FLUKE networks

AirMagnet Enterprise

AirMagnet Enterprise provides a simple, scalable WLAN security monitoring solution that enables any organization to proactively mitigate all types of wireless security threats, enforce enterprise policies, prevent wireless performance problems and audit the regulatory compliance of all their Wi-Fi assets and users worldwide. It offers 24x7 WLAN monitoring and protection, delivering:

- *Full-time scanning of the air so costly threats aren't missed*
- *Power to diagnose and remediate problems remotely in less time*
- *Dynamic update technology ensures the network is always protected as new threats emerge*
- *Easy integration with existing infrastructure and practices reducing burden on staff*

AirMagnet Enterprise offers complete visibility and control over the wireless airspace, enabling any enterprise to reliably deliver the same standards of security performance and compliance for their wireless networks as they expect from their wired networks.

AirMagnet Enterprise – Complete 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.

Full Visibility

AirMagnet Enterprise scans all possible 802.11 channels (including the 200 extended channels), ensuring there are no blind spots where rogue devices may be hiding. AirMagnet Enterprise goes beyond Wi-Fi analysis with optional spectrum analysis that detects and classifies RF jamming attacks, Bluetooth devices and many other non-802.11 transmitter types, such as unapproved wireless cameras.

Industry Leading Threat Detection

The AirMagnet Intrusion Research Team constantly investigates the latest hacking techniques, trends and potential vulnerabilities to keep organizations ahead of evolving threats. New Dynamic Threat Update technology speeds the creation, automation and immediate deployment of new threat signatures through the AirMagnet AirWISE® engine. As soon as any new threat definition is ready, it can be deployed with no impact to system operation, providing a unique framework for maintaining the most up-to-date WLAN security posture for the enterprise.

The 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, enabling detection of 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 802.11n DoS attacks.

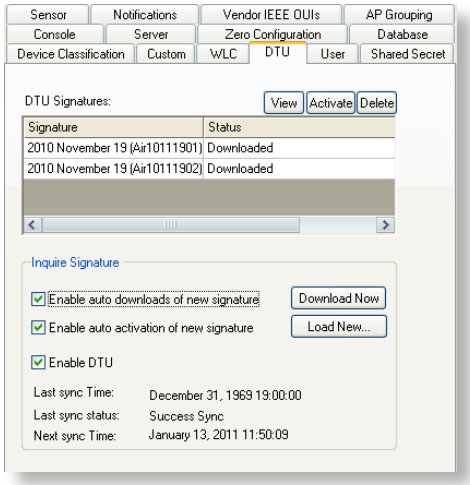

Figure 1: *Dynamic threat update*

24x7 WLAN Security and Performance Monitoring

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

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 wired 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.

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 see how much data was passed.

Event Forensics

AirMagnet Enterprise can capture a complete packet or RF forensic record of any network event, allowing appropriate staff to investigate the issue issue in depth, at any time. By leveraging its unique intelligent sensors, AirMagnet Enterprise provides the only solution in the industry to automatically capture forensic information from before, during and after the event.

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.

