AirMagnet Enterprise

How AME Fulfills the Technical Requirements for a

WIRELESS IPS AND PERFORMANCE MONITORING SYSTEM

Overview

This document describes how AirMagnet Enterprise fulfills the minimum specifications required for a Wireless Monitoring and Intrusion Prevention System.

In this case, the WIPS and wireless monitoring system shall be an intelligent sensor system that is centrally managed and allows for remote real-time views to any sensor for both frame and spectrum analysis. It will be purpose-built solution performingcontinuous detection of WLAN Security and Performance Problems.

The system shall have the characteristics as specified in this document:

1. Administration

AirMagnet enterprise will support tiered and delegated administration. Multiple network administrators can administer, monitor and manage the system. Administrators will be able to delegate administration and create and manage various locations where the system and devices can be managed independently. The access to functionality that delegated administrator sees and is able to act on will be controlled such as access to reporting or performance or security alerts.

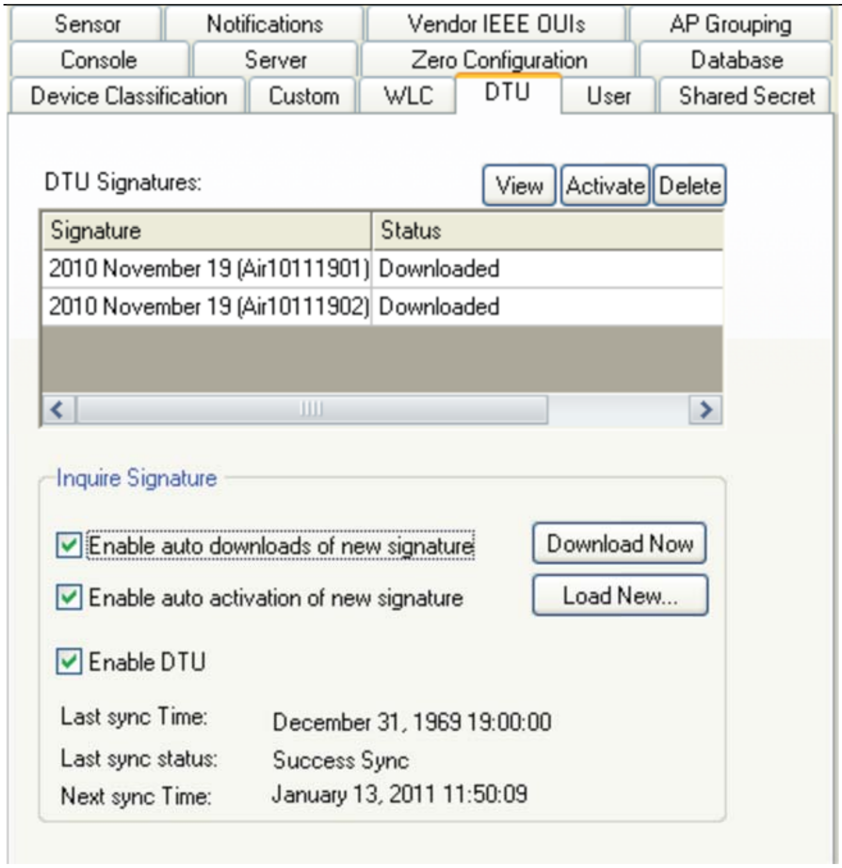
2. Active Wireless Health and Performance Validation and Verification

Active wireless LAN performance and security validation and verification shall be an integral part of the system. It will provide the capability to perform active WLAN testing to validate performance, security and compliance metrics using the user defined testing thresholds. Active WLAN tests shall be capable of running on a scheduled or manual basis or both. Active test profiles shall have to capability to utilize symmetric and asymmetric cryptography and shall at minimum support the following WLAN authentication types: WPA-PSK, WPA2-PSK WLAN authentication and all EAP types including PEAP and Certificate based TTLS/TLS. Data captured and measured during the test jobs shall be stored and available for display both by test or daily/weekly trend graphs. This information shall also be exportable to a format suitable for building custom and/or trend reports, such as Microsoft Excel.

