## Спецификации: AirMagnet Enterprise

*AirMagnet Enterprise — это масштабируемое решение для круглосуточного мониторинга производительности и безопасности WLAN, которое осуществляет упреждающее обнаружение и локализацию всех видов угроз безопасности беспроводных сетей, поддерживать корпоративные политики, предотвращать возникновение проблем производительности, а также проверять всю свою инфраструктуру WiFi на соответствие различным регулирующим документам.*

- *Непрерывное сканирование пакетов и РЧ-спектра, позволяющее не пропустить серьезных угроз*
- *Круглосуточный мониторинг проблем возможности подключения, таких как помехи канала, покрытие канала, искаженные пакеты, атаки повторной авторизации, чтобы обеспечить оптимальную и надежную доступность беспроводной сети*
- *Автоматизированная проверка состояния (AHC) упреждающе производить мониторинг и уведомляет о любых проблемах производительности беспроводной точки доступа*
- *Возможность удаленной диагностики и решение проблем за меньшее время*
- *Технологию динамического обновления списка уязвимостей (DTU), обеспечивает непрерывную защиту сети по мере появления новых угроз*

### AirMagnet Enterprise

Централизованная система обнаружения/предотвращения беспроводных вторжений (WIDS/WIPS) от AirMagnet Enterprise защищает вашу беспроводную среду путем автоматического обнаружения, блокирования, трассировки и обнаружения любой угрозы на всех каналах Wi-Fi. Она содержит непревзойденный набор оповещений о событиях, эскалации, удаленного устранения неполадок, анализа данных, проверки состояния сети и профессиональной PCI и других отчетов о соответствии политике. Конечным результатом является единая система, которая сканирует вашу среду 100% времени для обеспечения надежной и безопасной работы вашей сети WLAN и удовлетворяет потребности пользователей и приложений.

## AirMagnet Enterprise – полноценная защита Wi-Fi и сотовой связи

AirMagnet Enterprise защищает беспроводные сети от всех угроз, совмещая самый тщательный в отрасли мониторинг с передовыми методами исследования, анализа и нейтрализации угроз.

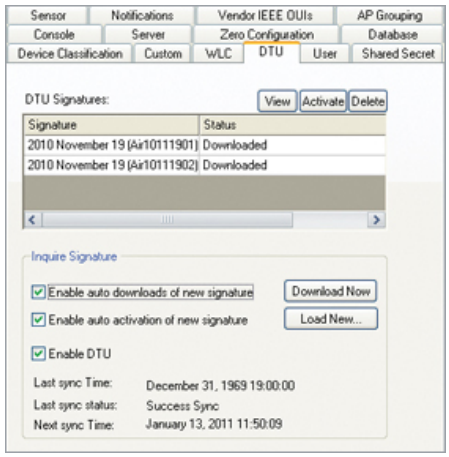
**Полная видимость**

В отличие от точек доступа (AP), продукт AirMagnet Enterprise сканирует все возможные каналы 802.11 (включая 200 расширенных канала) и каналы сотового спектра, обеспечивая отсутствие слабых мест для сокрытия неавторизованных или причиняющих помех устройств. AirMagnet Enterprise также предоставляет сотовый спектральный анализ, который обнаруживает и классифицирует атаки подавления РЧ, устройств Bluetooth и многих других типов передатчиков, отличных от стандарта 802.11, например, беспроводные камеры и сотовые телефоны.

**Лучшие в отрасли функции обнаружения угроз безопасности**

Команда исследования безопасности AirMagnet постоянно изучает новейшие приемы взлома, тенденции и потенциальные уязвимости, для того чтобы заранее обезопасить организации от вновь возникающих угроз. Наша технология динамического обновления списка уязвимостей (DTU) ускоряет создание, автоматизацию и немедленное развертывание новых сигнатур угроз. Новые сигнатуры DTU могут быть развернуты сразу же без последствий для работы системы, обеспечивая уникальную основу для самых современных средств обеспечения безопасности WLAN от более 230 угроз.

