1S1-E	AirMagnet Spectrum, 4th Gen, 1 X 11n Radio, External Ant.
SENSOR4-R2S0-E	AirMagnet Sensor, 4th Gen, 2 X 11n Radio, External Ant.
SENSOR4-R2S1-E	AirMagnet Spectrum, 4th Gen, 2 X 11n Radio, External Ant.
AM/A5032	Power Injector for AirMagnet Sensors
CABLEKIT-SENSOR4	Console Cable Kit for Sensor 4 Series
Gold Support (various)	Gold support services for each sensor model, 1 yr and 3 yr

Note: The AirMagnet Enterprise system requires a server/database. Users can purchase a server from NetScout or use their own server that meets the minimum requirements below.

Server Minimum Requirements	
Operating system	Microsoft Windows Server 2008 / VMware ESX
Processor	Intel Xeon E3 Series CPU
Memory	8 GB / 1600 MHz or faster
HD Size	450 GB / 15,000 RPM SAS

Note: Additional requirements may apply when sizing the server to support specific system configurations. Visit ***www.enterprise.netscout.com*** for further information.

Certifications
Common Criteria Evaluation Assurance Level 2
U.S. FIPS 140-2 Certification (does not apply to SENSOR4-R1S1W-E)