Datenblatt: AirMagnet Enterprise

AirMagnet Enterprise bietet eine skalierbare Lösung für die ständige Überwachung der WLAN-Sicherheit und -Leistung, die alle Arten von drahtlosen Sicherheitsrisiken minimieren, Unternehmensrichtlinien durchsetzen, Leistungsstörungen in drahtlosen Netzwerken vorbeugend erkennen und lokalisieren und die Einhaltung gesetzlicher Bestimmungen für alle Wi-Fi-Geräte überwachen kann.

- *Durchgehende Datenpaket- und HF-Prüfung des drahtlosen Netzwerks, sodass kostspielige Bedrohungen immer erkannt werden*
- *Überwachung rund um die Uhr auf Konnektivitätsprobleme wie Kanal-Interferenz, Deckung, fehlerhafte Pakete, Deautorisierungsangriffe, um eine optimale und zuverlässige WLAN-Verfügbarkeit zu gewährleisten*
- *Automatische Zustandsprüfung durch Automated Health Check (AHC) überwacht und meldet alle drahtlosen AP-Leistungsprobleme proaktiv*
- *Möglichkeit zur aktiven Durchführung von Remote-Tests, zur Remote-Diagnose und -Behebung bei gleichzeitiger Zeitersparnis*
- *Dynamisches Aktualisieren der Technologie mittels Dynamic Threat Update (DTU) stellt sicher, dass das Netzwerk jederzeit geschützt ist, auch gegen neue Bedrohungen*
- *802.11ac-Unterstützung mit 802.11ac-kompatiblen Access Points*

AirMagnet Enterprise

Das zentrale drahtlose System zur Angriffserkennung und Verhinderung (WIDS/WIPS) von AirMagnet Enterprise verteidigt Ihre drahtlose Umgebung durch automatische Erkennung, Blockierung, Verfolgung und Auffindung jeder Bedrohung auf allen Wi-Fi-Kanälen. Es enthält eine beispiellose Reihe von Programmen für Ereignis-Alarmierung, Eskalation, Remote-Fehlerbehebung, forensische Analyse, Netzwerk-Zustandsprüfung und professionelle PCI- und andere Richtlinienkonformitäts-Berichterstattung. Das Endergebnis ist ein vereinheitlichtes System, das Ihr System zeitlich zu 100 % scannt, um sicherzustellen, dass Ihr WLAN sicher arbeitet und die Bedürfnisse Ihrer Benutzer und Anwendungen erfüllt.

Zusätzlich zu umfangreichen Sicherheitsfunktionen überwacht AirMagnet Enterprise kontinuierlich den Zustand der WLAN-und HF-Umgebung, um die hier auftretenden Probleme proaktiv zu ermitteln, die zu Ausfallzeiten im Netzwerk führen können. Das System ermittelt Störungen, gibt Benutzern Korrekturratschläge und beinhaltet aktive Remote-Tools, um die Störung zu überprüfen. Dies ermöglicht dem Personal, Netzwerk-

AirMagnet Enterprise – Vollständige Mobilfunk- und Wi-Fi-Sicherheit

AirMagnet Enterprise schützt durch eine Kombination der branchenweit umfassendsten WLAN-Überwachung mit einer in Forschung, Analyse und Bedrohungsbehebung führenden Lösung vor allen erdenklichen WLAN-Risiken.

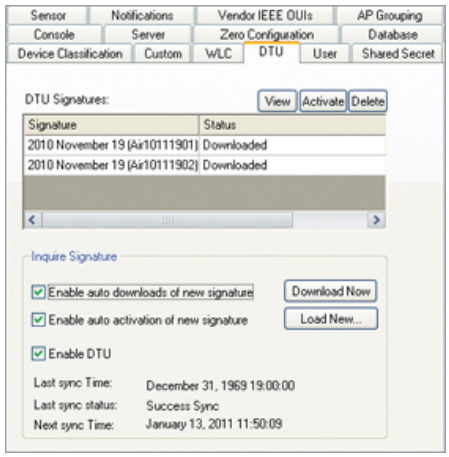
Vollständige Transparenz

Anders als Access Points (AP) fragt AirMagnet Enterprise alle möglichen 802.11-Kanäle (einschließlich der 200 erweiterten Kanäle) und die Kanäle des mobilen Spektrums ab und stellt sicher, dass es keine blinden Punkte gibt, an denen Fremdgeräte sich verstecken können. AirMagnet Enterprise bietet auch mobile Spektralanalyse, die HF-Blockierungsattacken, Bluetooth-Geräte und viele weitere nicht-802.11-Transmittertypen feststellt und einstuft, wie z. B. drahtlose Kameras und Mobiltelefone.

