FLUKE networks

AirMagnet Enterprise

AirMagnet Enterprise предоставляет масштабируемое решение мониторинга производительности и безопасности WLAN, которое позволяет любой организации осуществлять упреждающее обнаружение и локализацию всех видов угроз безопасности беспроводных сетей, поддерживать корпоративные политики, предотвращать возникновение проблем производительности, а также проверять всю свою WiFi-инфраструктуру на соответствие различным регулирующим документам. Оно реализует круглосуточный мониторинг и защиту WLAN, обеспечивающие следующее:

- *Непрерывное сканирование пакетов и РЧ-спектра, позволяющее не пропустить серьезных угроз*
- *Возможность удаленной диагностики и решение проблем за меньшее время*
- *Технологию динамического обновления списка уязвимостей, обеспечивающую непрерывную защиту сети по мере появления новых угроз*
- *Новые гибкие сценарии развертывания сенсоров с использованием программных агентов в качестве сенсоров позволяют уложиться в любой бюджет*
- *Простая интеграция в существующую инфраструктуру и практические методы снижения нагрузки на сотрудников*

AirMagnet Enterprise предоставляет полную видимость всей беспроводной инфраструктуры, позволяя тем самым ИТ-персоналу любой организации максимально эффективно и с меньшими затратами осуществлять подключение к WiFi пользователей, для которых надежность, безопасность, отказоустойчивость, а также соответствие регулирующим документам являются критическими.

AirMagnet Enterprise – полноценная защита Wi-Fi

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

Полная видимость

AirMagnet Enterprise сканирует все возможные каналы 802.11 (включая 200 дополнительных), исключая наличие "белых пятен", в которых могли бы быть скрыты несанкционированные устройства. AirMagnet Enterprise не просто анализирует Wi-Fi. Благодаря дополнительной функции спектрального анализа он выявляет и классифицирует преднамеренные радиочастотные помехи, устройства Bluetooth и множество типов передатчиков, не относящихся к 802.11, таких, например, как несанкционированные беспроводные видеокамеры.

Лучшие в отрасли функции обнаружения угроз безопасности

Команда исследования вторжений AirMagnet постоянно изучает новейшие приемы взлома, тенденции и потенциальные уязвимости, для того чтобы заранее обезопасить организации от вновь возникающих угроз. Новая технология динамического обновления списка угроз ускоряет создание, автоматизацию и немедленное развертывание новых сигнатур угроз в ядре AirMagnet AirWISE®. Как только новый список угроз готов, его можно развертывать, не оказывая влияния на работу систем, что создает уникальную основу для поддержания самых современных средств поддержания безопасности WLAN в организации.

Ядро AirWISE непрерывно анализирует все беспроводные устройства и трафик, используя комбинацию глубокого разбора кадров, анализа шаблонов трафика с учетом состояний, статистического моделирования, радиочастотного анализа и обнаружения аномалий. Это позволяет обнаруживать сотни специфических угроз, в числе которых несанкционированные и поддельные устройства, DoS-атаки, атаки Man-in-the-Middle, а также самые современные средства взлома и поиска уязвимостей, такие как атаки методом перебора, Karmetasploit и 802.11n fuzzing-атаки.

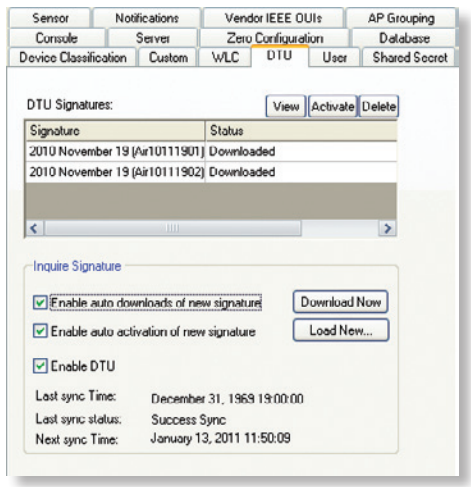

Рис. 1. *Динамическое обновление списка угроз*

Технические данные

Круглосуточный мониторинг производительности и системы обеспечения безопасности WLAN

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

Все устройства отслеживаются с использованием набора проводных и беспроводных методов трассировки с тем, чтобы быстро и надежно определять, подключено ли устройство к проводной сети. Система использует обновленный набор сложных методик, включая использование SNMP, автоматическое обнаружение коммутатора, а также автоматический анализ оборудования и трафика для обеспечения быстрой и точной трассировки любой сетевой топологии.