Механизм AME AirWISE® постоянно анализирует все беспроводные устройства и трафик, используя комбинацию инспекции кадра, потокового анализа, статистического моделирования, анализа РЧ и обнаружения аномалий.




*Динамическое обновление списка угроз*

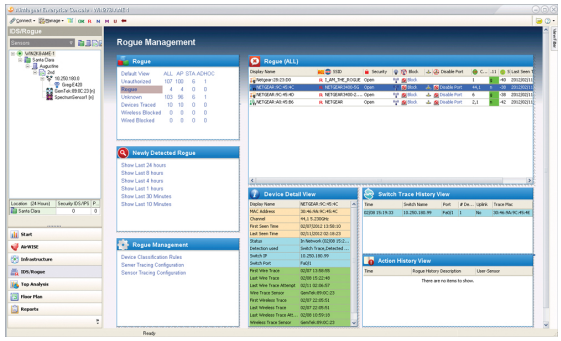
NETSCOUT

## Автоматическое реагирование и защита сети

AirMagnet Enterprise предоставляет полный арсенал функций исследования и нейтрализации угроз, которые могут быть активированы при помощи политики, что гарантирует быстрое и точное определение проблем WLAN с автоматическим запуском соответствующих защитных механизмов.

**Отслеживание угроз, блокирование/подавление и создание карты угроз**

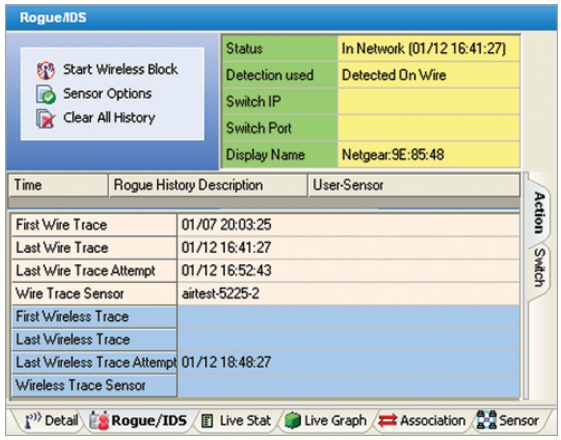
Все устройства отслеживаются с использованием набора проводных и беспроводных методов трассировки с тем, чтобы быстро и надежно определять, подключено ли устройство к сети. Система использует недавно расширенный набор сложных методов, включая использование SNMP, автоматизированного открытия выключателя и анализа аппаратных средств и трафика, чтобы гарантировать точную, быстро отслеживаемую топологию сети.




*Управление несанкционированными устройствами*

Угрозы могут быть вручную или автоматически устранены с помощью сочетания проводного и беспроводного подавления угроз. Беспроводное блокирование нацелено на угрозу в источнике и не позволяет целевому беспроводному устройству осуществлять любые беспроводные подключения. При проводном блокировании автоматически закрывается проводной переключатель, в котором была обнаружена угроза.

Все угрозы и устройства, их вызывающие, могут быть указаны на карте или плане этажа, чтобы включать сигнал тревоги в зависимости от местоположения устройства.




*Обнаружено и отслежено несанкционированное устройство*

**Расследование событий**

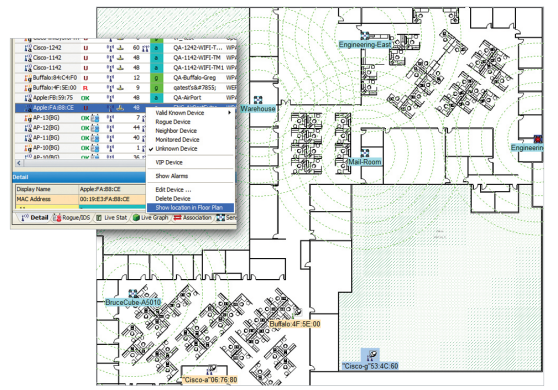
AirMagnet Enterprise захватывает как собственно кадры 802.11, так и события РЧ-спектра, позволяя сотрудникам соответствующей квалификации подробно расследовать событие в любой момент времени.