Branchenweit führende Gefahrenerkennung

Das Sicherheits-Forschungsteam von AirMagnet überprüft fortwährend die aktuellsten Hack-Techniken und -Trends sowie mögliche Schwachstellen, um Unternehmen gegenüber den sich ständig weiterentwickelnden Bedrohungen abzusichern. Unsere dynamische Technologie zur Anpassung an Bedrohungen Dynamic Threat Update (DTU) beschleunigt die Erstellung, Automatisierung und sofortige Bereitstellung von neuen Bedrohungssignaturen. Neue DTU-Signaturen können ohne Auswirkungen auf den Betrieb des Systems sofort bereitgestellt werden, was einen einzigartigen Rahmen für die Aufrechterhaltung der aktuellsten WLAN-Sicherheitslage für über 230 Bedrohungen bereitstellt.

Die AME AirWISE®-Engine analysiert ständig alle(n) Mobil-Geräte und -Verkehr mit einer Kombination aus Frame-Inspektion, zustandsorientierter Musteranalyse, statistischer Modellierung, HF-Analyse und Störungserkennung.



Dynamic Threat Update

Automatisierte Reaktion und Netzwerkschutz

AirMagnet Enterprise bietet eine vollständige Palette an richtliniengesteuerten Fehlerbehebungs- und Untersuchungsoptionen, um sicherzustellen, dass WLAN-Probleme schnell und präzise erfasst und die entsprechenden automatisierten Schutzmechanismen aktiviert werden.

Bedrohungsverfolgung, -blockierung/-unterdrückung und -zuordnung
Alle Geräte werden über eine Gruppe drahtgebundener und drahtloser Nachverfolgungsmethoden verfolgt, sodass schnell und zuverlässig ermittelt werden kann, ob ein Gerät mit dem Netzwerk verbunden ist. Das System verwendet einen kürzlich erweiterten Satz hoch entwickelter Techniken, einschließlich der Verwendung von SNMP, automatischer Switch-Feststellung sowie Hardware- und Verkehrsanalyse, um genaue, schnelle Verfolgung in jeder Netztopologie sicherzustellen.

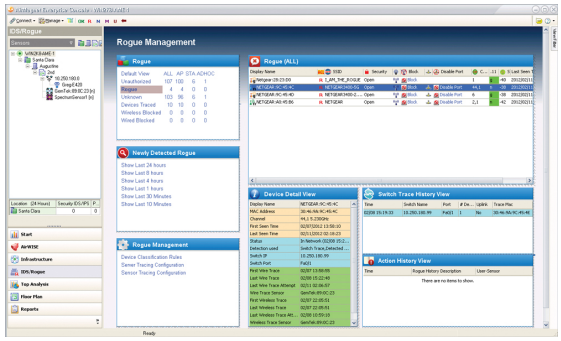
Bedrohungen können mit einer Kombination aus verdrahteter und drahtloser Bedrohungsunterdrückung manuell oder automatisch abgewehrt werden. Mit Wireless-Blockierung wird eine Bedrohung an der Quelle angegriffen und das spezifische Wireless-Gerät wird daran gehindert, drahtlose Verbindungen aufzubauen. Bei verdrahteter Blockierung wird der verdrahtete Switch-Port geschlossen, zu dem eine Bedrohung verfolgt worden ist.

Alle Bedrohungen und Geräte können auf einer Karte bzw. einem Grundriss zugeordnet und so eingerichtet werden, dass Alarme für nicht autorisierte Geräte anhand des Standorts des Geräts ausgelöst werden.

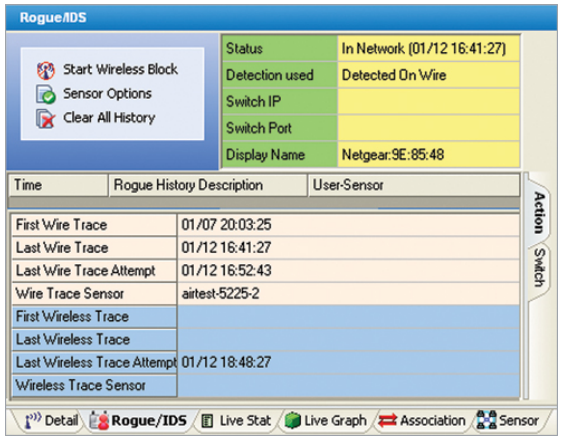
Ereignis-Forensik
AirMagnet Enterprise erfasst ein komplettes Datenpaket oder eine HF-Forensikaufzeichnung eines beliebigen Netzwerkereignisses, um den betreffenden Mitarbeitern eine umfassende Problemanalyse zu jeder Zeit zu ermöglichen.

