AirMagnet Enterprise

The most comprehensive 24x7 wireless intrusion detection system (WIDS) / wireless intrusion prevention system (WIPS) WiFi Network and Cellular security solution.

AirMagnet Enterprise is a full-time wireless intrusion prevention system (WIPS), wireless intrusion detection system (WIDS) and wireless network (WLAN) security monitoring system that provides dedicated monitoring of the airspace to enable the security, performance and compliance of WLANs. AirMagnet Enterprise is used by organizations for the most complete WIPS and WIDS, remote network troubleshooting, enforcing no-wireless zones, and proving compliance.

- Dedicated wireless intrusion prevention system (WIPS) and wireless intrusion detection system (WIDS) with integrated spectrum and 802.11ac analysis for complete WLAN security and visibility
- SmartEdge, Series 4 Sensors Tri-Radio, 802.11n 2x2 and 3x3 MIMO plus dedicated Cellular Spectrum radio
- Dynamic Threat Update technology for immediate wireless intrusion prevention of new threats
- Automated PCI 3 and regulatory compliance reporting
- Automated Health Check pinpoints and diagnoses problems impacting WiFI connectivity, performance, and WLAN network security
- Forensic analysis and event triangulation for rapid response

OVERVIEW

AirMagnet Enterprise – Complete Cellular and Wireless Network Security

AirMagnet Enterprise protects against every wireless network (WLAN) security threat by combining the industry's most thorough wireless intrusion detection system (WIDS) and wireless network security monitoring with leading research, analysis and security threat remediation.

Full Network Visibility

AirMagnet Enterprise scans all possible 802.11 wireless 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 goes beyond WiFi network analysis with optional WiFi and cellular spectrum analysis that detects and classifies RF jamming attacks, Bluetooth devices and many other non-802.11 transmitter types, such as unapproved wireless cameras and cell phones.

Industry Leading Wireless Intrusion Prevention System (WIPS) and Wireless Intrusion Detection System (WIDS)

The AirMagnet Intrusion Research Team constantly investigates the latest hacking techniques, trends and potential wireless network security vulnerabilities to keep organizations ahead of evolving wireless network security threats.

Dynamic Threat Update technology speeds the creation, automation and immediate deployment of new security threat signatures.

As soon as any new wireless network security 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 wireless network security posture for the organizations.

Provides significant security protection over existing AP infrastructure

Security is not the APs primary focus, thus APs typically miss many security threats. AirMagnet Enterprise dedicated WIDS/WIPS solution provides peace of mind and assurance that your critical wireless network is protected full time, not part of the time like with APs.

- Part time scanning by built-in security solutions miss attacks

- AP is likely too slow and resource constrained to do the job right
- AP's Integrated WIPS cover far fewer threats (usually <20% of threats) and require slow firmware upgrade to respond to new threats
- AP hardware can be limited by regulatory and configuration issues (cannot scan 200+ 5 GHz extended channels)
- If the AP is attacked, who monitors then?

Find Outages and Emerging Problems Before Users are Affected

AirMagnet Enterprise Automated Health Check (AHC) technology actively tests and verifies complete wireless LAN 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 to:

- Fully authenticate to the network and proactively probe for problem related to WLAN security issues or other network resources.
- Provides network staff with immediate and specific information on the root cause, so they can respond often before users are impacted.
- Perform Captive Portal to verify guess wireless network