AirMagnet Enterprise

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

- Full-time packet and RF scanning of the air so costly threats aren’t missed
- Power to actively test, diagnose and remediate problems remotely in less time
- Dynamic update technology ensures the network is always protected as new threats emerge
- Flexible deployment options with new Software Sensor Agents to meet any budget
- Easy integration with existing infrastructure and practices reducing burden on staff

AirMagnet Enterprise offers complete visibility and control over the wireless airspace, enabling any organization to maximize efficiency of IT staff to reliably deliver the safest and highest availability Wi-Fi access to mission critical users, while meeting all compliance requirements.

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 such as rogue devices, spoofed devices, DoS attacks, man-in-the-middle attacks, evil twins, as well as the most recent hacking tools and vulnerabilities such as WPS brute force attack, Karmetasploit and 802.11n fuzzing attacks.

Figure 1: Dynamic threat update
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.

Event Forensics

AirMagnet Enterprise can capture 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

Using the new Software Sensor Agent, security monitoring deployments for WIPS can be achieved on any budget and with increased flexibility. Installed on existing Windows PCs, the Software Sensor Agent provides essential protection for requirements such as PCI compliance without the need for costly installation or additional cabling and switch infrastructure. Hardware sensors can be combined with Software Sensor Agents to create the optimal combination of protection and analysis capabilities.
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:

**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.

**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.
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 Outages and Emerging Problems Before Users are Affected
Powered by the new Automated Health Check (AHC), AirMagnet Enterprise sensors and Software Sensor Agents can now 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.

Unmatched 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% of the time over both 2.4 GHz and 5 GHz Wi-Fi bands, and specifically classifies inference sources like video cameras, cordless phones and microwave ovens which can seriously impact the performance of the WLAN.

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.
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.

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.

Ordering Information

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5225</td>
<td>Sensor with internal antenna, 802.11n, dedicated spectrum analysis radio</td>
</tr>
<tr>
<td>A5220</td>
<td>Sensor with external antenna, 802.11n, dedicated spectrum analysis radio</td>
</tr>
<tr>
<td>A5031</td>
<td>Metal sensor mounting bracket with security lock option</td>
</tr>
<tr>
<td>A5231</td>
<td>Plastic sensor mounting bracket</td>
</tr>
<tr>
<td>A5505</td>
<td>Enterprise console and server software, unlimited sensors</td>
</tr>
<tr>
<td>A5115</td>
<td>Enterprise server license for 802.11n features, unlimited sensors</td>
</tr>
<tr>
<td>A5106</td>
<td>Enterprise server license for spectrum analysis features, unlimited sensors</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Microsoft Windows Server 2008 / VMware ESX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon E3 Series CPU</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB / 1333 MHz or faster</td>
</tr>
<tr>
<td>HD Size</td>
<td>146 GB / 10,000 RPM SAS</td>
</tr>
</tbody>
</table>


Certifications

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