Benachrichtigung und Integration
Manager haben Zugriff auf mehr als ein Dutzend Benachrichtigungs- und Eskalationsmechanismen, um die entsprechenden Mitarbeiter schnell auf bestimmte Probleme aufmerksam zu machen oder WLAN-Ereignisdaten in größere Unternehmensverwaltungssysteme und -vorgänge zu integrieren.

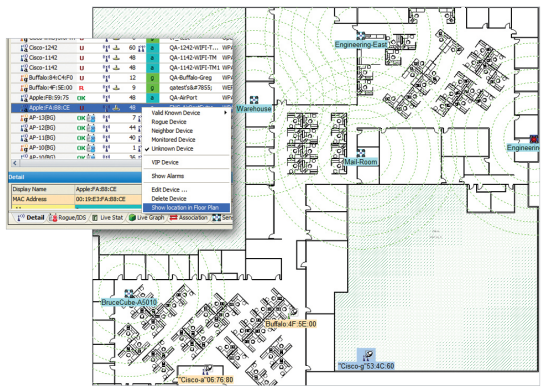
Flexible Sensor-Architektur
Der SmartEdge-Sensor, Serie 4 bietet ein Dreiband-Design mit zwei 802.11n-3x3-MIMO-Wi-Fi-Antennen, sowie dedizierter Wi-Fi- oder Mobil-Spektralanalyse. Dieses Design ermöglicht es, eine drahtlose Verbindung vom Sensor aus herzustellen. Dadurch sind kostspielige Ethernet-Verkabelung oder gleichzeitige Sicherheitsüberwachung und Leistungsprüfung nicht länger erforderlich.



Verwaltung nicht autorisierter Geräte



Nicht autorisiertes Gerät erkannt und geortet



Nicht autorisiertes Gerät auf Grundriss lokalisieren

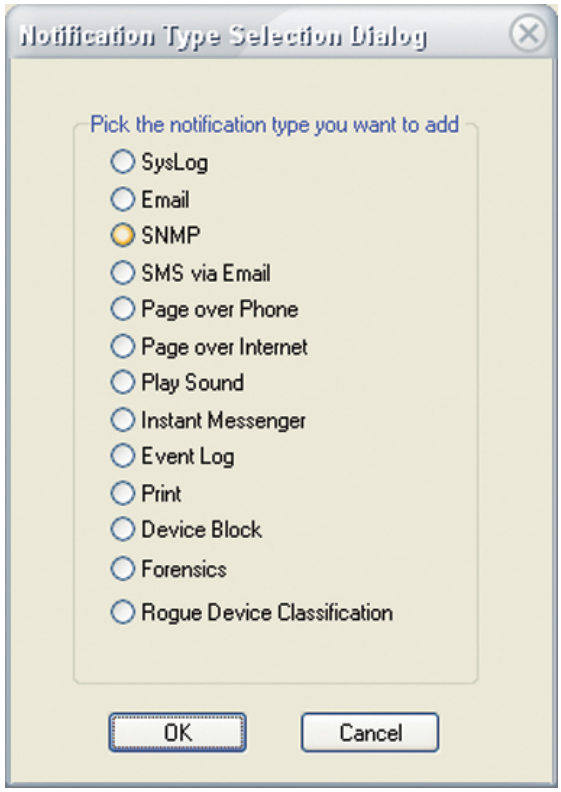
„Best-of-Breed“-Sicherheitsarchitektur

AirMagnet Enterprise bietet die einzige Lösung der Branche, die die etablierten Standards einer unternehmenskritischen Sicherheitsapplikation erfüllt. Es ist das einzige System, das Störungstoleranz in jede Komponente integriert, mit ausfallsicheren Boot-Images in jedem Sensor und automatischen Server-Ausfallsicherungslizenzen, die standardmäßig zum System gehören. Zusätzlich können Sensoren von AirMagnet Enterprise als völlig unabhängige IDS/IPS-Knoten fungieren, die Bedrohungen ohne Informationsverlust ermitteln und abwehren können, selbst wenn die Netzwerk-Verbindung zum Server für Tage verloren geht. Weitere einzigartige Vorteile der AirMagnet Enterprise-Architektur umfassen Folgendes:

