McAfee Application and Change Control

Комплексная защита от внесения нежелательных изменений и несанкционированного управления приложениями, конечными точками, серверами и устройствами фиксированного назначения

Постоянные угрозы повышенной сложности (advanced persistent threats — APT), реализуемые посредством удаленных атак и методов социальной инженерии, усложняют задачу защиты предприятий и могут привести к нарушениям безопасности, утечкам данных и сбоям в работе. В современных серверных и облачных средах, постоянно находящихся в процессе адаптации и усовершенствования, особенно велика вероятность того, что вредоносные изменения останутся незамеченными. Поэтому тем, кто стремится полностью избавиться от постоянных угроз повышенной сложности, следует внимательно присмотреться к программному обеспечению McAfee® Application and Change Control.

McAfee® Application Control помогает службам ИТ перехитрить киберпреступников и обеспечивает безопасность и производительность бизнеса. Используя динамическую модель доверия, функции локального и глобального сбора информации о репутации, анализ поведения в режиме реального времени и автоиммунизацию конечных точек, решение McAfee мгновенно блокирует сложные постоянные угрозы (APT), избавляя вас от трудоемкого управления списками приложений и обновления сигнатур.

McAfee® Change Control блокирует попытки внести несанкционированные изменения в критически важные системные файлы, каталоги и конфигурации, параллельно оптимизируя процесс внедрения новых политик и принятия мер по обеспечению нормативно-правового соответствия. 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 и блокирует изменения, вносимые на распределенных и удаленных ресурсах. Интуитивно понятный поисковый интерфейс помогает пользователям быстро находить информацию о событиях, связанных с какими-либо изменениями.

Ключевые преимущества

- Используйте McAfee Global Threat Intelligence и McAfee Threat Intelligence Exchange, чтобы получить информацию о глобальной и локальной репутации файлов и приложений!
- Усильте защиту и сократите стоимость владения благодаря использованию динамических белых списков, автоматически принимающих новое программное обеспечение, если оно установлено по доверенным каналам!
- Обеспечьте защиту на подключенных и не подключенных к сети серверах, виртуальных машинах, конечных точках и устройствах с фиксированными функциями, таких как терминалы для приема платежей и устаревшие системы!

Подписаться

McAfee Application and Change Control представляет собой сочетание этих двух технологий, обеспечивающее целостность систем, разрешая только авторизованный доступ к устройствам, блокируя несанкционированные исполняемые файлы, а также систематически отслеживая и предотвращая попытки внести изменения в файловую систему, реестр и учетные записи пользователей. Решение помогает обеспечивать непрерывное и эффективное обнаружение угроз и защиту от них в масштабах всего предприятия.

Интеллектуальные белые списки

Решение позволяет предотвращать атаки «нулевого дня» и атаки APT, блокируя выполнение несанкционированных приложений и разрешая запуск только тех приложений, которые внесены в белый список. Обнаружив двоичные файлы (EXE, DLL, драйверы и сценарии) во всех имеющихся в компании системах, McAfee Application and Change Control группирует их по приложениям и производителям, отображает их в интуитивно понятном иерархическом формате и автоматически распределяет по категориям «заведомо хорошие», «неизвестные» и «заведомо плохие».

Внедрение правильной системы обеспечения безопасности

Чтобы дать бизнес-пользователям, использующим в своей работе социальные сети и облачные приложения, больше свободы в выборе приложений, McAfee Application and Change Control предлагает организациям три варианта оптимизации стратегии предотвращения угроз с помощью белых списков, а именно:

Рис. 1. Три способа повышения эффективности стратегии предотвращения угроз с помощью белых списков.

Ключевые преимущества (продолжение)

- Разрешайте новые приложения на основе рейтинга приложений или «самостоятельного утверждения», повышая непрерывность бизнеса!
- Обеспечивайте непрерывный сбор информации об изменениях и управление (в режиме реального времени) изменениями, вносимыми в критически важные системные файлы, конфигурационные файлы и файлы контента!
- Предотвращайте внесение несанкционированных изменений в критически важные файлы и разделы реестра неавторизованными лицами!
- Обеспечивайте строгое применение политик путем упреждающего блокирования попыток внести внеочередные и нежелательные изменения!

