
**Enterprise Class Wireless Intrusion
Prevention Systems: Requirements and
Figure of Merit**

Enterprise Class Wireless Intrusion Prevention Systems: Requirements and Figure of Merit

This paper describes the essential attributes that define the Figure of Merit (FOM) of a Wireless Intrusion Prevention System (WIPS). The FOM can be used to quantify and compare the performance and functionality of a WIPS and distinguish enterprise class solutions from checkbox systems.

Wireless technology is growing in popularity. Businesses are not only migrating to wireless networking, they are steadily integrating wireless technology and associated components into their wired infrastructure. The demand for wireless access to Local Area Networks (LANs) is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and a desire by users for continual connections to the network without having to “plug in.”

Like most innovative technologies, using Wireless LANs (WLANs) poses both opportunities and risks. The wireless explosion has given momentum to a new generation of hackers who specialize in inventing and deploying innovative methods of hijacking wireless communications, and in using the wireless network to breach the wired infrastructure. In fact, hackers have never had it so easy. The reader is referred to the AirDefense white paper “*Wireless LANs: Is My Enterprise at Risk?*” for more details on the risks associated with wireless networks.

The ease with which WLANs can be compromised has fueled the need for WIPS. WIPS monitors airwaves, looking for attack signatures, protocol/policy violations and behavioral anomalies. It reports these events and could also take corrective measures, if required. AirDefense pioneered WIPS and its solutions are being used to monitor and protect tens of thousands of networks and over one million devices around the globe in 700+ blue chip enterprises, healthcare organizations and government agencies. This white paper outlines the essential attributes that define a true WIPS.

Figure of Merit

The FOM of a WIPS defines the broad functional and architectural requirements a system must have and establishes a benchmark for comparison of different systems.

Figure 1 shows the seven fundamental components of the WIPS FOM.

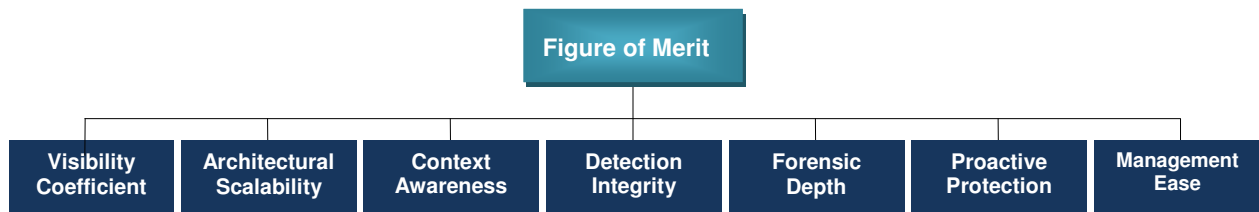


Figure 1: FOM attributes for a WIPS

Visibility Coefficient

Visibility is a fundamental requirement for WIPS. To defend a wireless network successfully the WIPS must be able to see and analyze everything. There are four dimensions that comprise the visibility coefficient:

1. **Space** - Wireless networks do not have well defined physical boundaries. RF signals propagate beyond the restricted confines of a building. Hackers can attack your network from a parking lot or worse still at an open hotspot. WIPS must protect wireless devices not only within the enterprise but also at hotspots and homes where the mobile workforce has significant and more vulnerable wireless usage.
2. **Time** - The WIPS must monitor and protect the user and the network 24x7. Part-time scanning solutions or occasional handheld sniffers are ineffective against the rising threat of transient wireless attacks.
3. **Frequency** - The WIPS must be able to monitor all wireless channels intelligently for suspicious traffic. With 34 channels in the US, a system that can get locked down on one channel or randomly scans a few channels will have significantly low frequency visibility.
4. **Protocol** - The final visibility dimension is the ability to decode all traffic. An 802.11b handheld sniffer will not decode higher rate 802.11g traffic. Newer wireless standards are constantly evolving. In addition, chipset vendors add proprietary extensions for higher throughput and extended range. Attacks with frames using these protocols can be completely below the radar for sensors that do not support them.