**Уведомления и интеграция**

Специалисты по управлению имеют доступ более чем к десятку механизмов уведомления и передачи на следующий уровень обслуживания, что облегчает оповещение конкретных сотрудников о возникновении неполадок или интеграцию данных о событиях в беспроводной сети в более крупные корпоративные службы и системы управления.

**Гибкая архитектура размещения сенсоров**

Сенсор семейства SmartEdge Series 4 конструктивно рассчитан на установку трех радиопередатчиков, включая два передатчика 802.11n 3x3 MIMO Wi-Fi и отдельный передатчик для анализа сотового или Wi-Fi спектра. Такая конструкция позволяет сенсору установить беспроводное соединение, устраняя необходимость в дорогостоящей прокладке кабелей Ethernet, или одновременно проводить мониторинг и выполнять тест производительности.




*Определение местоположения несанкционированного устройства на карте этажа*

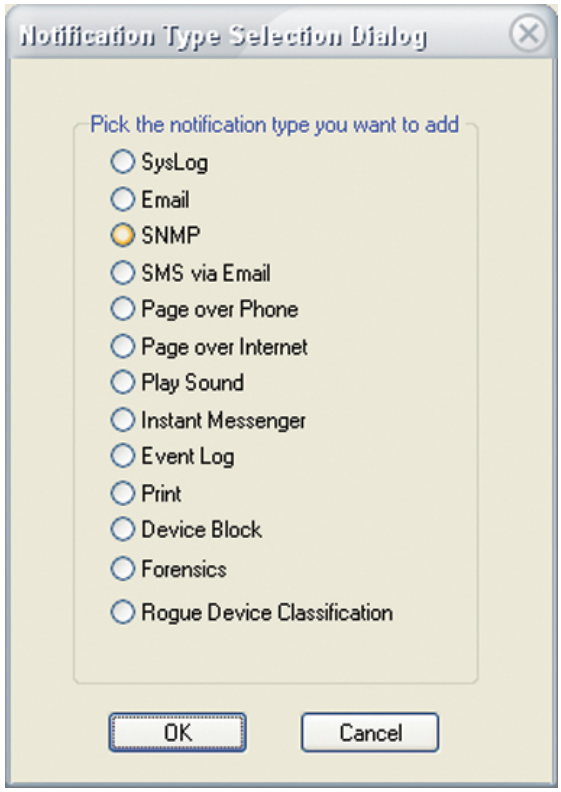
## Лучшая в своем классе архитектура безопасности

AirMagnet Enterprise обеспечивает единственное в отрасли соответствующее принятым стандартам решение защиты критически важных приложений. Это – единственная система для обеспечения надежности в каждом компоненте с помощью отказоустойчивых образов начальной загрузки в каждом датчике и автоматических лицензий на отказоустойчивость сервера, которые стандартно поставляются с системой. Кроме того, датчики AirMagnet Enterprise могут работать как полностью независимые узлы IDS/IPS, обнаруживающие и устраняющие угрозы без потери информации, даже если сетевое подключение к серверу потеряно на несколько дней. Дополнительные уникальные преимущества архитектуры AirMagnet Enterprise:

**Масштабируемость массива**
Благодаря интеллектуальным датчикам, которые локально анализируют состояния Wi-Fi, сотовые и RF, может поддерживаться больше чем 1,000 датчиков с помощью единственного централизованного сервера в центре обработки данных, для которого требуется минимальная пропускная способность сети.