Massive Skalierbarkeit
Mit den intelligenten Sensoren, die Wi-Fi und HF-Bedingungen lokal analysieren, können mehr als 1,000 Sensoren durch einen einzelnen zentralen Server im Rechenzentrum unterstützt werden, mit minimalem Bandbreitenbedarf.

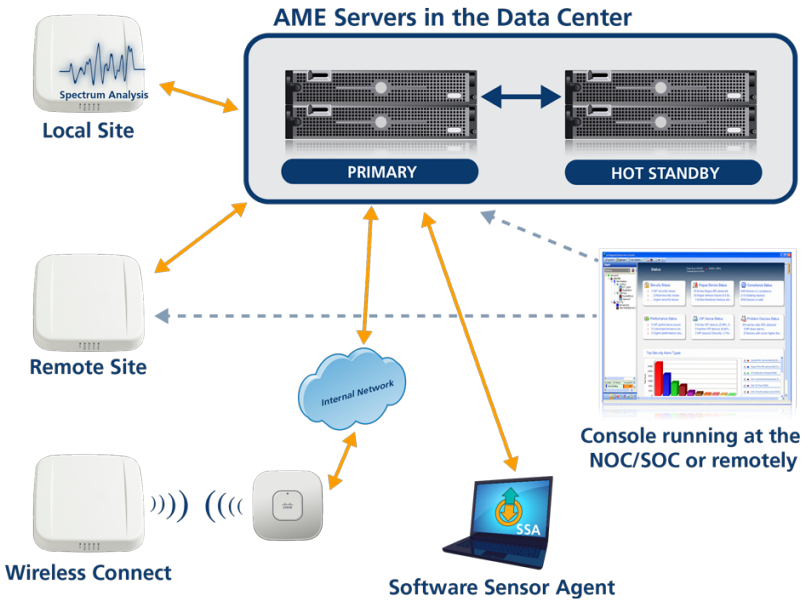
Höchste Systemwiderstandsfähigkeit
Die Verarbeitung auf der Sensor-Ebene bedeutet, dass jeder Sensor weiterhin die Sicherheitsregelung durchsetzt, selbst wenn die Verbindung mit dem Server für mehr als 24 Stunden unterbrochen ist. Hot-Standby-Serversoftware (inbegriffen) ermöglicht einen vollständig redundanten Datenzentrumsbetrieb für maximale drahtlose Sicherheit.

Auf Korrelation ausgelegt
Der AirMagnet Enterprise-Server führt fortwährend eine Analysekorrelation aller Sensoren durch, was sicherstellt, dass Informationen aus dem gesamten Unternehmen jederzeit koordiniert werden.