3. Automatic Signature Update

Threat definitions are separately and autonomously loadable, so they can be automatically installed without any disruption to operations requiring change control planning. The underlying IPS architecture will enable the system to further accelerate the development of new threat definitions by automating on-demand updating of threat signatures. This update capability shall run autonomously and without the need for user interaction or monitoring.

Automated Signature Updates



DTU Signatures:

Signature	Status
2010 November 19 (Air10111901)	Downloaded
2010 November 19 (Air10111902)	Downloaded

Inquire Signature

☑ Enable auto downloads of new signature

☑ Enable auto activation of new signature

☑ Enable DTU

Last sync Time: December 31, 1969 19:00:00
Last sync status: Success Sync
Next sync Time: January 13, 2011 11:50:09

4. Automated Health Check

AirMagnet Enterprise monitors WLAN health by actively auditing the network status measuring, monitoring and alarming on:

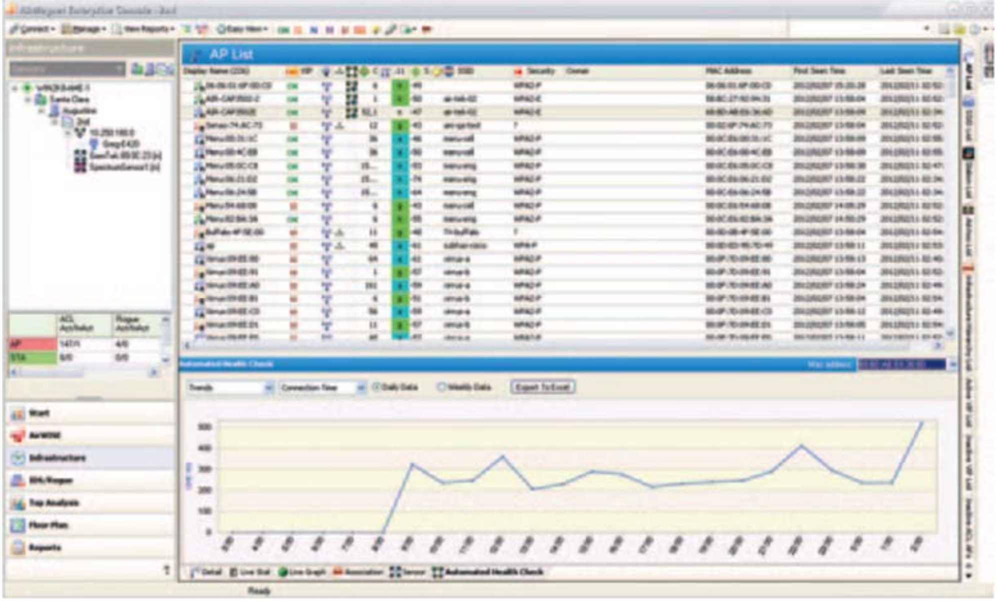
- Access Point Connection. The alarm contains information about the audited connection time versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point Authentication. The alarm contains information about the audited authentication time versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point DHCP. The alarm contains information about the audited DHCP connection time versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point PING. The alarm contains information about the audited PING host connection time versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point FTP Download. The alarm contains information about the audited FTP download speed versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point HTTPS Download. The alarm contains information about the audited HTTPS download speed versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.

- AHC Access Point HTTP Download. The alarm contains information about the audited HTTP download speed versus the threshold, the audit being performed, and the SmartEdge Sensor performing the audit.
- AHC Access Point Connection, failed by SSID. The alarm contains information about the audited SSID, the audit being performed and the SmartEdge Sensor performing the audit.
- AHC Job Failed: Signal Strength Threshold not met. The alarm contains information about the audit being performed and the SmartEdge Sensor performing the audit.

The information is presented in the graph format and consists of:

- AHC Daily Trends - trend data for the current day
- AHC Weekly Trends - trend data for the last 7 days
- AHC Monthly - trend dtafor the last 30 days

Automated Health Check performance test results



5. Context Sensitive Help

The system shall contain a help system that is contextually linked to each screen and an intelligent engine to help automate and identify the source of performance or security problems.

6. Database Support

The system shall support PostgresSQL database. No Database Synchronization will be required as primary and Secondary utilize common DB (Supports VIP's [Virtual IP Addresses])

7. Forensic Capture and Real-Time Views

The system will be capable of automated capture of targeted network traffic corresponding to the exact time period when potentially harmful activity triggered threat detection and alerting. Both WLAN and RF data will be captured. The data will be stored on the AirMagnet server. Historical data retention polices can be configured. Further you will be able to receive notifications of the forensic events. Forensic files contain data relating to the alarm that triggered the notification. Additionally spectrum forensic files contain a snapshot of the RF spectrum, which helps identify sources of non-802.11 problems (such as Bluetooth devices, cordless phones, etc.).

There are a variety of the security and performance issues that can be captured in the forensic logs such as:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on denial-of-service attacks

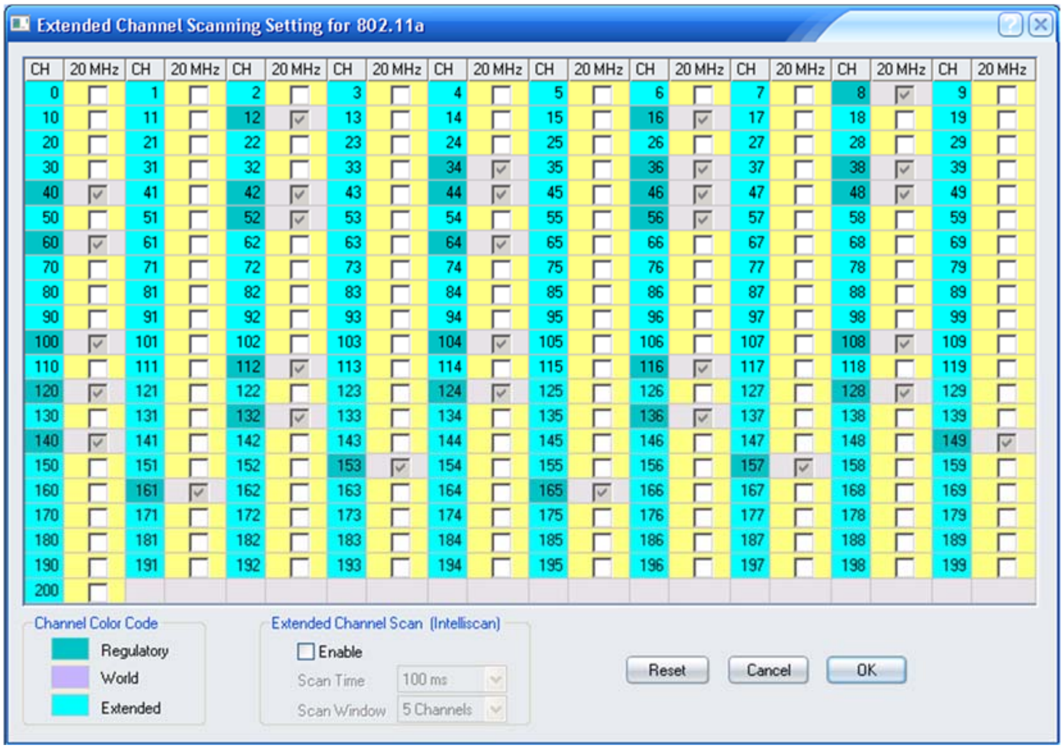
8. Scalable and Fault Tolerant Service

AirMagnet Enterprise will support mission critical applications. It will have built-in 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. Hot Standby Server can be anywhere in the world geographically. Additionally, AirMagnet Enterprise sensors will 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. This will be accomplished through local processing, “SmartEdge Technology” that eliminates single point of failure and improves MTTR and threat response as sensors will remediate the threat locally and there is no “Central Appliance” required for analysis. AirMagnet Enterprise intelligent sensors will locally analyze Wi-Fi and RF conditions. More than 1,000 sensors will be supported through single centralized server in the data center, requiring minimal network bandwidth.