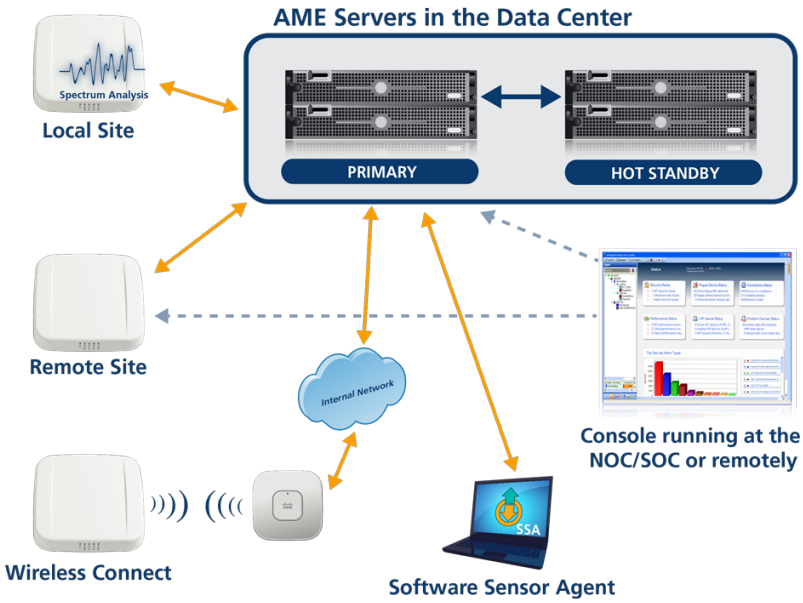
**Высочайшая производительность системы**
Обработка на уровне датчика означает, что каждый датчик продолжает применять политику безопасности, даже если связь с сервером потеряна на более чем 24 часа. """Горячее"" резервирование серверного ПО (включено в поставку) обеспечивает полную отказоустойчивость ЦОД и максимальную защиту беспроводной сети."

**Корреляция данных**
Сервер AirMagnet Enterprise непрерывно осуществляет корреляционный анализ данных со всех сенсоров, гарантируя постоянную координацию данных по всей корпоративной сети.




*Опции рассылки уведомлений*

*Сенсор AirMagnet*

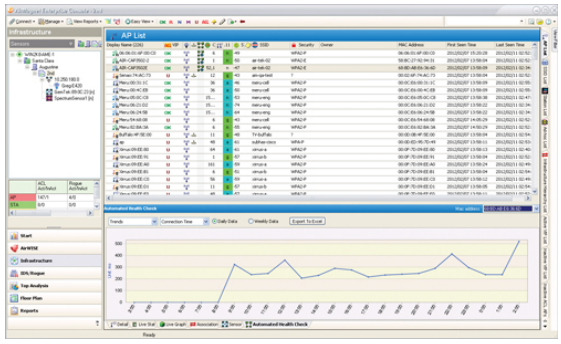



*Сuстема AirMagnet Enterprise*

NETSCOUT

## Оптимизация производительности и устранение неисправностей

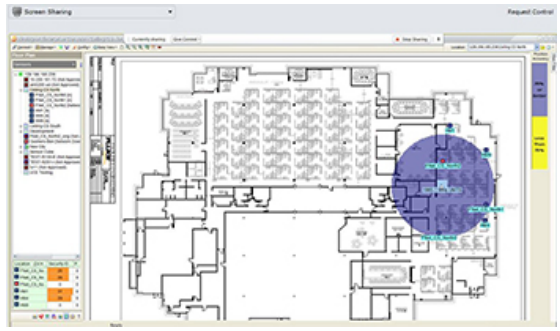
Производительность и надежность WLAN часто напрямую связаны с ценностью беспроводной сети для организации. Технология AirMagnet последовательно держалась на переднем крае инноваций, внедряясь в решения мониторинга беспроводных сетей, которые помогают специалистам в области ИТ идентифицировать и решать проблемы WLAN до того, как они скажутся на работе пользователей. Выясняя первопричины каждой неполадки и снабжая пользователей критические важными средствами, необходимыми для решения возникающих проблем, AirMagnet Enterprise гарантирует надежную поддержку жизненно важных для бизнеса приложений со стороны беспроводной сети.