Benachrichtigungsoptionen

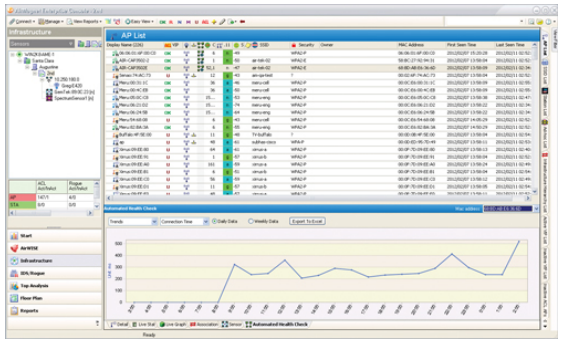
AirMagnet-Sensor



AirMagnet Enterprise-System

Leistungsoptimierung und Problembehandlung

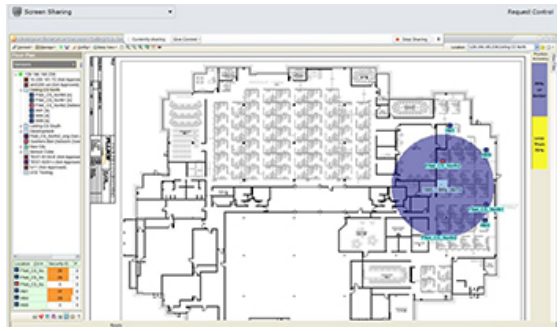
Leistung und Zuverlässigkeit eines WLAN stehen oft in direktem Bezug zum Wert, den das WLAN für eine Organisation hat. Mithilfe der fortlaufenden technologischen Innovationen von AirMagnet Enterprise wurden drahtlose Netzwerküberwachungslösungen entwickelt, mit denen IT-Fachleute WLAN-Probleme erkennen und beheben können, bevor sie Endbenutzer beeinträchtigen. Durch den auf die Grundursache eines Problems ausgerichteten Ansatz und die Bereitstellung von Benutzer-Tools zur umgehenden Problembehebung stellt AirMagnet sicher, dass WLANs zuverlässig geschäftskritische Anwendungen unterstützen.



Leistungstestergebnisse der automatischen Zustandsprüfung

AirMagnet Enterprise stellt eine Sicherheitslösung des Spektrums 24x7 zur Verfügung, die Kunden bevollmächtigt, vereinheitlichte nicht drahtlose (Mobilfunk und Wi-Fi) Zonen durchzusetzen. Sie bietet Entdeckung, Überwachung und Sanierung der Spektrumstätigkeit in einem breiten Frequenzbereich an, der 3G, 4G LTE und CDMA umfasst. Tätigkeit durch Mobilfunk-Geräte wie Mobiltelefone und Störsender wird aufgespürt und berichtet. AirMagnet Enterprise überwacht und berichtet des Weiteren 4 Arten von Sicherheitsverletzungen durch Mobilfunk:

- Mobilfunkaktionen, z. B. Anrufe von einem spezifischen Mobilfunknetz getätigt
- Störungsaktionen durch Mobilfunk, z. B. Mobilfunk-Störsender
- Nicht mit Mobilfunk in Verbindung stehende Energieaktionen, z. B. Veranstaltungen, die außerhalb der zugeteilten Mobilfunk-Bandbreite des Landes stattfinden
- Mobilfunkaktionen der Basisstation, z. B. Basisstationsleuchtfeuer
- Lage von Mobilfunk-Ereignis
- Informationen über Mobilfunkbetreiber bereitstellen

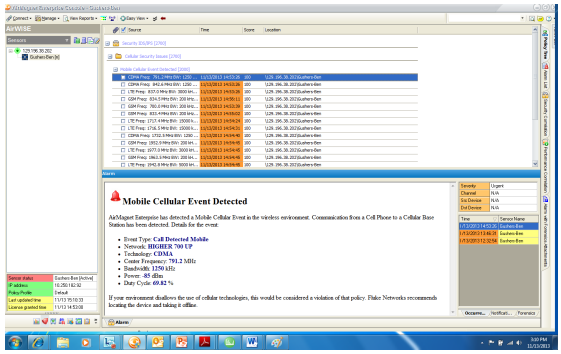


Überwachung von Mobilfunkstandort

Für weitere Analyse können Benutzer auf den eingebauten Mobilfunk-Spektralanalysator des Sensors zugreifen. Dies vermeidet teure Anfahrten und verkürzt die Lösungszeiten.

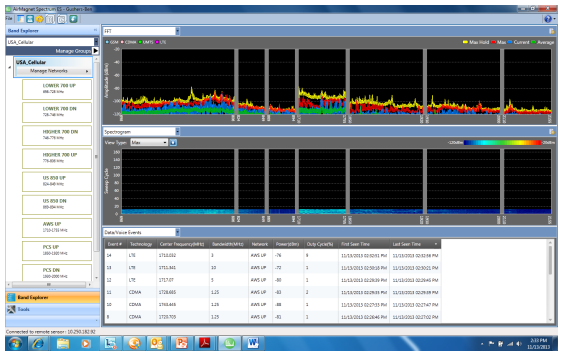
Ermitteln von Ausfällen und entstehenden Problemen, noch bevor Benutzer betroffen sind
Durch die automatische Zustandsprüfung (Automated Health Check, AHC) können die Sensoren und Software-Sensor-Agenten von Air Magnet Enterprise die vollständige WLAN-Anbindung vom WLAN-Link bis zu den Applikationsservern oder dem Internet aktiv testen und prüfen. Dabei erkennen Sie automatisch kritische Ausfälle oder Leistungsabfälle im Netzwerk und lokalisieren präzise die Fehlerquelle. Die Sensoren, die für den AHC verwendet werden, bieten eine Analyse aus Client-Sicht, da sie sich vollständig im Netzwerk authentifizieren und es auf Probleme untersuchen, die mit WLAN-Fehlern oder anderen Netzwerkressourcen zusammenhängen. Dadurch erhalten Netzwerkingenieure unmittelbar genaue Informationen zur Ursache von Problemen, sodass sie diese oft beheben können, noch bevor Benutzer betroffen sind.

