

McAfee Change Control

Предотвращение внесения несанкционированных изменений и автоматизация средств обеспечения нормативно-правового соответствия

Основные 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.
- **Согласование вносимых изменений.** Интеграция McAfee Change Control с корпоративными системами управления изменениями при помощи McAfee ePolicy Orchestrator® (McAfee ePO™), включая интеграцию с модулем BMC Remedy, активируемую одним щелчком мыши.

Экономия системных ресурсов и эксплуатационных расходов

- Легкость настройки и низкие расходы на запуск и эксплуатацию.
- Незначительный объем используемой памяти.
- Отсутствует снижающее быстродействие системы сканирование файлов.

В наше время во многих организациях имеет место непрерывное внесение изменений в серверные среды. И эти изменения остаются незамеченными. Такая ситуация опасна как с точки зрения безопасности, так и с точки зрения нормативно-правового соответствия. McAfee® Change Control дает вам возможность в масштабах всей вашей компании обнаруживать авторизованные изменения по мере их внесения. 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.

McAfee Change Control позволяет избежать внесения таких изменений, которые могут привести к нарушению системы безопасности, к утечке данных или к сбою в работе. К сожалению, в наше время на фирмах и предприятиях подобное случается слишком часто. Благодаря наличию таких функций, как мониторинг целостности файлов, предотвращение внесения изменений и согласование вносимых изменений (последнее в виде дополнительного программного компонента), McAfee Change Control позволяет применять политики внесения изменений, обеспечивать непрерывный мониторинг критически важных систем и обнаруживать изменения, вносимые на распределенных и удаленных ресурсах. А также он блокирует попытки внесения нежелательных изменений.

McAfee Change Control имеет интуитивно понятный поисковый интерфейс, который помогает пользователям быстро находить информацию о событиях, связанных с внесением каких-либо 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 PCI DSS требуют осуществлять отслеживание и мониторинг всех случаев доступа к сетевым ресурсам и данным владельцев карт, а также использовать средства мониторинга целостности файлов, позволяющие уведомлять сотрудников о попытках внесения несанкционированных изменений в критически важные системные, конфигурационные или информационные файлы. 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 системы.

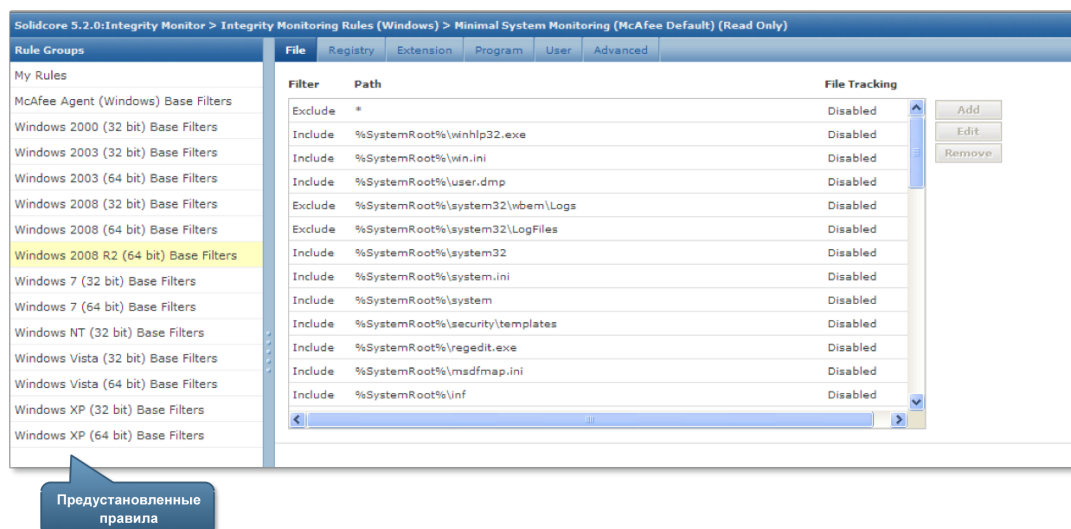


Рис. 1. McAfee Change Control содержит готовые правила мониторинга целостности файлов и продуманный набор фильтров, позволяющих следить только за теми файлами, которые вам необходимы.