*Результаты автоматической проверки состояния*

AirMagnet Enterprise обеспечивает круглосуточное решение для безопасности спектра, позволяющее клиентам определить объединенные сотовые и Wi-Fi зоны. Оно предлагает обнаружение, мониторинг и устранение проблем деятельности спектра в широком частотном диапазоне, который включает 3G, 4G LTE и CDMA. Деятельность сотовых устройств, таких как сотовых телефонов и глушителей прослеживается и о ней составляются отчеты. Далее AirMagnet Enterprise производит мониторинг и составляет отчеты о 4 типах событий нарушения безопасности сотовой связи:

- События мобильной сотовой связи, например, звонки, исходящие из определенной сотовой сети
- События помех сотовой связи, например, сотовые глушители
- События, не относящиеся к сотовой деятельности, например, события, происходящие за определенной полосы пропускания страны
- События сотовой связи базовой станции, например, маяки базовой станции
- Местоположение сотовых событий
- Предоставьте информацию об операторе сотовой связи

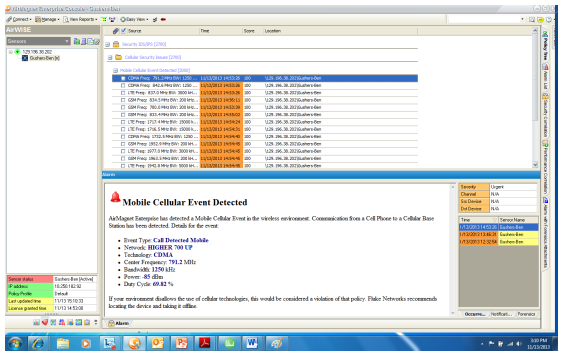


*Монитор местоположения сотовой связи*

Для дальнейшего анализа пользователи могут получить доступ к встроенному анализатору сотового спектра датчика. Это позволяет избежать дорогостоящих выездов на объект и сократить время решения проблемы.

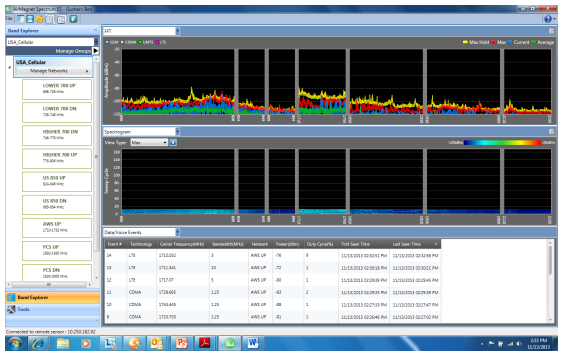
**Обнаружение перебоев в работе и сопутствующих проблем до того, как они скажутся на работе пользователей**
Снабженные функцией автоматической проверки состояния (AHC), сенсоры и программные агенты AirMagnet Enterprise активно тестируют соединение от беспроводного подключения до серверов приложений или Интернета, автоматически обнаруживая перебои или снижение производительности сети и точно указывая источник проблем. Выполняя тесты AHC, сенсоры предоставляют информацию с точки зрения пользователя, поскольку они полностью авторизуются в сети и активно обнаруживают проблемы, которые могут быть связаны со сбоями в работе как беспроводного участка сети, так и других ее компонентов. Это позволяет сетевым специалистам мгновенно получать конкретную информацию о причине неисправности, с тем чтобы они могли начать действовать до того, как это скажется на работе пользователей.

**Комплексный анализ беспроводной сети**
AirMagnet Enterprise идентифицирует проблемы производительности сети, связанные с такими причинами, как чрезмерный трафик, перегрузка устройств и каналов, неверные настройки устройств, коллизии, проблемы с роумингом, нарушение QoS, а также сложности взаимовлияния между устройствами стандартов 802.11a/b/g/n, и генерирует соответствующие предупреждения AirWISE. Средства оптимизации 802.11n позволяют сетевым специалистам обеспечивать ожидаемую отдачу от инвестиций в беспроводную сеть и качество обслуживания пользователей.