Umfassende WLAN-Analyse
AirMagnet Enterprise identifiziert Leistungsprobleme, wie z. B. Datenverkehrsüberlastung, überlastete Geräte oder Kanäle, fehlerhafte Gerätekonfiguration, Kollisionen, Roaming-Probleme, QoS-Probleme sowie Komplikationen bei der Interaktion zwischen 802.11a/b/g/n-Geräten, und generiert einen entsprechenden AirWISE-Alarm. Mithilfe der Tools für die 802.11n-Optimierung können Netzwerkingenieure sicherstellen, dass ihre Investitionen in das WLAN-Netzwerk auch die gewünschte praxisorientierte Leistung für den Benutzer erzielen.



AirWISE-Alarm mit Mobilfunk-Sicherheitsaktionen

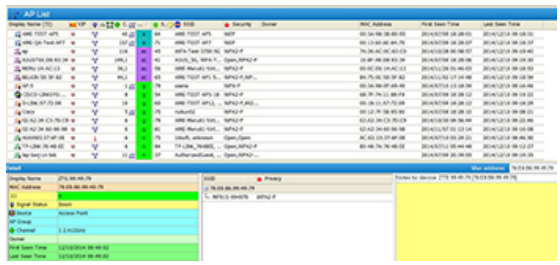
Ausführliche HF-Störungsanalyse
Bei AirMagnet Enterprise handelt es sich um das einzige WLAN-Überwachungssystem, das eine spezielle Spektralanalysehardware im Sensor unterstützt, um die genauste und umfassendste HF-Störungsanalyse und Remote-Echtzeitanalyse zu gewährleisten. Die Umgebung wird 100 Prozent der Zeit über 2.4-GHz- als auch über 5-GHz-Wi-Fi-Bänder gescannt, und Störungsquellen, wie Videokameras, schnurlose Telefone oder Mikrowellen, die die Leistung des WLANs ernsthaft beeinträchtigen können, werden speziell klassifiziert.


Mobilfunk-Spektrumanalysator mit Sicherheitsaktionen

Remote-Fehlersuche in Echtzeit
AirMagnet Enterprise ermöglicht es IT-Fachleuten, Probleme mit dem drahtlosen Netzwerk entfernt und dadurch schneller zu beheben. Außerdem werden so kostspielige Anfahrten vermieden. AirMagnet Enterprise-Sensoren umfassen eine Oberfläche für die Echtzeit-Analyse. Diese basiert auf AirMagnet Wi-Fi Analyzer und Spectrum XT. Mitarbeiter können so die Auslastung und die Bandbreite einsehen, Echtzeit-Entschlüsselungen anzeigen, Fehler bei der Benutzeranbindung sowie HF-Störungen beheben, ohne ihren Arbeitsplatz verlassen zu müssen.

802.11ac-Analyse
AirMagnet Enterprise bietet 802.11ac-Analysefunktionen, mithilfe vorhandener Sensoren Serie 4 von SmartEdge. AirMagnet Enterprise lässt sich für folgende Leistungen mit 802.11ac-fähigen AccessPoints integrieren:

- Nachweis von 802.11ac AccessPoints
- 802.11ac-Frame-Analyse
- Feststellung und Blockierung fremder 802.11ac-Geräte


Auflistung von Zugriffspunkten

NETSCOUT

Einfaches Management auf Richtlinienbasis

Mit zunehmender Wi-Fi-Nutzung wird es für Netzwerkverwalter und WLAN-Verantwortliche zunehmend wichtig, die Masse an Wi-Fi-Daten und -Geräten zu verringern und nur kritische Daten zu erfassen. AirMagnet Enterprise ermöglicht dies über Tools, die einfach neue Wi-Fi-Geräte klassifizieren, Netzwerkprobleme bewerten und priorisieren und rechtzeitig Daten an Netzwerkmitarbeiter und Managementsysteme weiterleiten.

