McAfee Application Control

Сокращение риска запуска несанкционированных приложений на конечных точках, серверах и устройствах с фиксированными функциями

Сложные постоянные угрозы (advanced persistent threats — APT), реализуемые путем удаленных атак или методов социотехники, усложняют задачу защиты предприятий. McAfee® Application Control помогает перехитрить киберхулиганов и обеспечивает безопасность и производительность вашей компании. Благодаря использованию динамической модели доверия и таких инновационных функций обеспечения безопасности, как локальный и глобальный сбор информации о репутации, анализ поведения в режиме реального времени и автоиммунизация конечных точек, решение McAfee моментально блокирует сложные постоянные угрозы (APT), позволяя обойтись без трудоемкого управления списками приложений и обновления сигнатур. Хотите избежать угроз «нулевого дня»? Тогда советуем вам познакомиться с решением McAfee Application Control.

Интеллектуальные белые списки

McAfee Application Control предотвращает атаки «нулевого дня» и угрозы APT, блокируя выполнение несанкционированных приложений. Разработанная нами функция инвентаризации приложений позволяет легко находить относящиеся к приложениям файлы и управлять ими. Обнаружив двоичные файлы (EXE, DLL, драйверы и сценарии) во всех имеющихся в компании системах, данная функция группирует их по приложениям и производителям, отображает их в интуитивно понятном иерархическом формате и интеллектуально распределяет по категориям «заведомо хорошие», «неизвестные» и «заведомо плохие». Использование белых списков, разрешающих запуск только включенных в белый список «заведомо хороших» приложений, позволяет предотвращать атаки со стороны неизвестных вредоносных программ.

Ключевые преимущества

- Защита от угроз «нулевого дня» и постоянных угроз повышенной сложности, не требующая обновления сигнатур
- Использование McAfee Global Threat Intelligence и McAfee Threat Intelligence Exchange для получения информации о глобальной и локальной репутации файлов и приложений
- Повышение уровня защиты и сокращение стоимости владения благодаря использованию динамических белых списков, автоматически принимающих новое программное обеспечение, если оно установлено по доверенным каналам
- Эффективный контроль доступа к приложениям с помощью программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™) — централизованной платформы управления защитными решениями McAfee

Внедрение правильной системы обеспечения безопасности

Бизнес-пользователям, применяющим в своей работе социальные сети и облачные приложения, требуется больше свободы в выборе приложений. Поэтому McAfee Application Control предлагает организациям три способа повысить эффективность стратегии предотвращения угроз с помощью белых списков, а именно:

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

Эффективные встроенные рекомендации

Используя функцию поиска по данным инвентаризации и предопределенные отчеты, вы можете быстро находить и устранять в своей среде проблемы, касающиеся уязвимостей, нормативно-правового соответствия и безопасности. Вы можете легко проводить поиск по интересующим вас параметрам, таким как приложения, добавленные недавно, несертифицированные двоичные файлы, файлы с неизвестной репутацией, системы с устаревшими версиями программных продуктов и т. д. Это позволяет быстро выявлять уязвимости и подтверждать нормативно-правовое соответствие лицензий на программное обеспечение.

Полное и быстрое реагирование

Для повышения эффективности белых списков используется информация об угрозах, собираемся с помощью McAfee Global Threat Intelligence (McAfee GTI) — единственной в своем роде технологии McAfee, в режиме реального времени отслеживающей 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 определения 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 и McAfee Application Control с McAfee Advanced Threat Defense позволяет динамически анализировать поведение неизвестных приложений в изолированной среде («песочнице») и автоматически обеспечивать невосприимчивость конечных точек к недавно обнаруженным вредоносным программам.

Ключевые преимущества (продолжение)

- Сокращение количества циклов установки исправлений благодаря использованию белых списков и передовой технологии защиты памяти
- Своевременная установка новейших пакетов исправлений с помощью доверенных средств обновления систем
- Обеспечение защиты на подключенных и не подключенных к сети серверах, виртуальных машинах, конечных точках и устройствах с фиксированными функциями, таких как терминалы для приема платежей, а также на устаревших системах, таких как Microsoft Windows XP
- Допуск новых приложений осуществляется на основе рейтинга приложений или самостоятельно, что позволяет улучшить показатель непрерывности ведения бизнеса
- Поддержка эффективной работы пользователей и быстродействия сервера благодаря использованию экономичного решения
- Возможность легко защитить инвестиции в устаревшие системы и современные информационные технологии

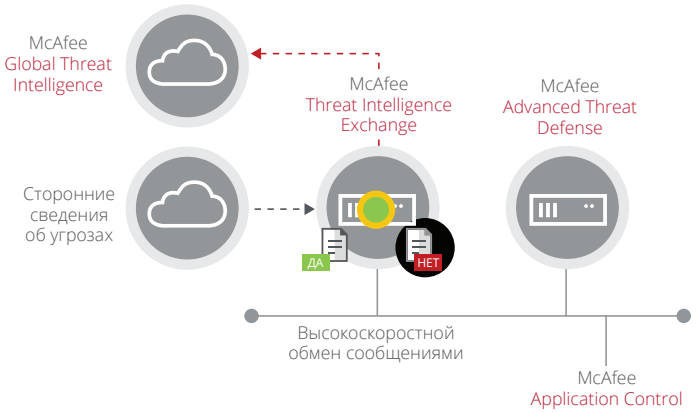

Рис. 2. McAfee GTI осуществляет непрерывный мониторинг репутации файлов и отправителей. Развертывание вместе с McAfee Threat Intelligence Exchange дает McAfee Application Control возможность автоматически обновлять белый список на основе локальной информации о репутации, а в случае необходимости получения дополнительной информации о файле координировать свои действия с McAfee Advanced Threat Defense.

Не сказывается на непрерывности ведения бизнеса

Во избежание нарушения непрерывности ведения бизнеса допуск новых приложений осуществляется автоматически на основе репутации приложений. В случае неизвестных приложений 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. Просмотрев 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

Бывают случаи, когда пользователь пытается установить неизвестное приложение. Для таких случаев в McAfee Application Control предусмотрено несколько разных возможностей:

- **Уведомление пользователей.** Пользователи получают всплывающие сообщения с пояснениями причин запрета того или иного приложения. В этих сообщениях пользователям предлагается отправить запрос (по электронной почте или через службу поддержки) на получение доступа к приложениям.
- **Право на самостоятельную установку.** Пользователи, имеющие такое право, могут устанавливать новое программное обеспечение, не дожидаясь разрешения со стороны ИТ-подразделения. Отдел ИТ оценивает эти самостоятельные пользовательские разрешения и создает корпоративные политики запрета или разрешения тех или иных приложений на уровне среды.

Поддерживаемые платформы

Microsoft Windows (32- и 64-разрядные версии)

- Встроенные: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, Embedded 8, 8.1 Industry, 10
- Серверные версии: Windows Server 2008, 2008 R2, 2012, 2012 R2
- Версии для рабочих станций: Windows NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

Своевременное обновление систем

Мы хорошо понимаем важность своевременной установки новейших пакетов исправлений. Именно поэтому мы предлагаем динамическую модель доверия, позволяющую автоматически обновлять системы, не нарушая непрерывность ведения бизнеса. В основе данной модели лежат такие понятия, как доверенные пользователи, сертификаты, процессы и каталоги. Также McAfee Application Control обеспечивает защиту включенных в белый список приложений от атак методом переполнения буфера памяти на 32-разрядных и 64-разрядных версиях Microsoft Windows.

Расширенные функции контроля выполнения

В целях повышения уровня защиты McAfee Application Control позволяет создавать комбинации правил в зависимости от имен файлов, названий процессов, названий родительских процессов, параметров командной строки и имен пользователей. Расширенные функции контроля выполнения дают возможность останавливать атаки, обходящие файловый ввод-вывод, блокировать интерактивный режим системных интерпретаторов и предотвращать использование уязвимостей системными утилитами. В дополнении к этому в вашем распоряжении оказывается более мощный и более надежный алгоритм SHA-256 для создания политик.

Программное обеспечение McAfee ePolicy Orchestrator: вся информация в одном окне

Программное обеспечение McAfee ePO позволяет консолидировать и централизовать процесс управления, давая вам полную картину ситуации с безопасностью в масштабах всей вашей компании — без «белых пятен». Эта платформа, получившая широкое признание специалистов, интегрирует McAfee Application Control с решением McAfee Host Intrusion Prevention и другими защитными продуктами McAfee, включая средства защиты от вредоносного ПО, служащие источником информации для черных списков. Простую одношаговую установку и обновление развертывания McAfee Application Control можно также выполнять из системного центра Microsoft System Center.

Режим наблюдения: смотри и учись

Режим наблюдения позволяет создавать политики для динамических сред, состоящих из настольных компьютеров, без использования фиксированного белого списка. Он позволяет проводить поэтапное развертывание программного обеспечения McAfee Application Control на стадии опытной среды и в ранней стадии производственной среды без нарушения работы приложений. McAfee Application Control дает администраторам возможность использовать единую страницу распознавания политик для создания политик, регулирующих порядок наблюдения за приложениями и порядок обработки запросов на получение права на самостоятельную установку приложений.

Защита инвестиций в устаревшие системы и новые технологии

Вам необходимо обеспечить защиту устаревших операционных систем, таких как Microsoft Windows NT, Microsoft Windows 2000 и Microsoft Windows XP? Хотя компания Microsoft и другие поставщики средств безопасности не поддерживают эти устаревшие системы, при обеспечении их защиты вы можете полностью положиться на McAfee Application Control. Кроме того, McAfee Application Control поддерживает такие недавно выпущенные операционные системы, как Microsoft Windows 10.

Дальнейшие действия

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

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