*Тревога AirWISE с событиями безопасности сотовой связи*

**Обширный анализ РЧ-помех**
AirMagnet Enterprise является единственной системой мониторинга беспроводной сети с поддержкой специализированного оборудования в сенсоре для анализа РЧ-спектра, обеспечивающей максимально полное и точное обнаружение РЧ-помех, а также удаленный анализ в масштабе реального времени. Производится непрерывное сканирование в частотных диапазонах 2,4 ГГц и 5 ГГц, отдельно классифицируются источники помех, такие как видеокамеры, радиотелефоны и микроволновые печи, которые могут серьезно влиять на производительность беспроводной сети.

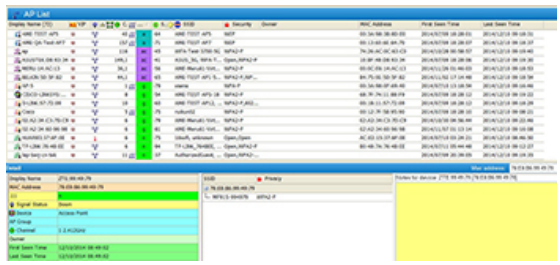


*Анализатор сотового спектра с событиями безопасности*

**Удаленный поиск и устранение неисправностей в реальном времени**
AirMagnet Enterprise позволяет ИТ-специалистам удаленно выполнять поиск неисправностей беспроводных сетей, что позволяет быстрее устранять неполадки и обойтись без дорогостоящих выездов на объект. Сенсоры AirMagnet Enterprise содержат интерфейс анализа в масштабе реального времени, аналогичный анализаторам AirMagnet Wi-Fi Analyzer и Spectrum XT, что позволяет сотрудникам отслеживать использование пропускной способности, просматривать декодированные данные в реальном времени, решать проблемы подключения пользователей и устранять РЧ-помехи, не покидая рабочего места.

**Анализ 802.11ac**
AirMagnet Enterprise предоставляет возможности анализа 802.11ac, используя существующие датчики серии SmartEdge 4. AirMagnet Enterprise интегрируется с точками доступа, поддерживающими стандарт 802.11ac, чтобы обеспечить:

- Обнаружение точек доступа 802.11ac
- Анализ кадров 802.11ac
- Обнаружение и блокировка неавторизованных устройств стандарта 802.11ac



*Список точек доступа*

## Простое управление на основе политик

По мере распространения Wi-Fi неизбежно возрастает важность повышения эффективности средств, применяемых специалистами по управлению сетями и специалистами по беспроводным сетям. Им необходим инструмент, позволяющий пробиться сквозь массивы данных и устройств Wi-Fi и обнаружить наиболее значимую информацию. AirMagnet Enterprise делает это при помощи средств, без труда классифицирующих новые устройства Wi-Fi, оценивающих и определяющих приоритеты событий в сети и своевременно информирующих персонал по обслуживанию сетей и сотрудников систем управления.

**Автоматическая классификация устройств**

Заложенный в AirMagnet Enterprise механизм классификации устройств позволяет пользователям легко и точно разделять устройства Wi-Fi на несанкционированные, соседние, разрешенные или наблюдаемые. Правила классификации созданы с использованием простых и понятных выражений, а также логических правил, и классифицируют устройства на основе результатов проводной трассировки, информации о производителе, настроек безопасности, уровня сигнала, журнала подключений и множества других факторов. Кроме того, система позволяет администраторам предварительно просматривать новые правила, с тем чтобы увидеть, какие именно устройства будут переквалифицированы, и перехватить возможные проблемы до того, как политика будет применена.