Ключевые преимущества

- Возможность непрерывного визуального контроля за изменениями и управления (в режиме реального времени) изменениями, вносимыми в критически важные системные, конфигурационные и информационные файлы
- Предотвращение внесения несанкционированных изменений в критически важные файлы и разделы реестра неавторизованными лицами
- Выполнение требования PCI DSS, касающегося системы мониторинга целостности файлов
- Легкость в использовании готовых правил мониторинга целостности файлов
- Наличие шаблонов аудиторских отчетов, облегчающих ведение отчетности о соответствии требованиям стандарта PCI
- Функция удаления объекта с помощью одного щелчка мыши, чтобы не вести 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
- Интеграция McAfee ePO с BMC Remedy, активируемая одним щелчком мыши

Поддерживаемые платформы Microsoft Windows (32- и 64-разрядные версии)

- Встроенные: XPE, 7E
- Серверы: NT, 2000, 2003, 2003 R2, 2008, 2008 R2
- Рабочие станции: XP, Vista, 7

Linux

- RHEL 3, 4, 5, 6
- Suse 9, 10, 11
- CentOS 4, 5
- SLED 11
- OpenSUSE 10/11

Solaris

- 8, 9, 10 на SPARC
- 10 на x86, x86-64

AIX

- AIX 5.3, 6.1

HPUX

- HPUX 11i v1, v2, v3



ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

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 аудиторскими системами безопасности (Qualified Security Assessor — QSA), позволяет облегчить процесс предоставления отчетности в соответствии с требованиями стандарта PCI.

Предотвращение сбоев в работе в результате внесения внеплановых изменений

Использование McAfee Change Control позволяет ИТ-специалистам с легкостью находить причины нарушений, автоматизировать процесс контроля за нормативно-правовым соответствием и предотвращать сбои в работе, связанные с внесением изменений. Более того, McAfee Change Control позволяет избавиться от необходимости ресурсоемкой и чреватой ошибками ручной работы по составлению политик обеспечения нормативно-правового соответствия, которое часто ассоциируется с выполнением требований закона Сарбейнза-Оксли. При использовании дополнительного программного обеспечения McAfee Change Reconciliation для согласования вносимых изменений 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 авторизованных 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 ePolicy Orchestrator® (McAfee ePO™) позволяет консолидировать и централизовать процесс управления, давая вам полную картину состояния безопасности в масштабах всей вашей компании. Оно обеспечивает требуемую гибкость в выборе систем, подлежащих контролю, и позволяет указывать, 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 партнеров McAfee, входящих в McAfee Security Innovation Alliance. Кроме того, в случае использования McAfee Change Control совместно с дополнительным программным модулем для согласования вносимых изменений возможна интеграция программного обеспечения McAfee ePO с модулем BMC Remedy, активируемая одним щелчком мыши.

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 разрешения на внесение изменений. Компонент программного обеспечения McAfee Change Control, отвечающий за предотвращение изменений, можно настроить таким образом, чтобы системные приложения могли без перебоев регулярно обновлять свои файлы, а другие приложения и пользователи не имели бы права вносить изменения или даже просматривать те или иные файлы.

Минимизация риска и максимизация нормативно-правового соответствия сразу на нескольких фронтах

McAfee предлагает широкий спектр решений для контроля за рисками и обеспечения нормативно-правового соответствия, которые помогают минимизировать риск, 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 является сочетание продуктов McAfee Change Control и McAfee Application Control.

McAfee, логотип McAfee, McAfee ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright © 2012 McAfee, Inc. 41100ds_mcc_1211_fnl_ETMG