Architectural Scalability

Architectural scalability allows the WIPS to scale from a single device to thousands of heterogeneous devices of an enterprise scattered across the globe without sacrificing central management and control. Scalability stems from two attributes:

1. **Device Concurrency** - The number of devices that a WIPS can concurrently monitor and protect is fundamental to architectural scalability.
2. **Sensor Bandwidth** - Bandwidth efficiency of the communication protocol between the WIPS sensor and the server allows the system to scale across wide area networks to sites with limited internet connectivity.

3. **Modularity** - The WIPS architecture should be modular such that it can seamlessly be migrated to different wireless infrastructure platforms.

Context Awareness

Context awareness is the ability of the WIPS to provide relevant alerts by adapting and learning over time. Context awareness stems from two attributes:

1. **Historical Filtering** - The WIPS should have the ability to store and analyze past events and device behavior for historically relevant alarms.
2. **Real-Time Network Knowledge** - The WIPS must be capable of detecting network topology in real-time so that it can focus its detection resources on devices that are on the network as opposed to firing irrelevant alarms about neighboring devices that are not posing any real threat.

Detection Integrity

Detection integrity refers to the ability of the WIPS to detect all known wireless attacks with the minimum possible false positive rate. Detection integrity has three components:

1. **Alarm Library** - The WIPS alarm library should be comprehensive and must include all known wireless threats. In addition the system must be able to detect day zero attacks.
2. **False Positive Rate** – False positive rate refers to the percentage of instances in which the WIPS reports an alarm when none should be triggered. High false positives increase management cost and compromise security by masking real alarms in a flood of irrelevant ones.
3. **Extensibility** - The WIPS alarm library should be easily extensible based on evolving threats.

Forensic Depth

Forensic depth is defined by the comprehensiveness and ease of retrieval of wireless activity logs. A wireless network can be audited only if comprehensive usage and event statistics are available. Forensic depth has three components:

1. **Storage Volume** - The WIPS system should have the ability to store all possible wireless events for every wireless device detected over a user defined period of time.
2. **Retrieval Efficiency** - The WIPS data store should be architected for efficient retrieval of forensic and historical information, possibly in real-time, if needed.
3. **Redundancy** - The forensic data store should have built-in redundancy and real-time failover fault-tolerance.

Proactive Protection

Proactive protection refers to the WIPS ability to defend the network and itself in real-time. It has the following four components:

1. **Rogue Termination** - The WIPS should have the ability to quickly and effectively terminate a rogue AP. The system should have the ability to perform wired side termination as well as liability free wireless termination.
2. **Accidental Association Termination** - The WIPS should have the ability to detect authorized devices having accidental associations with unauthorized devices and must be able to immediately terminate the connection.
3. **Vulnerability Assessment** - The WIPS must have the ability to proactively audit the entire wireless network and all its associated devices for known vulnerabilities before they are attacked. This should be done with the least possible disruption of regular network activity.
4. **Self-Defense** - The WIPS must be able to defend itself and operate as covertly as possible.

Management Ease

Securing a wireless network, maintaining performance and policy compliance can be a daunting task. Management ease allows the WIPS user to effectively and easily operate the system for uncompromised wireless protection. Management ease has two components.

1. **Self-Managing** - The WIPS should manage itself as much as possible. Once policies are defined, the system should automatically monitor and protect without human intervention.
2. **Expert System** - The WIPS must have expert system capabilities to analyze a problem and recommend step-by-step actions to the user for solving the issue quickly.

The AirDefense Solution

The AirDefense solution is based on a **Distributed Collaborative Intelligence Architecture (DCIA)**, pioneered by AirDefense, to provide the highest possible FOM for WIPS. DCIA uses a dedicated network of sensors and embedded client agents that continuously monitor the airwaves and wireless activity for attacks and policy violations.