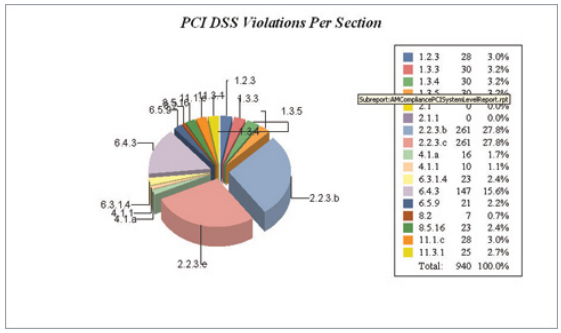
**Поиск важной информации**

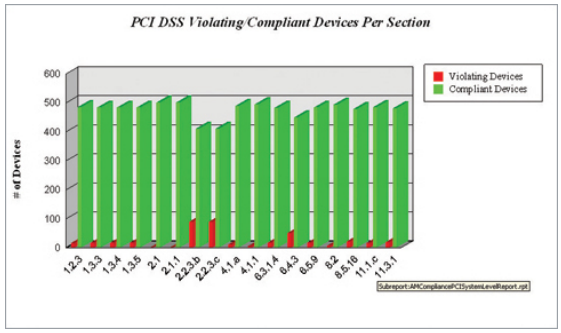
На инструментальной панели AirMagnet Enterprise отображается самая важная информация обо всех рабочих ролях, включая важнейшие события по безопасности, проблемы с производительностью, неполадки устройств и вопросы несоответствия стандартам. Все угрозы группируются и оцениваются в соответствии с управляемыми пользователями политиками. Это позволяет персоналу быстро находить и определять приоритеты важных событий, а также видеть устройства, являющиеся источниками множества проблем.

**Внимание к пользователям**

Кроме того, система имеет концепцию VIP-пользователей или устройств, что позволяет сотрудникам расставить приоритеты угроз, влияющих на важнейшие ресурсы. Подобным же образом оценивается влияние событий на сеть, что позволяет сотрудникам указать приоритетность неполадок, влияющих на множество пользователей, в сравнении с менее значимыми сбоями.


*Вид инструментальной панели с наиболее существенными неполадками WLAN*




*Краткий обзор соответствия PCI*

## Отчетность и соответствие стандартам

**Отчеты о соответствии стандартам**

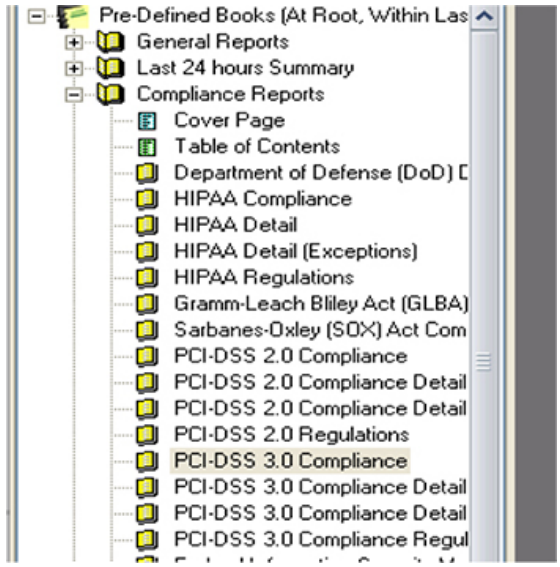
AirMagnet Enterprise выдает детализированные отчеты о соответствии стандартам, содержащие информацию о соответствии множеству стандартов, в том числе: Sarbanes-Oxley, HIPAA, PCI, DSS GLBA, DoD 8100.2, ISO 27001, BASEL 2 и CAD3. Отчеты предоставляют поэтапную оценку прохождения/непрохождения каждого раздела стандарта. В результате сотрудники ИТ-службы могут исключить догадки из процесса аудита на предмет соответствия отраслевым требованиям и завершить работу в мгновение ока.