9. Security and Performance Monitoring

The system will scan 200+ channels collecting the IDS/IPS data on the channels as shown below:

Channels Scanned



Extended Channel Scanning Setting for 802.11a

CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz	CH	20 MHz
0	☐	1	☐	2	☐	3	☐	4	☐	5	☐	6	☐	7	☐	8	☑	9	☐
10	☐	11	☐	12	☑	13	☐	14	☐	15	☐	16	☑	17	☐	18	☐	19	☐
20	☐	21	☐	22	☐	23	☐	24	☐	25	☐	26	☐	27	☐	28	☐	29	☐
30	☐	31	☐	32	☐	33	☐	34	☑	35	☐	36	☑	37	☐	38	☑	39	☐
40	☑	41	☐	42	☑	43	☐	44	☑	45	☐	46	☑	47	☐	48	☑	49	☐
50	☐	51	☐	52	☑	53	☐	54	☐	55	☐	56	☑	57	☐	58	☐	59	☐
60	☑	61	☐	62	☐	63	☐	64	☑	65	☐	66	☐	67	☐	68	☐	69	☐
70	☐	71	☐	72	☐	73	☐	74	☐	75	☐	76	☐	77	☐	78	☐	79	☐
80	☐	81	☐	82	☐	83	☐	84	☐	85	☐	86	☐	87	☐	88	☐	89	☐
90	☐	91	☐	92	☐	93	☐	94	☐	95	☐	96	☐	97	☐	98	☐	99	☐
100	☑	101	☐	102	☐	103	☐	104	☑	105	☐	106	☐	107	☐	108	☑	109	☐
110	☐	111	☐	112	☑	113	☐	114	☐	115	☐	116	☑	117	☐	118	☐	119	☐
120	☑	121	☐	122	☐	123	☐	124	☑	125	☐	126	☐	127	☐	128	☑	129	☐
130	☐	131	☐	132	☑	133	☐	134	☐	135	☐	136	☑	137	☐	138	☐	139	☐
140	☑	141	☐	142	☐	143	☐	144	☐	145	☐	146	☐	147	☐	148	☐	149	☑
150	☐	151	☐	152	☐	153	☑	154	☐	155	☐	156	☐	157	☑	158	☐	159	☐
160	☐	161	☑	162	☐	163	☐	164	☐	165	☑	166	☐	167	☐	168	☐	169	☐
170	☐	171	☐	172	☐	173	☐	174	☐	175	☐	176	☐	177	☐	178	☐	179	☐
180	☐	181	☐	182	☐	183	☐	184	☐	185	☐	186	☐	187	☐	188	☐	189	☐
190	☐	191	☐	192	☐	193	☐	194	☐	195	☐	196	☐	197	☐	198	☐	199	☐
200	☐																		

Channel Color Code

- Regulatory
- World
- Extended

Extended Channel Scan (Intelliscan)

☐ Enable

Scan Time: 100 ms

Scan Window: 5 Channels

AirMagnet Enterprise’s security engine, AirWISE, will analyze the wireless network for over 70 unique security vulnerabilities andattacks, triggering over 136 security alarms. It will also analyze the network for performance violations.

The security alarms cover variety of areas such as:

- authentication and encryption violations
- security penetration attacks
- DoS
- configuration vulnerabilities

The performance violations alarms cover the following:

- channel/device overload
- deployment and operation errors
- IEEE 802.11e and VoWLAN Issues
- FR management
- preconfigured policy profiles

This extensive sect of both security and performance alarms allows technical staff to see issues as they evolve and to respond before actual violations occurs. Furthermore, AirMagnet alarms provide the information and advice that IT staff needs in order to respond to various network events. Each alarm singles out the device (down to the MAC address) and/or channel involved, accompanied by detailed explanation of what the alarm means and why it is important. It even suggests best practices for resolving the problem. This capability ties prevention, detection, and response into one unified process that the network team can act on.

The system will allow administrators to customize the types and destinations of notifications that will be sent upon various security and performance violations events. The notification list includes a wide verity of notification mechanisms such as Syslog, SNMP, email, SMS over email, IM and others.SNMP alerts and Syslog will be designed to feed into a variety of SIEM solutions. At this point there will not be tight integration with any particular SIEM solution. Instead, we will test with a variety of network monitoring solution including HP OpenView and Splunk. The interoperability method will be through forwarding alert emails to these systems.

10. Spectrum Analysis

Because the 2.4-GHz and 5-GHz radio bands are unlicensed, there are numerous 2.4-/5-GHz analog cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11b/g or 802.11a WLANs are deployed. They have been recognized as a major source of RF interference for 802.11b/g or 802.11a WLANs.

