McAfee Policy Auditor Software

Интеграция + инновации = эффективность обеспечения нормативно-правового соответствия

Предлагаем вам передовое программное обеспечение для проведения аудита информационной безопасности, позволяющее сократить расходы на подтверждение нормативно-правового соответствия. В программном обеспечении McAfee® Policy Auditor реализован оптимизированный подход. Встроенные механизмы интеграции и новаторский характер решения позволяют обеспечить реальную окупаемость инвестиций и значительное повышение производительности труда при одновременном снижении сложности и стоимости аудитов.

Обеспечение соответствия основным отраслевым нормам

Путем сопоставления средств управления ИТ с заданными положениями политик программное обеспечение McAfee Policy Auditor автоматизирует процессы аудита, ранее осуществлявшиеся вручную, и помогает создавать последовательные и точные отчеты о соответствии внутренним и внешним политикам. Программное обеспечение McAfee Policy Auditor поставляется в комплекте с готовыми шаблонами для целого ряда отраслевых норм: PCI DSS (в McAfee Policy Auditor есть панель мониторинга требований PCI, позволяющая получить консолидированное представление об уровне соответствия по каждому требованию PCI или по каждому средству защиты), SOX, HIPAA, FISMA и ряда других. Кроме того, оно поддерживает стандарты ISO 27001 и COBIT, в которых изложены лучшие отраслевые практики. В число поддерживаемых платформ входят Microsoft Windows, Oracle Solaris, Red Hat Linux, CentOS, HP/UX, IBM AIX и Apple Macintosh (Mac) OS X.

Снижение затрат на управление благодаря интеграции с программным обеспечением McAfee ePolicy Orchestrator®

Полная интеграция с McAfee ePolicy Orchestrator (McAfee ePO™) позволяет упростить процессы развертывания агентов, управления отдельными продуктами и генерирования отчетности.

Основные преимущества

Оптимизация операций
Объединение процессов управления аудитами систем на соответствие политикам и процессов обеспечения безопасности конечных точек

Сокращение времени, необходимого для обеспечения нормативно-правового соответствия
Проведение консолидированных аудитов как всех управляемых (с установленными агентами), так и всех неуправляемых (без агентов) систем

Систематичный подход к обеспечению нормативно-правового соответствия
Составление отчетов о соответствии основным отраслевым нормам и внутренним политикам

Использование единой консоли McAfee ePO дает возможность консолидировать процессы управления защитой конечных точек и нормативно-правовым соответствием, что ведет к снижению стоимости владения всей системой обеспечения безопасности и нормативно-правового соответствия. Экономя на аппаратном обеспечении, обучении персонала и эксплуатационных издержках, вы получаете возможность осуществлять централизованный контроль над политиками и средствами защиты на каждом узле.

Централизация аудитов позволяет сократить время, необходимое для обеспечения нормативно-правового соответствия

Организации получают возможность проводить консолидированные аудиты как всех управляемых (с установленными агентами), так и всех неуправляемых (без агентов) систем. Один раз создав и выбрав в консоли McAfee ePO единый набор контрольных показателей, они смогут проводить оценку большого количества активов разных типов. Это позволяет сократить трудозатраты, необходимые для проведения аудитов, и дает организациям долгожданную возможность генерировать единый общий отчет по всем активам.

Расширение возможностей программного обеспечения McAfee Policy Auditor с помощью сценариев

Если вы хотите еще больше расширить возможности агентов, осуществляющих проверки на соответствие политикам, то можете создать свои собственные правила, используя для этого любой язык написания сценариев, поддерживаемый проверяемой системой. Это может быть VBScript, Batch, Perl, Python и др.

Представляем новый стандарт подтверждения нормативно-правового соответствия: SCAP

В программном обеспечении McAfee Policy Auditor предложен новый стандарт, представляющий собой реализацию семейства протоколов Secure Content Automation Protocol (SCAP). Это открытый стандарт, обеспечивающий функциональную совместимость продуктов и служб и помогающий сократить временны́е, финансовые и трудовые затраты на проведение аудитов.