**Интегрированные отчеты**

Встроенный в AirMagnet Enterprise механизм создания отчетности позволяет с легкостью создавать профессиональные и персонализированные отчеты по любому множеству местоположений или интервалу дат. Отчеты охватывают все сферы управления, включая события сотовой безопасности, статистику по РЧ, отчеты об устройствах, отчеты по безопасности и производительности. Можно запланировать создание и рассылку отчетов на электронные адреса ключевых сотрудников на регулярной основе.

**Соответствие стандартам PCI 3.0**

Отчеты AirMagnet Enterprise о соответствии PCI 3.0 автоматически определяют и обеспечивают актуальные результаты и указывают на области, на которых нужно сосредоточиться для того, чтобы соответствовать требованиям стандартов PCI 3.0.




*Отчет PCI 3.0*

NETSCOUT

| Информация для заказа | |
|---|---|
| **Модель** | **Описание** |
| **AM/A5505** | Консоль управления и ПО Enterprise Server, неограниченное количество сенсоров |
| **AM/A5115** | Лицензия Enterprise Server для функций 802.11n, неограниченное количество сенсоров |
| **AM/A5106** | Лицензия Enterprise Server для спектрального анализа, неограниченное количество сенсоров |
| **AM/A5311G** | Лицензия сервера AirMagnet Enterprise для программного сенсорного агента (100) |
| **AM/A5630G** | Лицензия сервера AirMagnet Enterprise для функции AHC |
| **SENSOR4-R1S1W1-E** | Сенсор AirMagnet, сотовый спектр, 4-е поколение, один модуль 11n, внешняя антенна. |
| **SENSOR4-R1S0-I** | Сенсор AirMagnet, 4-е поколение один модуль 11n, внутренняя антенна. |
| **SENSOR4-R1S1-I** | Спектральный сенсор AirMagnet Spectrum, 4-е поколение, один модуль 11n, внутренняя антенна. |
| **SENSOR4-R2S0-I** | Сенсор AirMagnet, 4-е поколение, модули 2 x 11n, внутренняя антенна. |
| **SENSOR4-R2S1-I** | Спектральный сенсор AirMagnet Spectrum, 4-е поколение, модули 2 x 11n, внутреняя антенна. |
| **SENSOR4-R1S0-E** | Сенсор AirMagnet, 4-е поколение, один модуль 11n, внешняя антенна. |
| **SENSOR4-R1S1-E** | Спектральный сенсор AirMagnet Spectrum, 4-е поколение, один модуль 11n, внешняя антенна. |
| **SENSOR4-R2S0-E** | Сенсор AirMagnet, 4-е поколение, модули 2 x 11n, внешняя антенна. |
| **SENSOR4-R2S1-E** | Спектральный сенсор AirMagnet Spectrum, 4-е поколение, модули 2 x 11n, внешняя антенна. |
| **AM/A5032** | Инжектор питания для сенсоров AirMagnet |
| **CABLEKIT-SENSOR4** | Комплект консольных кабелей для сенсоров серии 4 |
| **Программа технической поддержки Gold Support (различные варианты)** | Услуги по программе технической поддержки для каждой модели сенсора на 1 и 3 года |

**Примечание**. Система AirMagnet Enterprise требует наличия сервера/базы данных. Пользователи могут приобрести сервер у компании NetScout или использовать собственный сервер, соответствующий приведенным ниже требованиям.

| Минимальные требования к серверу | |
|---|---|
| **Операционная система** | Microsoft Windows Server 2012 R2/VMware vSphere |
| **Процессор** | Процессор Intel Xeon E5 |
| **Память** | 16 ГБ/1600 МГц или быстрее |
| **Размер жесткого диска** | 200 ГБ/ {{15 000}} об/мин SAS |

**Примечание**. При необходимости поддержки сервером определенных системных конфигураций могут возникнуть дополнительные требования. Для получения дополнительной информации посетите ***www.enterprise.netscout.com***.

| Сертификация |
|---|
| Гарантия оценки общих критериев 2 уровня |
| Сертификация по федеральному стандарту США по обработке информации 140-2 (не относится к SENSOR4-R1S1W-E) |