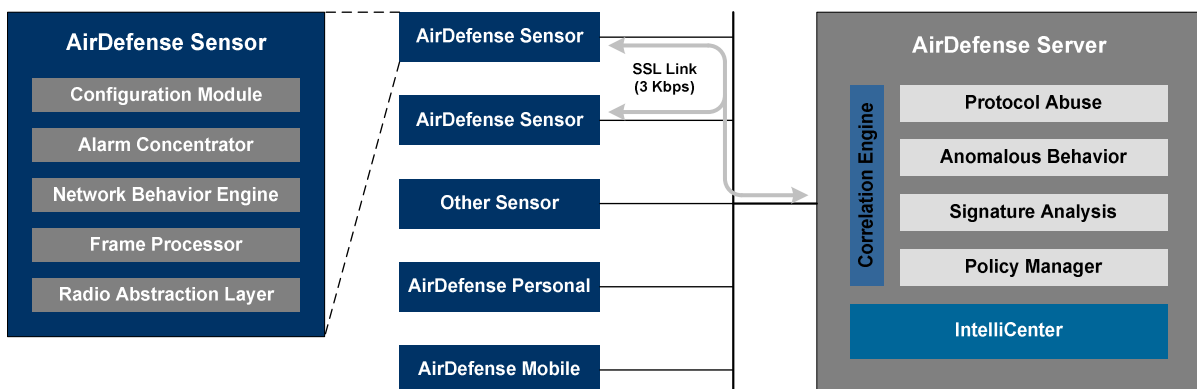


Figure 2: AirDefense's distributed collaborative intelligence architecture using sensors, agents and server

The DCIA architecture, shown in **Figure 2**, has the following salient features:

5. APs with special firmware allowing promiscuous mode are used as dedicated sensors. Promiscuous mode allows sensors to listen to all packets picked up by the antenna. In addition, the sensors use an intelligent channel scanning algorithm to detect traffic across the RF spectrum. The sensors locally analyze all the received packets, collect several statistics and events of interest and use a very efficient Application Programming Interface (API) to communicate selected events and statistics over a secure link to a centralized server.
6. Lightweight software agents are installed on laptops and other wireless devices. These agents monitor wireless activity and enforce pre-determined security policies even when the device is not within the monitored enterprise perimeter.
7. The centralized server correlates events and statistics from all the sensors and agents and runs a multi-dimensional engine that integrates several detection technologies. Security policies are centrally managed and monitored from the server.

AirDefense sensors are modular by design allowing sensor functionality to be quickly ported onto any AP hardware. The modular sensor design provides a flexible framework to address various customer requirements. A complete stand-alone system can be readily built by placing all the modules on the same host. A sensor-only server-less distributed system can be installed without the need for a server, with configuration and alarms being handled by a third-party, such as an SNMP manager. The sensors use a bandwidth efficient SSL link to communicate with the server. In addition, sensors can collaborate among themselves using an efficient message-based API between the modules, optimizing distributed processing power across several units. Sensors are used as transmitters for wireless termination.

Client based agents are an integral part of DCIA. AirDefense Personal is a small software agent that runs on Windows PCs and monitors wireless activity and threats. It reports wireless attacks and policy violations to the user and a central manager. The manager runs on the server and can be used to enforce policy and monitor each client even when it is outside the range of dedicated DCIA sensors. AirDefense Mobile is a special sensor that runs on a laptop and can be used for site surveys at field offices and remote locations that do not have dedicated DCIA sensors. Alarms and statistics from Mobile are also available through the server.

The AirDefense server runs on a hardened Linux kernel and can be supported on a range of hardware platforms from standard laptops to a dedicated multi-processor server appliance. Several detection technologies such as anomalous behavior, stateful protocol analysis and signature matching are used. In addition, the server has a sophisticated correlation engine that analyzes data across sensors and individual detection engines to minimize false positives. The system architecture is such that functionality can be adaptively shifted between the server and sensor. The server can ask the sensor to process more events and statistics and provide a consolidated report periodically. It can also ask the sensor to provide a real-time feed of all packets it is detecting at any given time. The AirDefense server also incorporates the IntelliCenter. The IntelliCenter assimilates several statistics for every wireless device on a minute by minute basis and is designed to allow the WIPS to seamlessly scale.

“After completing an exhaustive search of wireless LAN security and management solutions, DeCA concluded that AirDefense offers the only enterprise-class solution for 24x7, real-time monitoring of the airwaves that scales to support a wireless LAN deployment with more than 1,000 access points around the globe. AirDefense provides the central management functionality that allows our IT staff to monitor and manage the entire wireless LAN from a single location.”

Kendra Warren, CIO, Defense Commissary Agency (DeCA)

Visibility Coefficient

The AirDefense solution meets the complex requirement of four dimensional wireless visibility through the following mechanisms.

- AirDefense Enterprise sensors monitor wireless activity within your enterprise 24x7 across the deployment area.
- AirDefense Personal and BlueWatch client based agents follow your mobile workers in hotspots, homes and everywhere else they use wireless networks, providing comprehensive spatial and temporal protection.
- AirDefense sensors use intelligent scanning across frequencies and support the latest protocols so that no wireless attacks can fly below their radar.
- AirDefense Personal and BlueWatch work in collaboration with the AirDefense Enterprise server for centralized policy administration and threat management of not only Wi-Fi devices but other wireless protocols such as Bluetooth and EvDO.

Architectural Scalability

AirDefense’s DCIA is built on the fundamental notion of architectural scalability without security compromise.

- AirDefense’s IntelliCenter technology is designed such that a single server can monitor over 100,000 total wireless devices and several hundred sensors deployed globally.
- AirDefense Enterprise sensors use a very efficient, FIPS compliant, secure communication link to communicate with the server requiring using less than 3 Kbps of wired bandwidth when providing full-fidelity analysis of all WLAN communications.
- The sensors are extremely modular by design as shown in Figure 2. The Radio Abstraction Layer allows AirDefense sensor functionality to be quickly ported onto any infrastructure hardware.

Context Awareness

As wireless networks expand and the number of wireless threats grow, administrators face the daunting task of resolving the hundreds of events detected by a WIPS. While other systems offer simple methods for prioritizing alarms, AirDefense employs context-aware detection schemes that take both real-time and historical data into account when analyzing wireless activity.

- Sophisticated threat index assessment algorithms can factor historical context in real-time to provide only relevant alerts. The system adapts and learns over time from prior information.

- Close integration with network infrastructure allows the system to have real-time network knowledge. Real-time network knowledge facilitates advanced rogue discovery algorithms while allowing liability free rogue termination.
- Wired side context awareness enables the AirDefense system to detect rogue wireless devices in “no wireless” environments without using any sensors.

Detection Integrity

The AirDefense WIPS is designed to stop the true threats to your network without wasting time on false positive alarms.

- AirDefense provides the most comprehensive alarm library capable of detecting over 200 different wireless attacks.
- The anomalous behavior and correlation engines are capable of detecting day zero attacks.
- By using multiple detection technologies coupled with context aware processing, AirDefense is able to achieve the lowest false positive rate.

“Synopsys evaluated the market for WLAN monitoring, including AP switching and scanning vendors, and quickly recognized the need for a dedicated sensor-based system with centralized policy monitoring and enforcement. Only AirDefense could provide this level of security and policy enforcement. Synopsys chose AirDefense for their robust intrusion detection engine that does not overwhelm you with false positives.”
Van Nguyen, Director of Security, Synopsys

Forensic Depth

The AirDefense WIPS is designed with total forensic and incident analysis capabilities that are necessary for compliance management, performance optimization and liability free wireless network operation.

- The AirDefense IntelliCenter stores almost 270 different statistics per wireless device per minute. It can concurrently support over 100,000 devices and accumulate data over years. The IntelliCenter enables the system to have “RF Rewind” capability with high resolution.
- The forensic engine allows the user to access all the stored information efficiently. The module has built-in analysis, historical trending and reporting features that allows users to analyze intrusions and wireless performance issues with rich historical context.
- The system maintains comprehensive historical data required by many regulations such as SOX, HIPAA, GLBA and the Department of Defense.
- The IntelliCenter has complete failover protection.

Proactive Protection

The AirDefense self-managing WIPS offers proactive protection in a number of ways.

- The AirDefense system offers policy-based, liability-free, wired and wireless terminations for rogue devices. Policy-based wireless terminations are available for accidental associations as well.
- The system uses smart termination allowing continued scanning while termination is in progress for uninterrupted protection. Multiple simultaneous terminations are also allowed.
- Built-in location tracking allows users to physically locate and track rogue as well authorized devices.
- The AirDefense system also has a built-in vulnerability assessment module that proactively audits the wireless network for known security threats and policy violations.
- The AirDefense system operates in stealth mode, never revealing its identity over the air.
- AirDefense is the only WIPS to receive Common Criteria certification from the National Information Assurance Partnership (NIAP) program. Common Criteria certification provides our customers with the confidence that AirDefense Enterprise meets the stringent security requirements stipulated by the federal government.
- AirDefense Enterprise utilizes FIPS 140-2 compliant encryption modules and is the only system to implement digital signature authentication between system components.

“For Carilion, rogue wireless LANs are a serious matter. AirDefense provides the peace of mind from knowing that we can identify and eliminate all unsanctioned wireless laptops, APs, ad hoc networks and application-specific wireless devices as they enter our airspace.”

Greg Walton, Senior VP & CIO, Carilion Health System

Management Ease

Monitoring systems are famous for presenting a lot of alarms that administrators are required to plow through to resolve problems. Information overload often results in process inefficiencies and security compromises. AirDefense uses intuitive and efficient WIPS management.

- The system is a virtually self-managing platform for day-to-day operations once policies are defined.
- The system includes multiple dashboards that present succinct information about the operation of the network and provide quick ways to drill down into problems.
- Role-based partitioning allows the WIPS to be administered by users with different levels of expertise and security clearance.
- Threat index based alarm management enables prioritized actions to be taken with finite time and resource constraints. Several filtering options allow the user to have a better handle on large scale deployments.
- Expert system capabilities are provided through intuitive wizard driven problem solving.

- Automated policy templates are available for standard as well as user defined compliance management.

FOM Comparison

Table 1 compares the AirDefense WIPS with several other commercial solutions based on our assessment of their products and feedback from several customers on each FOM attribute described in **Section 2**. Each FOM attribute is graded on a relative scale of 0 to 10. A score of 10 is perfect, 5 is average and 0 implies non-existent attribute. The FOM attributes are reasonably orthogonal. This allows the evaluation to be objective and prevents undue system advantage or disadvantage based on any single criteria. The average score of the individual sub-attributes determines the score for each of the seven main attributes. The final FOM score is computed based on the average of the seven attributes. This method results in equal weight being assigned to each FOM attribute and might not always be justified. Different users have different requirements and some attributes may be more important to them than others, requiring the use of a weighted average for the FOM calculation based on user assigned relative importance. In order to avoid emphasizing any one attribute for this paper, we have use equal weights. **Figure 3** compares the overall FOM of the leading WIPS solutions based on equal weights for each attribute.