To address this AirMagnet Enterprise comes with the AirMagnet Remote Spectrum Analyzer, which integrates AirMagnet's advanced spectrum-sensing hardware and analytical and visual display software into one application. This will allow network professionals to use the AirMagnet Enterprise system to monitor and collect spectrum data as the basis for network design and planning, troubleshooting, and optimization.

The system will offer real-time detection and identification of a number of non-WLAN sources that interfere with the WLAN Networks, including but not limited to:

- bluetooth devices
- digital and analog cordless phones
- conventional and inverter microwave ovens
- wireless game controllers
- digital video converter
- baby monitors
- RF Jammers
- radar signals
- motion detectors
- zibgee devices
- variety of other devices that can be classified utilizing unique RF signatures

Besides detecting interfering devices the system will also provide the best Recommended Courses of Action. Once interfering devices are successfully located, the actions will be recommended to minimize or eliminate the RF interference.

Further, the system will provide real-time FFT graphs, FFT Duty Cycle plots, Swept Spectrogram, and professional RF Spectrum graphs and Wi-Fi charts using a dedicated, full-time radio for spectrum analysis. System will also have Channel Duty Cycle and Interference Power v Time Trending to monitor how interference signals are affecting the noise on a per channel basis. System should provide a complete inventory of all Wi-Fi devices operating in the 802.11 environment and will include info such as: AP Signal Strength, Channels by Speed/Address/Media; Top 10 APs by CRCs/Retry, Channel SNR; Errors/Retry; Channel Utilization and Channel Occupancy.

System will retain evidence of interferers and record and playback events. System shall cover, at minimum the following frequency bands: 2402 - 2494MHz, 4910 - 4990MHz, 5160 - 5330MHz, 5490 – 5710MHz and 5735 – 5835MHz. System shall have the ability to support either external or internal antenna configurations.

11. Wireless Discovery

The system shall display the current list of active AP's and Stations as seen in the network air space of the <Customer Name Here>. The screen must display a device tree that may be expanded to show all AP's that are authorized, neighbors or rogues. The system will provide the SSID, security type, vulnerabilities and timestamp of authorized, neighbor, rogue and unknown devices.

The system shall automatic classify unknown wireless devices based on Boolean rules defined and editable by the user. These rule sets shall be exportable and importable into the classification engine.

12. Wireless Traffic Blocking

AirMagnet Enterprise can automatically block the rogue device. Whether the rogue device is a client station, ad-hoc station or an AP, AirMagnet SmartEdge sensor will terminate its wireless communication. The block is ingenious in that it blocks bi-directionally, spoofing the AP to the station and the station to the AP (or ad-hoc to ad-hoc) without interrupting normal (authorized) wireless traffic. This is true even of a blocked station attacking an AP. The AirMagnet sensor will continue to scan as it blocks the devices and can adjust its blocking to "follow" a blocked device if it changes channels, SSIDs, Media bands etc. Additionally, the sensor will continue to generate alerts on other devices that may or may not be associated with the blocked device as normal with no interruption of service.

AirMagnet Management Server coordinates the blocking effort so that the closest sensor (sensor with the strongest rogue signal strength) does the tracing (if not already traced) and blocking. Each sensor can effectively block up to ten devices on the same channel.

13. Wired/Wireless Traffic Blocking

AirMagnet Enterprise interoperates in standardized fashion with a variety of LAN switching equipment. This is done to assure that rogue devices are not accessing the wired network potentially compromising the sensitive information. AirMagnet Enterprise issues SNMP commands to obtain MAC addresses of the rogue APs and stations that are attached to the wired network.If a rogue AP is connected to an infrastructure network, one of the measures to be taken is to quarantine the rogue AP from the network. This can be done by shutting down the switch port to which the rogue AP is connected.AirMagnet Enterprise supports a rogue policy that automatically blocks the rogue device from its directly connected switch by shutting down the switch port. Some key AirMagnet advantages are:

- Both automated blocking and manual blocking are supported. For automated blocking, a time period can be specified so that the switch port will be automatically unblocked making the switch port functional again. If the rogue device continues to be detected at the time when the blocking expires, a rogue alarm will be regenerated to trigger the reinstated blocking action.
- When automated device blocking is used, the user needs to be aware that the notification action will work in combination with the device policy and classification rules. Once the rogue devices are detected according to the policy and classification rules, AirMagnet Enterprise will start device blocking either from the sensor or the server depending on the tracing configuration.

