

McAfee Change Control

Предотвращение внесения несанкционированных изменений и автоматизация управления нормативно-правовым соответствием

В наше время во многих организациях происходит непрерывное внесение изменений в серверные среды. Причем эти изменения остаются незамеченными. Такая ситуация опасна как с точки зрения безопасности, так и с точки зрения нормативно-правового соответствия. Решение McAfee® Change Control, входящее в линейку продуктов McAfee, дает вам возможность непрерывного и мгновенного обнаружения авторизованных изменений в масштабах всего предприятия. Решение блокирует попытки внесения несанкционированных изменений в критически важные системные файлы, каталоги и конфигурации, параллельно оптимизируя процесс внедрения новых политик и принятия мер по обеспечению нормативно-правового соответствия.

Программное обеспечение McAfee Change Control полностью устраняет возможность самого внесения изменений, ставшего сегодня расхожей практикой на многих предприятиях. Внесение изменений может вызвать нарушения безопасности, утечки данных и сбои в работе систем. Благодаря наличию таких функций, как мониторинг целостности файлов и предотвращение внесения изменений, McAfee Change Control обеспечивает принудительное применение политик внесения изменений и непрерывный мониторинг критически важных систем. Кроме того, решение обнаруживает изменения, вносимые на распределенных и удаленных ресурсах, и блокирует нежелательные изменения.

Благодаря интуитивно понятному поисковому интерфейсу McAfee Change Control помогает пользователям быстро находить информацию о событиях, связанных с внесением изменений. С помощью этого интерфейса вы можете, например, найти информацию обо всех изменениях, имевших место в каталоге c:\windows\system32 на сервере xyz.acme.com.

Новый уровень мониторинга целостности файлов

Положения разделов 10 и 11. 5 Стандарта защиты информации в индустрии платежных карт PCI DSS требуют осуществлять отслеживание и мониторинг всех случаев доступа к сетевым ресурсам и данным владельцев карт, а также внедрять средства

Ключевые функции

- **Мониторинг целостности файлов.** Непрерывное отслеживание изменений, вносимых в файлы и разделы реестра; контроль за тем, кем и в какие файлы были внесены изменения
- **Предотвращение внесения изменений.** Защита критически важных файлов и разделов реестра от внесения изменений, не соответствующих политикам установки обновлений

Экономия системных ресурсов и эксплуатационных расходов

- Легкость настройки и низкие расходы на запуск и эксплуатацию
- Незначительный объем используемой памяти
- Отказ от сканирования файлов, снижающего быстродействие систем

ЛИСТ ДАННЫХ

мониторинга целостности файлов, позволяющие уведомлять сотрудников о попытках внесения несанкционированных изменений в критически важные системные файлы, конфигурационные файлы и файлы контента. McAfee Change Control позволяет вам внедрять средства мониторинга целостности файлов в режиме реального времени и эффективным и недорогим способом подтверждать соответствие требованиям стандарта PCI. Включенная в McAfee Change Control функция мониторинга целостности файлов дает возможность собирать важную информацию о том, кем, когда, где и почему были внесены те или иные изменения. С ее помощью вы сможете в режиме реального времени получать информацию об именах пользователя, времени внесения изменений, названиях программ и содержимом файлов и реестра. Кроме того, она поможет вам обнаруживать причины сбоев в работе систем.

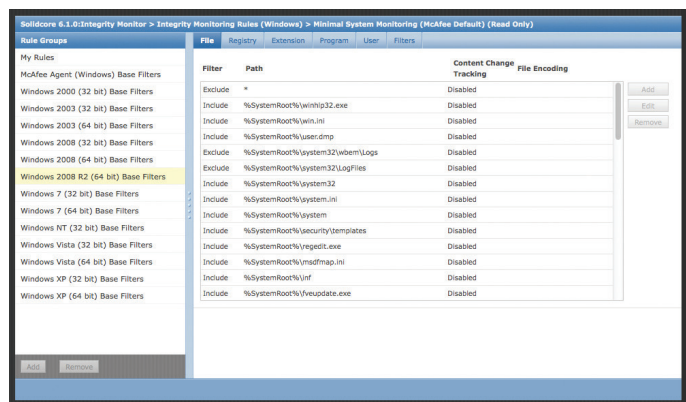


Рис. 1. McAfee Change Control содержит готовые правила мониторинга целостности файлов и продуманный набор фильтров, позволяющих следить только за теми файлами, которые вам необходимы.

Отслеживание изменений в содержимом

McAfee Change Control позволяет отслеживать изменения, вносимые в содержимое и атрибуты файлов. Возможность просмотра и параллельного сравнения изменений, внесенных в содержимое файлов, позволяет видеть, что было добавлено, удалено или изменено. Эта функция очень помогает устранять сбои в работе, вызванные изменениями в конфигурациях.

Имеющиеся фильтры включения/исключения могут быть настроены таким образом, что McAfee Change Control будет учитывать только интересующие вас изменения, в отношении которых может понадобиться принять те или иные меры. Более того, специальные механизмы рассылки уведомлений мгновенно сообщают вам о внесении критически важных изменений, что дает вам возможность избежать сбоев в работе, вызванных ошибками в конфигурации; это соответствует рекомендациям, содержащимся в сборнике Information Technology Infrastructure Library (ITIL). Наличие шаблонов отчетов для аудитов, проводимых квалифицированными аудиторами систем безопасности (Qualified Security Assessor — QSA), позволяет облегчить процесс предоставления отчетности в соответствии с требованиями стандарта PCI.