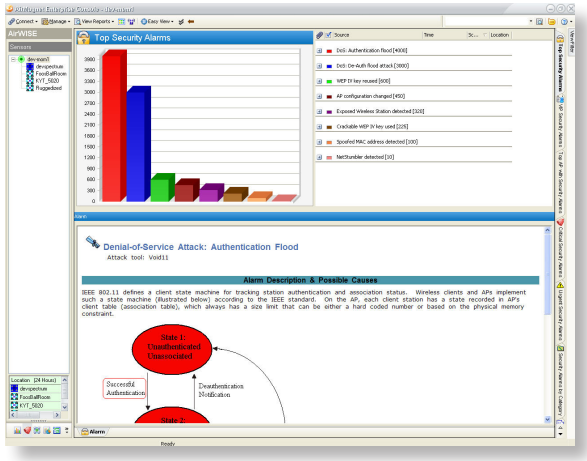

Figure 2: *DoS attack detected*

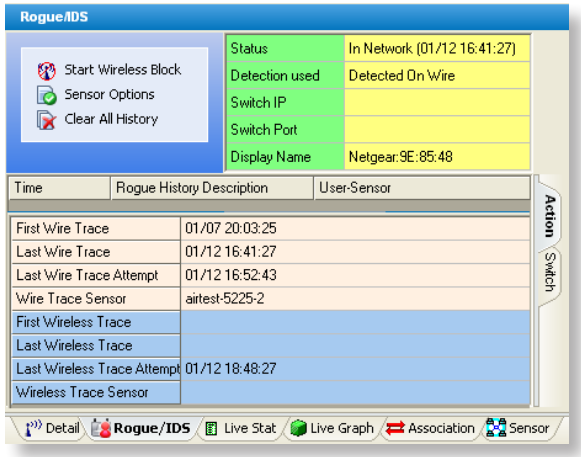

Figure 3: *Rogue device detected and traced*

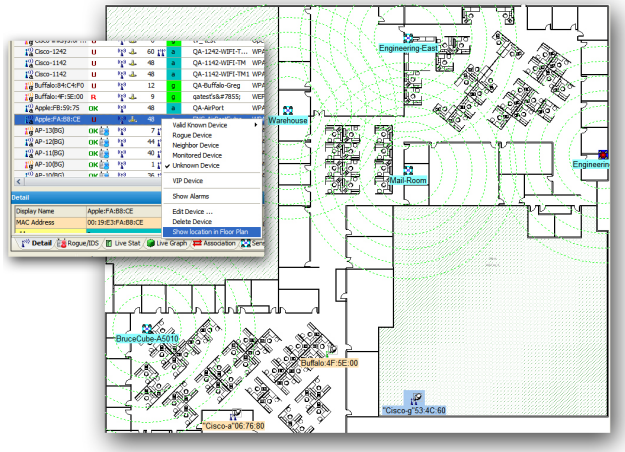

Figure 4: *Locate rogue device on a floor map*

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:

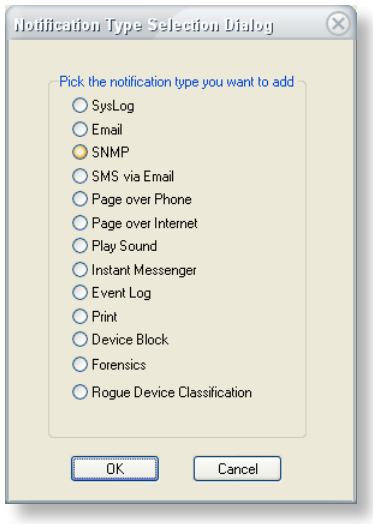

Figure 5: *Notification options*

Massive Scalability

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

Figure 6: *AirMagnet Sensor*

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.

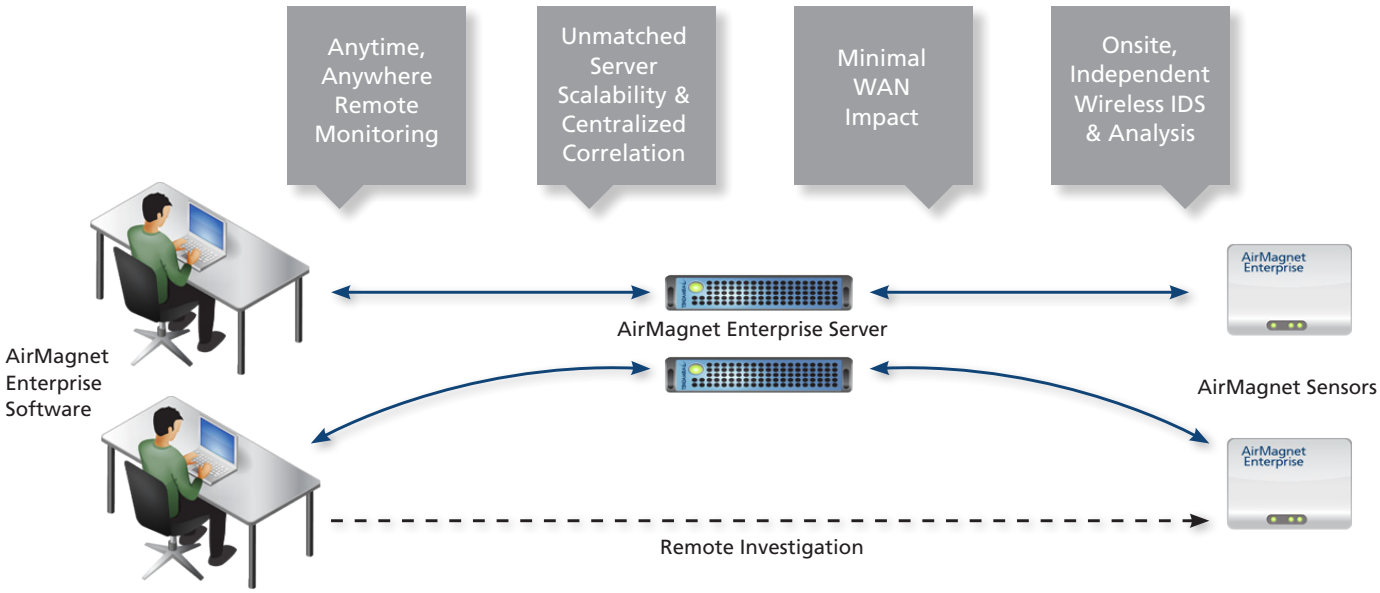

Figure 7: *AirMagnet Enterprise system*

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 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.

Find Emerging Problems Before Users are Affected

AirMagnet Enterprise proactively identifies performance issues such as traffic congestion, overloaded devices and channels, device mis-configurations, collisions, roaming problems, QoS issues, as well as complications between 802.11a/b/g/n devices. 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 802.11n technology in their environment. AirMagnet Enterprise goes beyond simple 802.11n support to provide managers with hands-on 802.11n optimization tools and intelligence focused on real-world performance and network throughput. Tools include live diagnostics of any 802.11n connection that automatically highlights and explains how performance can be improved.

Interference Analysis

AirMagnet Enterprise performs a complete interference analysis of the air. This includes co-channel interference from Wi-Fi devices, as well as optional spectrum analysis of non-Wi-Fi devices, such as microwave ovens, cordless phones or legacy wireless equipment.

Active, 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 WiFi Analyzer, enabling staff to track utilization and bandwidth, packet statistics, view real-time decodes, troubleshoot user connectivity problems and perform connnectivity tests.

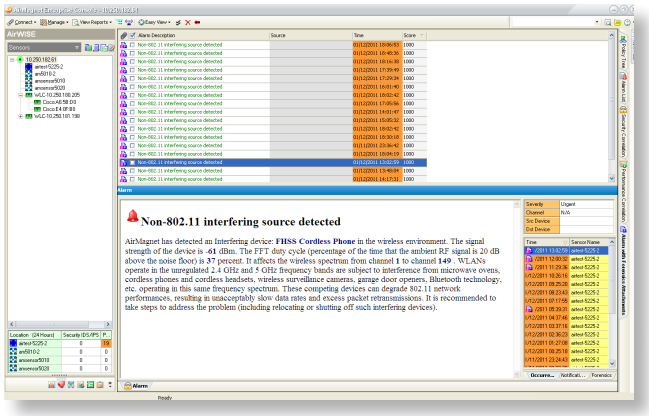

Figure 8: *AirWISE alarm with details of source of interference*

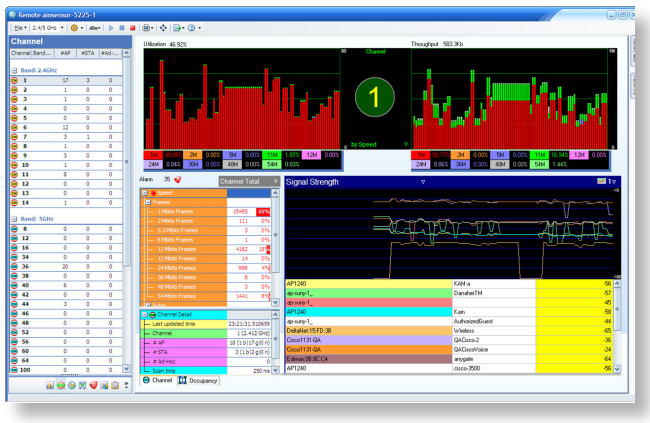

Figure 9: *AirMagnet WiFi Analyzer*

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.