Блокировка и подавление угроз

Угрозы могут быть нейтрализованы вручную или автоматически при помощи комбинации методов подавления как проводных, так и беспроводных угроз. Методы беспроводной блокировки нацелены на источник угрозы и предотвращают установление каких-либо беспроводных соединений с указанным беспроводным устройством. Методы проводной блокировки автоматически закрывают порты проводного коммутатора, на котором была обнаружена угроза.

Составление карты угроз

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

Расследование событий

AirMagnet Enterprise умеет захватывать как собственно кадры 802.11, так и события РЧ спектра, позволяя сотрудникам с соответствующей подготовкой 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

Использование новых программных агентов в качестве сенсоров позволяет развертывать систему WIPS при любом бюджете с достаточной гибкостью. Будучи установленным на ПК под управлением Windows, программный агент в качестве сенсора обеспечивает базовый уровень защиты в соответствии с требованиями PCI без дорогостоящей необходимости расширения существующей кабельной инфраструктуры. Совместное использование аппаратных сенсоров и программных агентов позволяет подобрать оптимальную комбинацию защитных и аналитических возможностей.

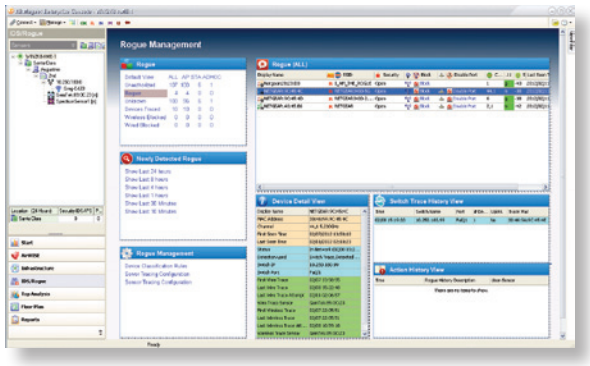

Рис. 2. *Экран "Управление несанкционированными устройствами"*

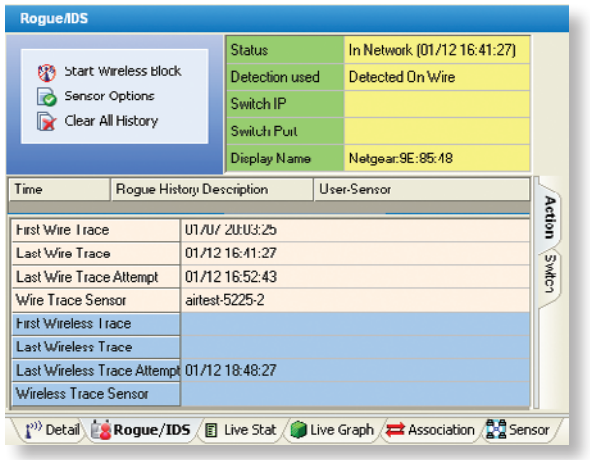

Рис. 3. *Обнаружено и отслежено несанкционированное устройство*

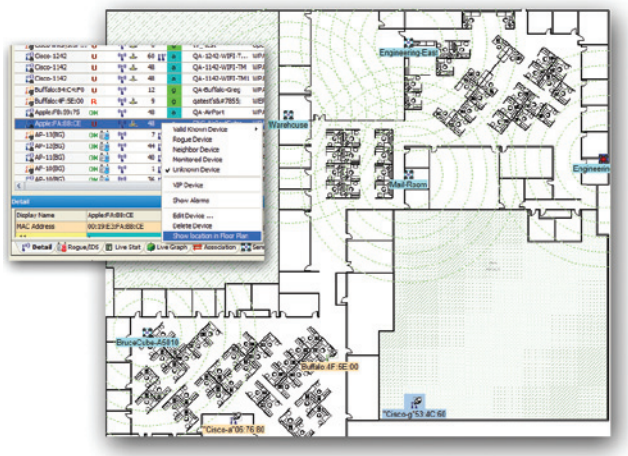

Рис. 4. *Определение местоположения несанкционированного устройства на карте этажа*

Лучшая в своем классе архитектура безопасности

AirMagnet Enterprise предлагает единственное в отрасли соответствующее принятым стандартам решение защиты критически важных приложений. Это единственная система, все компоненты которой отказоустойчивы, имеющая восстановительные загрузочные образы в каждом сенсоре и поставляемая с системой лицензией на автоматическое восстановление сервера. Кроме того, сенсоры AirMagnet Enterprise могут действовать в качестве независимых узлов IDS/IPS, обнаруживающих и устраняющих угрозы без потери информации, даже если сетевое подключение к серверу отсутствует в течение нескольких дней. Дополнительные уникальные преимущества архитектуры AirMagnet Enterprise:

Масштабируемость массива

Благодаря использованию интеллектуальных сенсоров, локально анализирующих параметры Wi-Fi и РЧ, один централизованный сервер, размещенный в ЦОД, может поддерживать до 1000 сенсоров, минимально используя пропускную способность сети.

Высочайшая производительность системы

Обработка данных на уровне сенсоров означает поддержание политики безопасности даже в том случае, когда соединение с сервером отсутствует более 24 часов. "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.

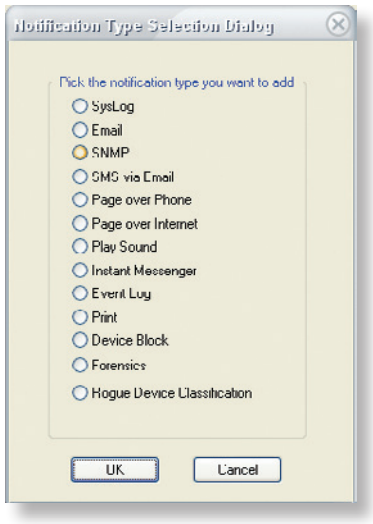

Рис. 5. *Опции рассылки уведомлений*

Рис. 6. *Сенсор AirMagnet*

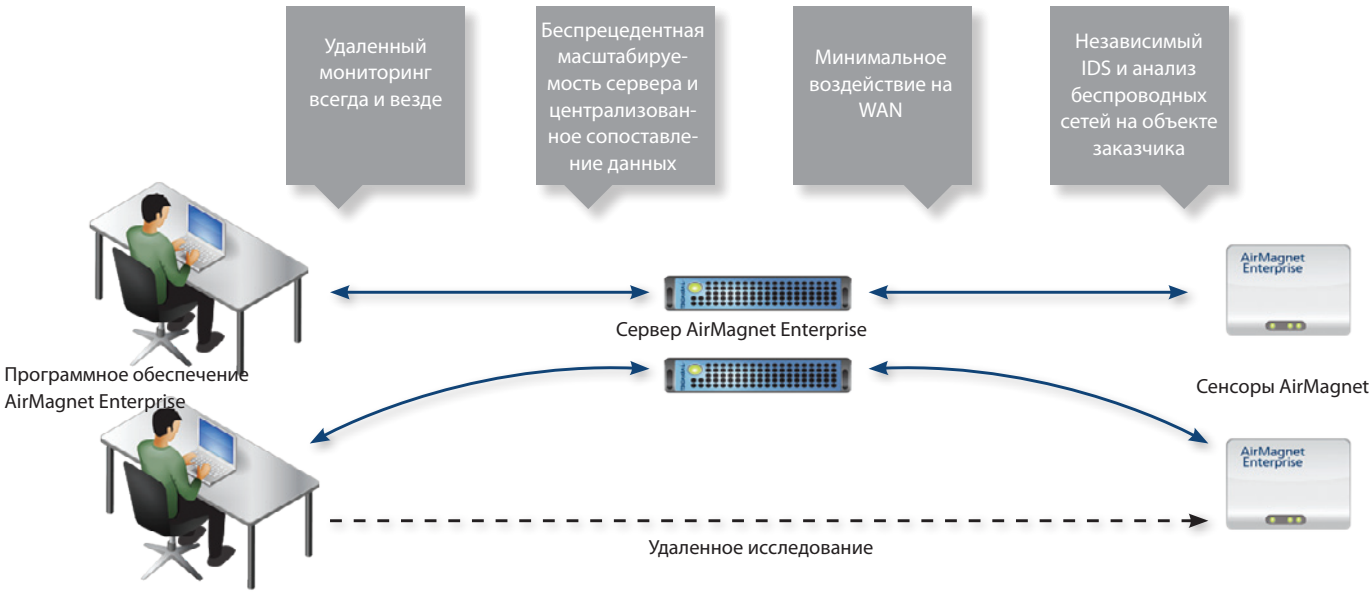

Рис. 7. *Система AirMagnet Enterprise*

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.

Обнаружение перебоев в работе и сопутствующих проблем до того, как они скажутся на работе пользователей

Снабженные новой функцией автоматической проверки состояния (AHC), сенсоры и программные агенты AirMagnet Enterprise теперь могут активно тестировать 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.

Беспрецедентные возможности анализа РЧ-помех

AirMagnet Enterprise является единственной системой мониторинга беспроводной сети с поддержкой специализированного оборудования для анализа РЧ-спектра, обеспечивающей максимально точное и комплексное обнаружение РЧ-помех и 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.

Обнаружение неисправностей в режиме реального времени на удаленных площадках

AirMagnet Enterprise позволяет ИТ-специалистам удаленно устранять неисправности беспроводных сетей, делая это быстрее и 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.

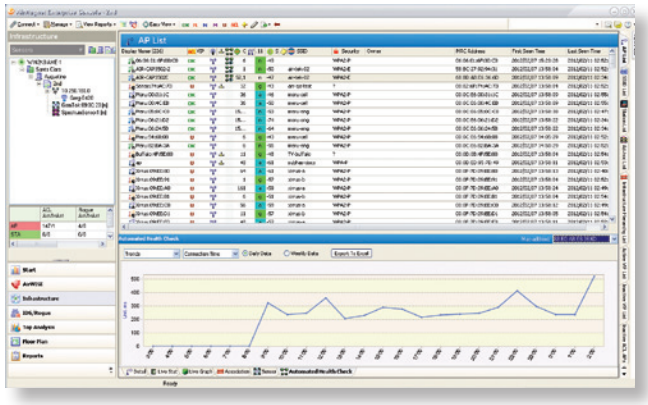

Рис. 8. *Результаты теста проверки состояния производительности*

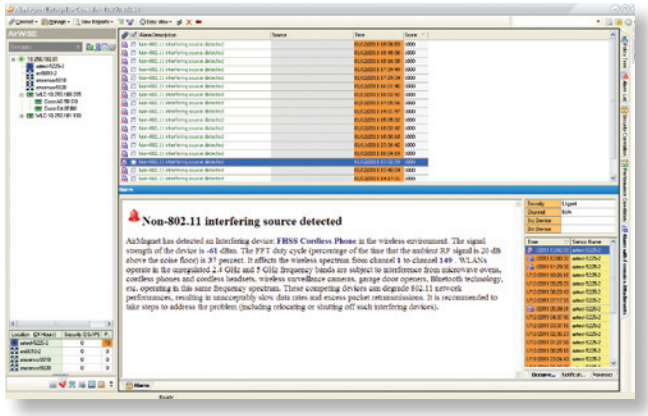

Рис. 9. *Предупреждение AirWISE с детальной информацией об источнике помех*

Рис. 10. *Интерфейс удаленного анализа сенсором сетей Wi-Fi в режиме реального времени*

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.

Рис. 11. *Вид инструментальной панели с наиболее существенными неполадками WLAN*

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, GLBA, DoD 8100.2, ISO 27001, BASEL 2 и CAD3. Отчеты предоставляют возможность поэтапной проверки в режиме "прошел/не прошел" по каждому разделу стандарта. В результате сотрудники ИТ-службы могут исключить догадки из процесса аудита на предмет соответствия отраслевым требованиям и завершить работу в мгновение ока.

Встроенный генератор отчетов

Встроенный в AirMagnet Enterprise генератор отчетности позволяет с легкостью создавать профессиональные и персонализированные отчеты по любому множеству местоположений или интервалу дат. Отчеты охватывают все сферы управления, включая 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.

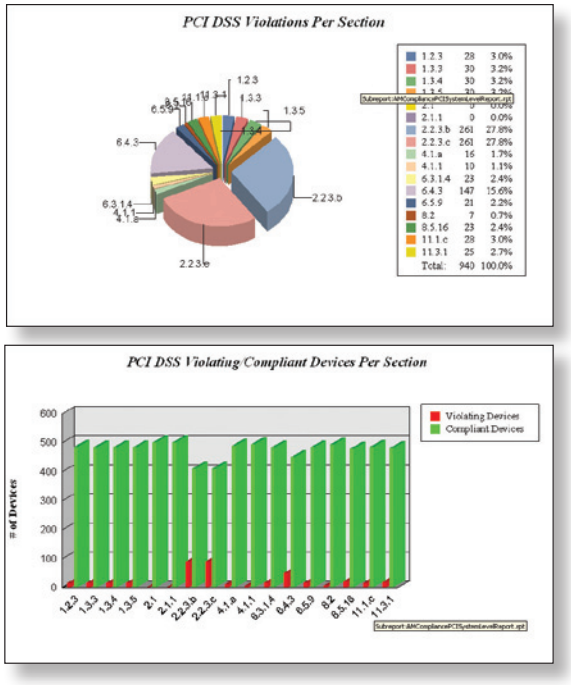

Рис. 12. *Помехи*

Информация для заказа

Модель	Описание
A5225	Сенсор с внутренней антенной, 802.11n, радиомодуль анализа выделенного спектра
A5220	Сенсор с внешней антенной, 802.11n, радиомодуль анализа выделенного спектра
A5031	Металлический хомут крепления сенсора с возможностью установки защелки
A5231	Пластиковый хомут крепления сенсора
A5505	Серверное и консольное ПО Enterprise-версии, неограниченное количество сенсоров
A5115	Серверная лицензия Enterprise-версии для поддержки функций 802.11n, неограниченное количество сенсоров
A5106	Серверная лицензия для функций анализа спектра Enterprise-версии, неограниченное количество сенсоров

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

Минимальные требования к серверу

Операционная система	Microsoft Windows Server 2008 / VMware ESX
Процессор	Серия Intel Xeon E3
Память	8 Гб / 1333 МГц или быстрее
Размер жесткого диска	146 Гб / 10 000 об/мин, SAS

Примечание. *При необходимости поддержки сервером определенных системных конфигураций могут возникнуть дополнительные требования. Для получения дополнительной информации посетите веб-страницу* ***http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Enterprise***.

Сертификация

Гарантия оценки общих критериев второго уровня
США: Сертификация по FIPS 140-2

Компания Fluke Networks
P.O. Box 777, Everett, WA USA/США 98206-0777

Fluke Networks работает более чем в 50 странах мира. Чтобы найти ближайшее к вам представительство, посетите веб-сайт **www.flukenetworks.com/contact**.

Отпечатано в США 2/2012 4004068C