Комплексное и быстрое реагирование

Для повышения эффективности белых списков используется информация об угрозах, собираемая с помощью McAfee® Global Threat Intelligence — единственной в своем роде технологии McAfee, которая в режиме реального времени отслеживает репутацию файлов, сообщений и отправителей с помощью миллионов датчиков, расположенных по всему миру. Полученная с помощью технологии GTI информация используется в McAfee Application Control для оценки репутации файлов в вашей вычислительной среде и их классификации на «хорошие», «плохие» и «неизвестные».

При развертывании вместе с McAfee® Threat Intelligence Exchange (дополнительный модуль, приобретаемый отдельно) McAfee Application Control обновляет белый список на основе локальной информации о репутации, что позволяет мгновенно отражать угрозы безопасности. Взаимодействие McAfee Threat Intelligence Exchange с McAfee® Advanced Threat Defense позволяет динамически анализировать поведение неизвестных приложений в изолированной среде («песочнице») и автоматически обеспечивать невосприимчивость всех конечных точек к недавно обнаруженным вредоносным программам.

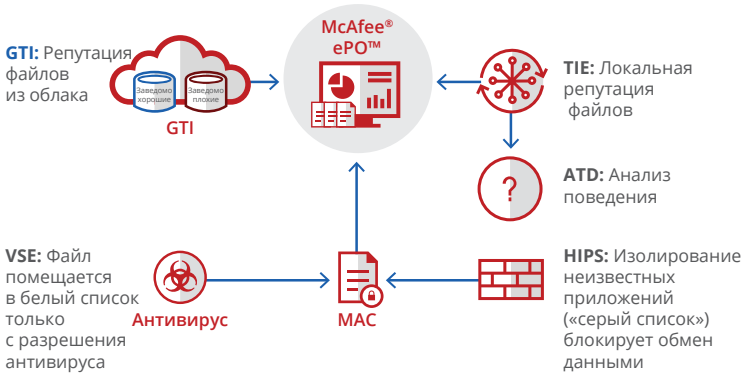

Рис. 2. McAfee Global Threat Intelligence и McAfee Threat Intelligence Exchange собирают для McAfee Application Control информацию о глобальной и локальной репутации файлов и приложений.

Эффективные встроенные рекомендации

Функция поиска по инвентарным данным и возможность генерировать предопределенные отчеты помогают пользователям легко решать проблемы, связанные с уязвимостями, нормативно-правовым соответствием и безопасностью файлов и сред приложений. Вы сможете проводить поиск по интересующим вас параметрам, таким как недавно добавленные приложения, несертифицированные двоичные файлы, файлы с неизвестной репутацией, системы с устаревшими версиями ПО и т. д.

В McAfee Application and Change Control 8.3 появился режим инвентаризации, позволяющий регулярно обновлять инвентарные данные по каждой системе

и каждому устройству. Это позволяет сократить объем используемых ресурсов ЦП, а также ресурсов систем и устройств без нарушения требований SWAM/CPE и PCI DSS. Режим инвентаризации позволяет пользователям отслеживать изменения, вносимые в двоичные и другие файлы на конечных точках по прошествии времени. Дополнительная функция CPE (Common Platform Enumeration — «Список типовых платформ») позволяет сопоставлять данные из списка CPE Национального института стандартов и технологий (NIST) США с собранными инвентарными данными и использовать полученные результаты при создании белых списков и составлении отчетов о нормативно-правовом соответствии.

Не сказывается на непрерывности бизнеса

Во избежание нарушения непрерывности ведения бизнеса допуск новых приложений осуществляется автоматически на основе репутации приложений. При попытках установить неизвестные приложения интерфейс рекомендаций предлагает новые политики установки обновлений, создаваемые на основе результатов наблюдения за запуском приложений на конечных точках. Это превосходный способ управления исключениями, которые генерируются заблокированными приложениями. Проверив все исключения и информацию о заблокированных приложениях, администратор может либо допустить файл и включить его в белый список, либо просто проигнорировать его, и тогда приложение будет заблокировано.

Помогите пользователям стать частью решения

При попытках установить неизвестные приложения McAfee Application and Change Control объясняет пользователям, почему им не разрешен доступ к несанкционированным приложениям, и дает пользователям возможность получить разрешение на использование того или иного приложения либо путем «самостоятельного утверждения», либо путем подачи запроса на утверждение.