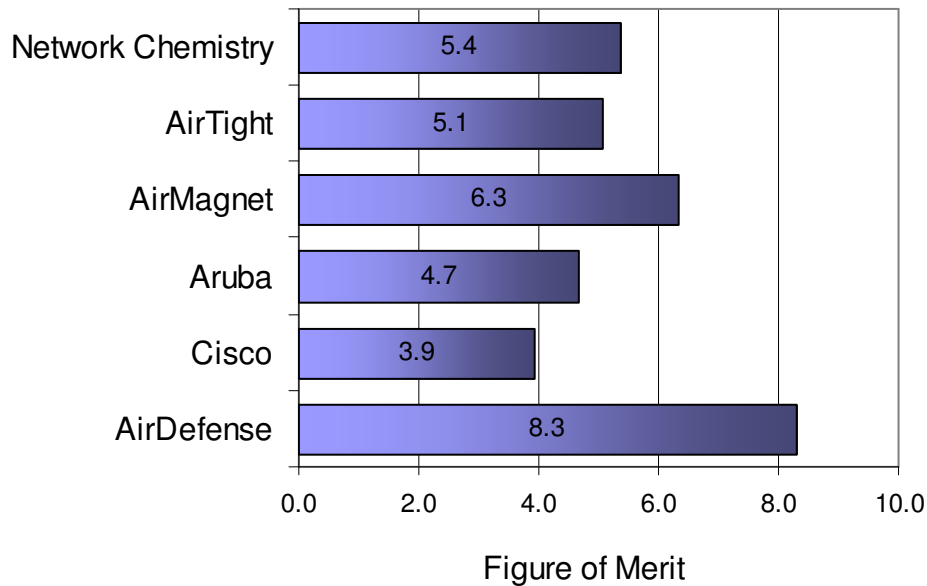


Figure 3: FOM comparison of leading WISP vendors

Figure of Merit Attribute		AirDefense	Cisco	Aruba	AirMagnet	AirTight	Network Chemistry	Weights
Visibility Coefficient		9	6	6	7	7	8	1
Space	9	5	5	4	4	4		
Time	10	4	4	10	10	10		
Frequency	8	7	7	6	6	8		
Protocol	8	9	9	8	7	8		
Architectural Scalability		9	6	8	8	6	7	1
Device Concurrency	10	6	7	7	4	7		
Sensor Bandwidth	10	9	9	10	9	9		
Modularity	8	4	7	6	6	5		
Context Awareness		7	5	5	3	2	1	1
Historical Filtering	7	0	0	0	0	0		
Real Time Network Knowledge	6	9	9	5	4	2		
Detection Integrity		8	2	3	7	5	7	1
Alarm Library	9	2	4	8	5	8		
False Positive Rate	9	1	4	6	5	6		
Extensibility	7	2	2	7	5	6		
Forensic Depth		9	4	4	7	5	5	1
Storage Volume	10	1	1	6	4	3		
Retrieval Efficiency	8	5	5	6	5	5		

Figure of Merit Attribute		AirDefense	Cisco	Aruba	AirMagnet	AirTight	Network Chemistry	Weights
	Redundancy	8	7	7	8	5	6	
Proactive Protection		9	2	3	7	5	6	1
	Rogue Termination	9	4	7	7	6	7	
	Accidental Association Termination	9	0	0	7	6	7	
	Vulnerability Assessment	7	0	0	6	4	6	
	Self Defense	9	2	3	6	5	5	
Management Ease		8	3	4	7	6	5	1
	Self-managing	8	4	6	7	6	6	
	Expert System	8	2	2	7	5	3	
FOM		8.3	3.9	4.7	6.3	5.1	5.4	

Table 1: Detailed FOM scorecard of leading WISP vendors

Summary

The FOM of a WIPS is defined by its visibility coefficient, architectural scalability, context awareness, detection integrity, forensic depth, proactive protection and management ease. It is easy for vendors to claim that they have WIPS with one or two of these FOM requirements. A true enterprise-class WIPS must meet all the FOM attributes. The AirDefense solution has the highest WIPS FOM in the industry.

“AirDefense is a clear leader in wireless surveillance and offers the best available solution on the market.”

Rene Hirsch, Managing Director, AirWire

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. **All trademarks are the property of their respective owners.**