Ключевые преимущества

- Непрерывный сбор информации об изменениях и управление (в режиме реального времени) изменениями, вносимыми в критически важные системные файлы, конфигурационные файлы и файлы контента
- Предотвращение внесения несанкционированных изменений в критически важные файлы и разделы реестра неавторизованными лицами
- Выполнение требования Стандарта PCI DSS, касающегося системы мониторинга целостности файлов
- Простые в освоении готовые правила мониторинга целостности файлов
- Наличие шаблонов аудиторских отчетов, облегчающих ведение отчетности о соответствии требованиям стандарта PCI
- Функция исключения объекта с помощью одного щелчка мыши позволяет отменить мониторинг ненужной информации
- Надежный процесс применения политик путем упреждающего блокирования попыток внесения внеочередных и нежелательных изменений
- Возможность интеграции с консолью McAfee® ePolicy Orchestrator® (McAfee ePO™) с целью централизации управления информационными технологиями

Предотвращение сбоев в работе в результате внесения внеплановых изменений

Использование McAfee Change Control позволяет ИТ-специалистам легко находить причины нарушений, автоматизировать управление нормативно-правовым соответствием и предотвращать сбои в работе, связанные с внесением изменений. Более того, McAfee Change Control позволяет избавиться от необходимости затратной и чреватой ошибками ручной работы по составлению политик обеспечения нормативно-правового соответствия, связанных с выполнением требований Закона Сарбейнза-Оксли. McAfee Change Control дает вам возможность создать автоматизированную систему информационно-технического контроля, в которой вся информация, необходимая для проверки нормативно-правового соответствия, представлена в рамках единой системы отчетности. Согласование санкционированных изменений производится автоматически. Документирование и согласование срочных исправлений и иных внеочередных изменений производится автоматически с целью облегчения аудита.

Централизованное управление безопасностью и нормативно-правовым соответствием

Программное обеспечение McAfee ePO позволяет консолидировать и централизовать процесс управления, давая вам полное представление о состоянии безопасности на вашем предприятии. Оно обеспечивает требуемую гибкость в выборе систем, подлежащих контролю, и позволяет вам определять, какие файлы, каталоги и конфигурации

должны быть включены в систему оповещения о внесении изменений; вы можете также настраивать приоритеты оповещений. Наличие готовых профилей для самых распространенных видов серверных операционных систем и корпоративных приложений позволяет вести мониторинг критически важных компонентов без необходимости с нуля создавать новые профили. Используя McAfee Change Control и программное обеспечение McAfee ePO, вы можете в любое время активировать новые профили, повышая тем самым уровень защиты, например, с режима простого мониторинга до режима принудительного применения политик.

Программное обеспечение McAfee ePO является масштабируемым, и к нему легко подключать дополнительные модули. Оно позволяет интегрировать программное обеспечение McAfee Change Control и другие продукты McAfee для управления средствами защиты с соответствующими продуктами наших партнеров.

Все дело в применении политик

Программное обеспечение McAfee Change Control в режиме реального времени отслеживает и проверяет каждую попытку внесения изменений на вашем сервере. Оно обеспечивает применение политик, касающихся внесения изменений, требуя, чтобы изменения вносились в течение определенного промежутка времени, только из доверенных источников или при наличии разрешений на внесение изменений. Компонент программного обеспечения McAfee Change Control, отвечающий

Поддерживаемые платформы

Microsoft Windows (32- и 64-разрядные версии)

- Встроенные: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009
- Серверы: Windows NT, 2000, 2003, 2003 R2, 2008, 2008 R2, 2012
- Рабочие станции: Windows XP, Vista, 7

Linux

- RHEL 5, 6
- Suse 10, 11
- CentOS 5, 6
- OEL 5, 6
- SLED 11
- OpenSUSE 10/11

AIX

- AIX 6.1, 7.1

ЛИСТ ДАННЫХ

за предотвращение изменений, можно настроить таким образом, чтобы системные приложения могли без перебоев постоянно обновлять свои файлы, а другие приложения и пользователи не имели бы права вносить изменения или даже просматривать те или иные файлы.

Как минимизировать риск нарушений и совершенствовать нормативно-правовое соответствие сразу на нескольких фронтах

Мы предлагаем широкий спектр решений для контроля за рисками и обеспечения нормативно-правового соответствия, которые помогают минимизировать риск нарушений, автоматизировать процесс подтверждения нормативно-правового соответствия и оптимизировать систему защиты. В частности, мощным инструментом для устранения уязвимостей и обеспечения нормативно-правового соответствия в масштабах всей вашей компании служит сочетание продуктов McAfee Change Control и McAfee Application Control.

Последующие действия

Программное обеспечение McAfee Change Control устраняет возможность внесения изменений в серверных средах: нежелательные изменения могут приводить к случаям нарушения безопасности, утечкам данных и сбоям в работе систем. Кроме того, оно упрощает процессы обеспечения нормативно-правового соответствия. McAfee Change Control предотвращает внесение несанкционированных изменений и автоматизирует управление нормативно-правовым соответствием.



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

McAfee, логотип McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2017 McAfee, LLC. 60736ds_mcc_1213B
Декабрь 2013 г.