Поддержание систем в актуальном состоянии

Своевременная установка новейших пакетов исправлений — чрезвычайно важна. Используемая в McAfee Application and Change Control динамическая модель доверия позволяет автоматически обновлять системы, не нарушая при этом непрерывность бизнеса. В основе модели лежат такие понятия, как доверенные пользователи, доверенные локальные группы, сертификаты, процессы и каталоги. Кроме того, McAfee Application Control обеспечивает защиту включенных в белый список приложений от атак методом переполнения буфера памяти на операционных системах Microsoft Windows.

Предотвращение внесения изменений и мониторинг целостности

Нередко происходит изменение конфигураций («дрейф конфигураций»), при котором невозможно понять, кто выполнил то или иное изменение, что может привести к нарушениям безопасности, утечкам данных и сбоям в работе. McAfee Application and Change Control может блокировать или ограничивать любые

Поддерживаемые платформы

McAfee Application and Change Control:

- 8.3.x, 8.2.x, 8.1.x, 8.0.x, 7.0.x (операционные системы на базе Windows)
- 6.4.x, 6.3.x (операционные системы на базе Linux) 6.2.x, 6.1.x (операционные системы на базе Windows и UNIX)
- Linux
- Microsoft Windows

попытки внести в систему или устройство изменения, не соответствующие действующим политикам. Все попытки внести изменения регистрируются в журнале, а информацию обо всех событиях изменений можно получить в режиме реального времени. Модуль системного контроллера обеспечивает связь между системным контроллером и агентами.

Новый уровень мониторинга целостности файлов

McAfee Application and Change Control позволяет осуществить реализацию программных средств мониторинга целостности файлов (File Integrity Monitoring, FIM) в режиме реального времени и внедрить эффективный и недорогой механизм проверки соответствия требованиям PCI DSS. Реализованная с помощью McAfee Application and Change Control функция FIM дает возможность собирать важную информацию о том, кем, когда, где и почему были внесены те или иные изменения, т. е. с ее помощью вы сможете в режиме реального времени централизованно получать информацию об именах пользователей, времени внесения изменений, названиях программ, содержимом файлов и реестра и др. Кроме того, она поможет вам обнаруживать причины сбоев в работе систем.

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. Имеющиеся фильтры включения и 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. Внесение изменений в системы и устройства можно также ограничить определенным кругом пользователей, локальных групп пользователей, типами приложений, сертификатов и(или) веб-сервисов. Внесение изменений в системы и устройства можно даже ограничить определенным временем и определенными датами (например: разрешить применение обновлений Windows только с 2:00 до 4:00 утра по вторникам). Более того, специальные механизмы рассылки уведомлений мгновенно сообщают ИТ-специалистам о внесении критически важных изменений, что дает 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), облегчает процесс подготовки отчетности в соответствии с требованиями стандарта PCI.

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, решение позволяет избавиться от необходимости затратной и чреватой ошибками ручной работы по составлению политик обеспечения нормативно-правового соответствия, связанных с выполнением требований Закона Сарбейнза-Оксли (SOX). McAfee Application and 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 ePolicy Orchestrator® (McAfee ePO™) позволяет консолидировать и централизовать процесс управления, давая вам полную картину состояния безопасности в масштабах всей вашей компании. Получившая широкое признание специалистов платформа интегрирует McAfee Application and Change Control с решением McAfee® Host Intrusion Prevention и другими защитными продуктами McAfee, включая средства защиты от вредоносного ПО, служащие источником информации для создания черных списков. Простую одношаговую установку и обновление развертывания McAfee Application and Change Control можно также выполнять из системного центра Microsoft System Center. Вы можете в любое время активировать новые профили, повышая тем самым уровень защиты, например, с режима простого мониторинга до режима принудительного применения политик.

Дальнейшие действия

Вам необходимо надежно заблокировать или ограничить выполнение несанкционированных приложений, ставящих под угрозу безопасность данных, и обеспечить систематическое отслеживание и предотвращение внесения изменений в файловую систему, реестр и учетные записи пользователей. McAfee Application and Change Control обеспечивает целостность систем, разрешая только авторизованный доступ к устройствам и блокируя несанкционированные исполняемые файлы.

Для получения дополнительной информации посетите страницу www.mcafee.com/ru/products/application-control.aspx или позвоните нам по телефону +7(495) 653-8513 (основной).

Дополнительная информация

Дополнительную информацию см. в нашем Руководстве по поддерживаемым средам — KB87944.

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