Поддерживаются следующие протоколы:

- eXtensible Checklist Configuration Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)
- Common Vulnerabilities and Exposures (CVE)

Основные преимущества (продолжение)

Автоматизация аудитов, прежде выполнявшихся вручную
Наличие регулярно обновляемых данных, многофункциональных панелей мониторинга, подробных отчетов и встроенных функций управления отступлениями от требований, что позволяет упростить работу на каждом этапе

Подтвержденное соответствие стандартам SCAP-FDCC
Соответствие данного решения стандарту SCAP, подтвержденное Национальным институтом стандартов и технологий США (National Institute of Standards and Technology — NIST)

- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)

Возможность за считанные минуты импортировать и адаптировать отраслевые эталонные тесты

Благодаря поддержке SCAP и нашим собственным новаторским разработкам мы в состоянии облегчить вам задачу подтверждения нормативно-правового соответствия даже в случае изменения отраслевых норм и политик. Мы предоставляем возможность загружать с проверенных сайтов отраслевые эталонные тесты (например, Federal Desktop Core Configuration [FDCC] с веб-сайта NIST) и просматривать подробные комментарии к этим тестам, составленные специалистами по безопасности. Использование унифицированных эталонных тестов снижает вероятность того, что их результаты будут по-разному толковаться сотрудниками отделов информационной безопасности и внешними аудиторами.

Регулярное обновление данных и сокращение количества нарушений в работе

Использование новаторской модели непрерывного аудита помогает сотрудникам отделов информационной безопасности и аудиторам обеспечивать актуальность и точность данных. Данная модель позволяет отказаться от таких процессов подготовки к внутренним и внешним аудитам, которые требуют генерирования данных вручную. Во избежание нарушений в работе критически важных бизнес-приложений отделы ИТ-операций могут задавать временны́е промежутки, в которых не допускается проведение аудитов.

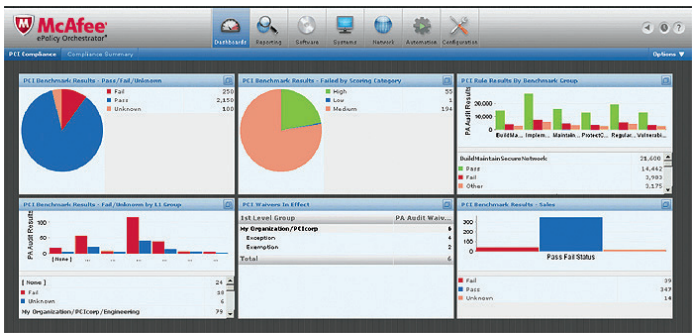

Рис. 1. Многофункциональные графические панели мониторинга помогают измерять уровень нормативно-правового соответствия, осуществлять мониторинг и генерировать отчеты

Согласование бизнес-процессов и аудитов

Аудиты всегда приходят «не вовремя». Но теперь у вас есть возможность минимизировать нарушения в работе, связанные с проведением аудитов. Вы можете документировать и разрешать отступления от требований политик, а также задавать сроки действия таких отступлений, позволяющие ограничивать риски.

- **Освобождение**. Позволяет освободить систему от всех аудитов
- **Блокировка**. Позволяет исключить систему из отчетов.

Упрощение обработки заявок на устранение проблем

Если в ходе аудита обнаружились проблемы, программное обеспечение McAfee ePO позволяет создать заявки на их устранение и легко их отслеживать. К вашим услугам также дополнительные механизмы интеграции, позволяющие принудительно направлять заявки в сторонние системы обработки заявок, такие как BMC Remedy.

Обеспечение непрерывного нормативно-правового соответствия с помощью McAfee Change Control

После проведения аудита и устранения обнаруженных проблем вы можете заблокировать внесение несанкционированных изменений в систему, обеспечив тем самым непрерывное соответствие системы требованиям политики.

McAfee Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru