McAfee Embedded Control

Контроль за целостностью систем, изменениями и соответствием политикам — все в одном решении

Решение McAfee® Embedded Control поддерживает целостность вашей системы, блокируя выполнение неавторизованного кода и запрещая вносить неавторизованные изменения. Он автоматически создает динамический «белый список» «авторизованного кода» на встроенной системе. После создания и активации «белого списка» в системе фиксируется базовое безопасное состояние: запуск любых программ и фрагментов кода, не включенных в авторизованный набор, блокируется, а попытки внесения неавторизованных изменений отклоняются. Решение McAfee Integrity Control, сочетающее в себе McAfee Embedded Control и консоль McAfee ePolicy Orchestrator® (McAfee ePO™), способно генерировать интегрируемые отчеты, позволяющие удовлетворить широкий спектр требований нормативно-правового соответствия и аудита.

Инструмент McAfee Embedded Control предназначен для решения проблемы повышенного риска нарушения безопасности, возникающего в связи с использованием на встроенных устройствах коммерческих операционных систем. McAfee Embedded Control почти не оставляет следа в системе, потребляет мало системных ресурсов, работает независимо от приложений и обеспечивает защиту по принципу «установил и забыл». McAfee Embedded Control превращает систему, построенную на основе коммерческой операционной системы, в «черный ящик», который выглядит как закрытая, проприетарная операционная система. Он блокирует запуск любых неавторизованных программ, находящихся на диске или внедренных в память устройства, и предотвращает внесение неавторизованных изменений в авторизованную базовую систему. Это решение дает изготовителям встроенных систем возможность использовать преимущества коммерческих операционных систем, не беря на себя дополнительных рисков и не теряя контроль над тем, как их системы используются в рабочих ситуациях.

Ключевые преимущества

- Минимизация риска нарушения безопасности благодаря контролю за тем, какие программы запускаются на встроенных устройствах, и благодаря защите памяти этих устройств
- Помогает предоставлять доступ пользователям, позволяя контролировать доступ и снижать расходы на поддержку
- Выборочное применение политик
- Процесс «установил и забыл»
- Позволяет привести устройства в соответствие с нормативно-правовыми требованиями и требованиями аудита
- Сбор информации в режиме реального времени
- Комплексный аудит
- Возможность поиска по архиву изменений
- Замкнутый цикл согласования

Гарантия целостности системы

Контроль за исполняемыми файлами

При использовании McAfee Embedded Control к запуску допускаются только те программы, которые включены в динамический «белый список» McAfee. Все остальные программы (исполняемые файлы, динамические библиотеки, сценарии) считаются неавторизованными. Попытки их запуска пресекаются и по умолчанию заносятся в журнал событий. Это позволяет пресекать несанкционированный запуск самоустанавливающегося вредоносного ПО: червей, вирусов, шпионских программ и т. п.

Контроль памяти

Функция контроля памяти защищает запущенные процессы от попыток перехвата. При попытке внедрения неавторизованного кода в запущенный процесс происходит блокирование этого кода и регистрация данной попытки в журнале событий. Это позволяет регистрировать и нейтрализовать попытки перехвата управления системой, предпринимаемые с помощью таких методов использования уязвимостей, как переполнение буфера, переполнение динамически распределяемой области, выполнение стека и т. п.[1]

Интеграция с McAfee GTI — интеллектуальный способ борьбы с глобальными угрозами в физически изолированных средах

McAfee Global Threat Intelligence (McAfee GTI) — это эксклюзивная технология McAfee, позволяющая в режиме реального времени отслеживать репутацию файлов, сообщений и отправителей с помощью миллионов датчиков, расположенных по всему миру. Полученная с помощью облачной технологии GTI информация используется для определения репутации всех файлов в вашей вычислительной среде и их классификации на «хорошие», «плохие» и «неизвестные». Интеграция с технологией McAfee GTI позволит с уверенностью выявлять случаи непреднамеренного включения вредоносных программ в «белые списки». Служба анализа репутации GTI доступна во всех средах с программным обеспечением McAfee ePO независимо от того, подключена среда к Интернету или нет.

Контроль за изменениями

McAfee Embedded Control обнаруживает вносимые в систему изменения в режиме реального времени. Он предоставляет информацию об источниках изменений; подтверждает, что изменения были внесены туда, куда следует; регистрирует изменения в журнале событий и блокирует попытки использования неавторизованных средств внесения изменений.

С помощью McAfee Embedded Control вы можете внедрять процессы контроля за изменениями путем указания того, какие средства внесения изменений являются дозволенными. Вы можете определять, кто имеет право вносить изменения, какие сертификаты требуются для внесения изменений, куда можно вносить изменения (вы можете, например, разрешить вносить изменения только в отдельные файлы или директории) и когда (например, вы можете ограничивать время установки обновлений Microsoft Windows, указывая определенные часы и дни недели).

Функция упреждающей проверки проверяет все вносимые в системы изменения до того, как они будут применены. Если этот модуль активирован, то установку обновлений программных систем можно проводить только в контролируемом режиме.

Модуль отслеживания изменений в реальном времени регистрирует все изменения состояния системы, включая изменения кода, конфигурации и реестра. Изменения регистрируются по мере их внесения в режиме реального времени, и информация о них передается на системный контроллер с целью ее систематизации и архивирования.

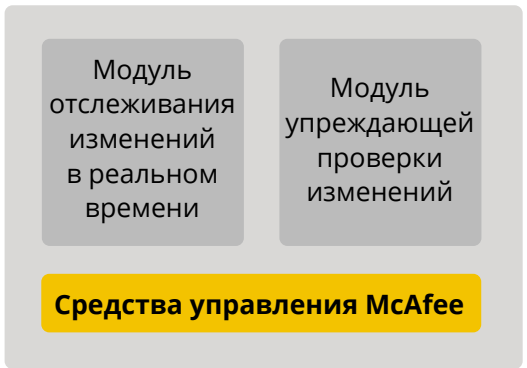

Рис. 1. Средства управления McAfee

Модуль системного контроллера обеспечивает связь между системным контроллером и агентами. Он собирает и сохраняет в независимой системе учета информацию о внесенных изменениях, поступающую от агентов.

Рис. 2. Модули отчетов, поиска и анализа

Аудит и соответствие политикам

Благодаря наличию панелей мониторинга и возможности генерировать отчеты McAfee Integrity Control помогает выполнять нормативно-правовые требования. Генерирование отчетов осуществляется посредством консоли McAfee ePO, имеющей веб-интерфейс для пользователей и администраторов.

McAfee Embedded Control позволяет использовать интегрированный замкнутый цикл аудита и обеспечения нормативно-правового соответствия в режиме реального времени, чему способствует наличие защищенной от фальсификаций системы учета авторизованных действий и попыток неавторизованных действий.

О решениях McAfee для защиты встроенных систем

Решения McAfee для защиты встроенных систем помогают производителям обеспечивать защиту своих продуктов и устройств от атак и киберугроз. Решения McAfee охватывают широкий спектр технологий: «белые списки» приложений, средства защиты от вирусов и вредоносных программ, средства управления устройствами, средства шифрования, средства управления нормативно-правовым соответствием и рисками и т. д. Во всех этих решениях используется технология McAfee Global Threat Intelligence, занимающая ведущее положение в отрасли. Наши решения могут быть адаптированы к конкретным техническим требованиям, предъявляемым производителем к своему устройству и его архитектуре.

Дальнейшие действия

Для получения дополнительной информации посетите веб-страницу **www.mcafee.com/ru/partners/oem-alliances/index.aspx** или обратитесь к своему региональному представителю McAfee.

Функция	Описание	Преимущество
Гарантия целостности системы		
Защита от внешних угроз	Допускает выполнение только авторизованного кода. Неавторизованный код не может быть внедрен в память. Авторизованный код защищен от фальсификации.	▪ Позволяет отказаться от внеплановой установки исправлений, сократить число и частоту циклов установки исправлений, уделять больше внимания тестированию исправлений перед их установкой и понизить уровень риска систем, на которых установка исправлений затруднена. ▪ Сокращает риск полиморфных атак «нулевого дня» с использованием вредоносных программ (червей, вирусов, троянских коней и т. п.) и попыток внедрения кода (переполнение буфера, переполнение динамически распределяемой области, переполнение стека и т. п.). ▪ Обеспечивает целостность авторизованных файлов, поддерживая рабочую систему в заведомо безопасном состоянии. ▪ Снижает эксплуатационные расходы за счет сокращения запланированных (для установки исправлений) и незапланированных (для устранения нарушений безопасности) простоев и увеличению времени непрерывной работы системы.

Функция	Описание	Преимущество
Защита от внутренних угроз	Блокировка локальных администраторов позволяет запретить вносить изменения в список авторизованных программ в защищенной системе даже администраторам, если они не имеют соответствующего подлинного ключа.	▪ Обеспечивает защиту от внутренних угроз. ▪ Фиксирует набор программ, используемых на встроенных системах, и не позволяет вносить изменения даже администраторам.
Расширенные функции контроля за изменениями		
Установка безопасных авторизованных обновлений от производителя	Допускает установку на рабочих встроенных системах только авторизованных обновлений.	▪ Не допускает внесения внеплановых изменений в рабочие системы. Блокирует попытки внесения неавторизованных изменений, чтобы избежать простоев и обращений в службу поддержки. ▪ Производители могут либо оставить за собой контроль над всеми изменениями, либо разрешить контролировать изменения только доверенным агентам клиента.
Проверяет, действительно ли изменения были внесены в согласованный период времени	Не допускает внесения изменений вне заданных временных рамок.	▪ Блокирует попытки внесения неавторизованных изменений, если они приходятся на пиковое рабочее время или на временной интервал, связанный с повышенным финансовым риском, чтобы избежать сбоев в работе и нарушений нормативно-правового соответствия.
Использование авторизованных субъектов установки обновлений	Допускает внесение изменений в рабочие системы только авторизованными субъектами установки обновлений, к которым могут относится люди и процессы.	▪ Не допускает внесения внеплановых изменений в рабочие системы.
Замкнутый цикл аудита и обеспечения нормативно-правового соответствия в реальном времени		
Отслеживание изменений в режиме реального времени	Отслеживает изменения в масштабах всего предприятия сразу при их внесении.	▪ Не допускает внесения внеплановых изменений в рабочие системы.
Комплексный аудит	Собирает полную информацию о каждом изменении, вносимом в систему: кто, что, где, когда и как.	▪ Составляет точный, полный и исчерпывающий список всех внесенных в систему изменений.
Обнаружение источников изменений	Устанавливает связь каждого изменения с его источником: кто внес изменение, какие события этому предшествовали, какие процессы или программы на это повлияли.	▪ Подтверждает разрешенные изменения; быстро обнаруживает неразрешенные изменения; повышает процент успешно внесенных изменений.
Низкие эксплуатационные расходы		
«Установил и забыл»	Установка программного обеспечения занимает всего несколько минут. Подготовка и настройка конфигурации не требуются. Также не требуется регулярно вносить изменения в конфигурацию.	▪ Продукт имеет стандартные настройки и начинает работать сразу после установки. Не требует постоянного технического обслуживания, поэтому рекомендуется тем, кому необходима система безопасности с низкими эксплуатационными расходами.

Функция	Описание	Преимущество
Отсутствие правил, сигнатур, и периода обучения; независимость от приложений	Не зависит от баз данных с правилами и сигнатурами; начинает действовать сразу, не требуя периода обучения; действителен для всех приложений.	▪ Требует очень мало внимания администратора на протяжении жизненного цикла сервера. ▪ Обеспечивает защиту сервера, на котором (пока) не установлены исправления, имея при этом низкий уровень текущих эксплуатационных затрат. ▪ Эффективность его работы не зависит от качества тех или иных правил или политик.
Низкое потребление системных ресурсов	Занимает менее 20 МБ пространства на диске. Не влияет на быстродействие приложений.	▪ Готов к развертыванию в любой критически важной рабочей системе, не снижая при этом ее быстродействия и не повышая требований к объему жесткого диска.
Гарантия отсутствия ложных положительных и ложных отрицательных результатов	В журнал событий вносятся только авторизованные действия.	▪ Благодаря точности получаемых результатов проведение ежедневного и еженедельного анализа журналов требует намного меньше времени, что позволяет снизить эксплуатационные расходы по сравнению с другими решениями для предотвращения вторжений на узел. ▪ Повышает эффективность работы администраторов, сокращает эксплуатационные расходы.

1. Данная функция доступна только на платформах Microsoft Windows.

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