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.

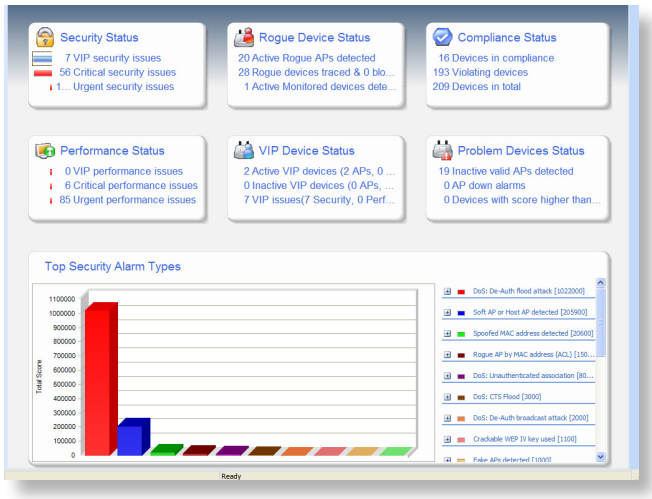

Figure 10: *Dashboard view of top WLAN issues*

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.

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, 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.

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

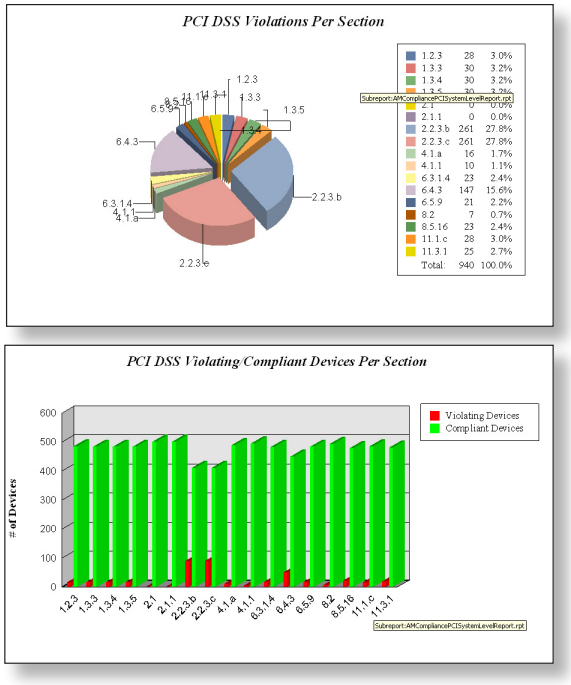

Figure 11: *Interference*

Ordering Information

Model	Description
A5225	Sensor with internal antenna, 802.11n, dedicated spectrum analysis radio
A5205	Sensor with external antenna, 802.11n, dedicated spectrum analysis radio
A5031	Metal sensor mounting bracket with security lock option
A5231	Plastic sensor mounting bracket
A5505	Enterprise console and server software, unlimited sensors
A5115	Enterprise server license for 802.11n features, unlimited sensors
A5106	Enterprise server license for spectrum analysis features, unlimited sensors

Note: *The AirMagnet Enterprise system requires a server/database. Users can purchase a server from Fluke Networks 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 X3400 Series CPU
Memory	8 GB / 1333 MHz or faster
HD Size	146 GB / 10,000 RPM SAS

Note: *Additional requirements may apply when sizing the server to support specific system configurations. Contact Fluke Networks for more information.*

Certifications

Common Criteria Evaluation Assurance Level 2
U.S. FIPS 140-2 Certification

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 2/2011 3988735B D-ENG-N