Automatische Geräteklassifizierung

Die Geräteklassifizierungs-Engine von AirMagnet Enterprise ermöglicht Benutzern, Wi-Fi-Geräte schnell und präzise als nicht autorisiert, Nachbargeräte, überwacht oder genehmigt einzuordnen. Klassifizierungsregeln sind integrierte und logische Sätze und boolesche Regeln für die Klassifizierung von Geräten basierend auf Verkabelungs- und Nachverfolgungsstatus, Gerätehersteller, Sicherheitseinstellungen, Signalpegel, Assoziierungsverlauf und einer Vielzahl sonstiger Faktoren. Über das System können Manager auch neue Regeln vor ihrem Einsatz einsehen und so Probleme beheben sowie ermitteln, welche Geräte neu klassifiziert werden.

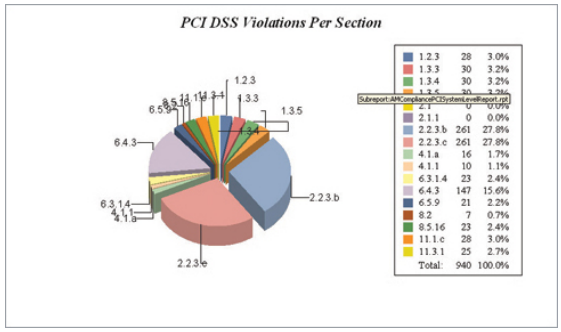
Ermittlung von kritischen Daten

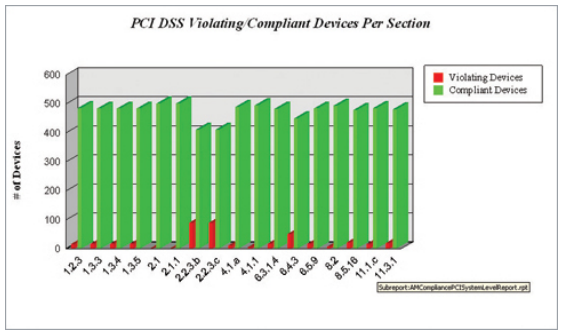
In der Übersicht von AirMagnet Enterprise werden geschäftskritische Daten aller wichtigen Positionsrollen angezeigt, darunter wichtige Sicherheitsprobleme, Leistungsprobleme, problematische Geräte und Konformitätsprobleme. Alle Bedrohungen werden korreliert und anhand benutzergesteuerter Richtlinien bewertet. So können Mitarbeiter wichtige Ereignisse umgehend erkennen und priorisieren sowie Geräte identifizieren, die mehrere Probleme verursachen.

Benutzerausrichtung

Das System umfasst auch Konzepte für VIP-Benutzer oder -Geräte, wodurch Mitarbeitern Alarmmeldungen bezüglich essenzieller Ressourcen priorisieren können. Gleichzeitig werden Ereignisse anhand ihrer Auswirkung auf das Netzwerk eingestuft, sodass Mitarbeiter Probleme mit Auswirkungen auf viele Benutzer vor Problemen mit einer geringeren Benutzerbeeinträchtigung behandeln können.

Zentrale Übersicht der wichtigsten WLAN-Probleme





Zusammenfassung der PCI-Compliance

Berichterstattung und Konformität

Konformitätsberichte

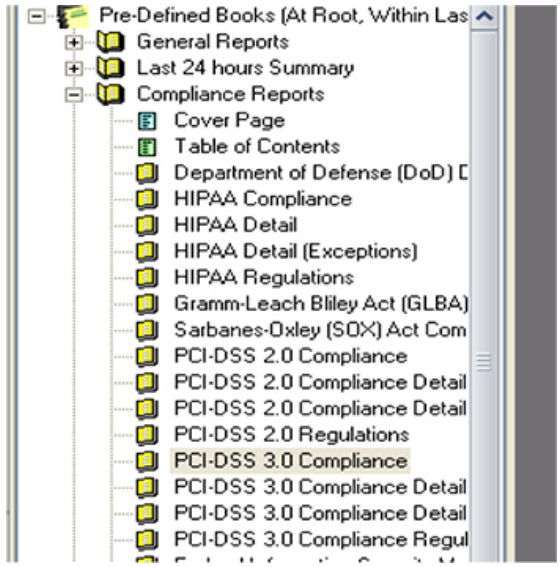
AirMagnet Enterprise liefert detaillierte Konformitätsberichte, die eine Vielzahl von Richtlinienstandards abdecken, einschließlich Sarbanes-Oxley, HIPAA, PCI, DSS GLBA, DoD 8100.2, ISO 27001, BASEL 2 und CAD3. Berichte liefern eine schrittweise Pass/Fail-Einschätzung jedes Standardabschnitts. Entsprechend stehen IT-Mitarbeitern bei Konformitätsprüfungen sofort die einschlägigen Daten bereit, wodurch die Prüfungszeiten minimiert werden.

Integrierte Berichterstattung

Die integrierte Berichterstattungs-Engine von AirMagnet Enterprise vereinfacht die Erstellung von professionell angepassten Berichten unabhängig von Standort oder Zeitbereich. Die Berichte decken alle Management-Bereiche ab, einschließlich Mobilfunk-Sicherheitsaktionen, HF-Statistiken, Geräteberichten, Sicherheits- und Leistungsberichten. Berichte können automatisch in regelmäßigen Intervallen durchgeführt und Entscheidungsträgern per E-Mail zugestellt werden.

PCI 3.0-Konformität

AirMagnet Enterprise PCI 3.0-konforme Berichte identifizieren und liefern automatisch verwertbare Ergebnisse und verweisen auf die Bereiche, auf die man sich zu konzentrieren hat, um mit den PCI 3.0-Normen konform zu werden.



PCI 3.0 Bericht

Bestellinformationen	
Modell	**Beschreibung**
AM/A5505	Unternehmenskonsole und Serversoftware, unlimitierte Anzahl an Sensoren
AM/A5115	Unternehmensserverlizenz für 802.11n-Funktionen, unlimitierte Anzahl an Sensoren
AM/A5106	Unternehmensserverlizenz für Spektralanalysefunktionen, unlimitierte Anzahl an Sensoren
AM/A5311G	AirMagnet Enterprise-Serverlizenz für Software Sensor Agent (100)
AM/A5630G	AirMagnet Enterprise-Serverlizenz für Automated Health Check (AHC)
SENSOR4-R1S1W1-E	AirMagnet Sensor, Mobilfunkspektrum, 4. Generation, 1 x 11n Funk, externe Antenne
SENSOR4-R1S0-I	AirMagnet Sensor, 4. Generation, 1 x 11n Funk, interne Antenne
SENSOR4-R1S1-I	AirMagnet Spectrum, 4. Generation, 1 x 11n Funk, interne Antenne
SENSOR4-R2S0-I	AirMagnet Sensor, 4. Generation, 2 x 11n Funk, interne Antenne
SENSOR4-R2S1-I	AirMagnet Spectrum, 4. Generation, 2 x 11n Funk, interne Antenne
SENSOR4-R1S0-E	AirMagnet Sensor, 4. Generation, 1 x 11n Funk, externe Antenne
SENSOR4-R1S1-E	AirMagnet Spectrum, 4. Generation, 1 x 11n Funk, externe Antenne
SENSOR4-R2S0-E	AirMagnet Sensor, 4. Generation, 2 x 11n Funk, externe Antenne
SENSOR4-R2S1-E	AirMagnet Spectrum, 4. Generation, 2 x 11n Funk, externe Antenne
AM/A5032	Power-Injektor für AirMagnet-Sensoren
CABLEKIT-SENSOR4	Konsolen-Kabelkit für Sensoren-4Series
Gold Support (variierend)	Gold Support Services für jedes Sensoren-Modell, 1 Jahr und 3 Jahre

Hinweis: Das AirMagnet Enterprise-System erfordert einen Server bzw. eine Datenbank. Benutzer können von NetScout einen Server erwerben oder eigene Server verwenden, sofern diese den nachstehenden Systemanforderungen entsprechen.

Server-Mindestsystemanforderungen	
Betriebssystem	Microsoft Windows Server 2012 R2 / VMware vSphere
Prozessor	Intel Xeon CPU Serie E5
Speicher	16 GB/ 1600 MHZ oder schneller
Festplattenspeicher	200 GB / 10,000 RPM SAS

Hinweis: Weitere Anforderungen gelten möglicherweise, wenn der Server für die Unterstützung bestimmter Systemkonfigurationen angepasst werden muss. Weitere Informationen finden Sie unter ***www.enterprise.netscout.com***.

Zertifikate
Common Criteria Evaluation Assurance Level 2
U.S. FAVs 140-2 Zertifikation (trifft nicht auf SENSOR4-R1S1W-E) zu