14. VoIP over Wi-Fi Performance and Security

VoWLAN calls are negatively affected by the high Wi-Fi bandwidth utilization leading to choppy voice quality and degraded performance. To monitor this issue AirMagnet Enterprise will track the AP and bandwidth utilization. Further in conjunction with AirMagnet mobile critical performance characteristics like Jitter can be monitored and acted on as well.

AirMagnet will monitor the APs utilization by VoWLAN clients. It will generate alarms when pre-configured thresholds will be crossed.   AirMagnet tracks Quality of Service 802.11e data such as channel utilization.

FurtherThe AirMagnet Jitter tool available on the AirMagnet Mobile product allows the user to effectively measure RF signal jitter in both incoming and outgoing WLAN traffic between an access point and a station. Based on this information the user can make the appropriate changes to the configuration or the placement of the APs to reduce the interference.

15. Wi-Fi Vendors Interoperability

AirMagnet has been tested and interoperates and monitors a variety of the Wi-Fi vendors. Further, for Access Control List (ACL) integration AirMagnet Enterprise is integrated with the Cisco WLC, WLS and Aruba's Airwave.

16. AirMagnet SmartEdge Sensor

The AirMagnet SmartEdge Sensors are deployed in the wireless network to proactively monitor the environment for more than 135 alarms that could impact the security and performance of the network. Unlike simple packet sniffing probes, each AirMagnet SmartEdge Sensor has a built-in intelligent AirWISE analysis engine, allowing it to automatically monitor the network environment. This unique ability allows the "heavy lifting" of the analysis to be performed locally at the edge of the network and avoids the additional bandwidth overhead of capturing and re-sending each and every packet to a central server for processing. The AirMagnet SmartEdge Sensors are placed throughout the network and report back to the AirMagnet Enterprise Server using the 10/100 Ethernet.

AirMagnet Enterprise Sensor 4 Series SmartEdge Sensor: These models represent the next generation in 3X3 11n sensor technology. It features the new high performance 1.8 GHz ARM based processor, a 10/100/1000 MB Ethernet Base-T port with IEEE 802.3af Power over Ethernet (PoE) compliance, one or two 802.11n 3X3 3 stream 450mbps radios and a spectrum analyzer option. AirMagnet dual radio sensors such as AirMagnet Series 4 R2 models enables some new AirMagnet Enterprise capabilities including the following functions:

- Wireless connection and configuration in the AirMagnet Enterprise Console
- Dual Mode Support: Simultaneous Automatic Health Check (AHC) and passive scanning using a wired connection
- Passive scanning using a wireless connection
- AHC mode using wireless connection

17. Reporting

The system will have automated reporting for compliance and performance. Reporting will include but be not limited to PCI-DSS, HIPAA, and any performance-related events triggered by breeching of a performance threshold in the WLAN such as excessive retries. AirMagnet Enterprise will provide 50 customizable reports to show trends in the network, the history of security issues and overall policy compliance. Reports can be generated on schedule or instantaneously. Reports will cover a variety of categories such as:

- General system reports
- Compliance reports
- Alarm reports
- Device reports
- Rogue device reports
- Monitored device reports
- Security IDS/IPS reports
- Performance Intrusion reports
- And others

For instance, the system will provide very rich compliance reporting for DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley, and Payment Card Industry Data Security Standard (PCI DSS) Compliance Reports provide a security framework to comply with regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on wireless network security and aim to guide network administrators in documenting their security policies and responding to security threats and incidents in compliance with industry best practice and government regulations.

The reports contain the location, time period, context of the issue or compliance report such as applicable law and then the statistic represented in data and graphical format.

18. 24/7 Monitoring Through Dedicated Sensors

The Sensors do not “Time Slice”. The sensors 802.11b/g/a/n radio and Spectrum Analysis (SAgE) engine shall operate independently of each other, have their own process and perform simultaneous scanning/analysis.