McAfee Application Control

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

Постоянные угрозы повышенной сложности в виде удаленных атак или социальной инженерии все более усложняют задачу защиты вашего бизнеса. McAfee® Application Control помогает перехитрить киберхулиганов и обеспечивает безопасность и эффективность работы вашей компании. В этом централизованно управляемом решении, работающем по принципу белого списка, используется динамическая модель доверия и инновационные функции безопасности, которые блокируют несанкционированные приложения и сводят на нет постоянные угрозы повышенной сложности (APT), позволяя при этом отказаться от трудоемкой работы по составлению списков. Вы не хотите тратить время на угрозы «нулевого дня»? Тогда потратьте немного времени на изучение McAfee Application Control.

Ключевые преимущества

- Защита от угроз «нулевого дня» и постоянных угроз повышенной сложности, не требующая обновления сигнатур
- Использование технологии McAfee Global Threat Intelligence (McAfee GTI) для подтверждения репутации файлов и приложений в масштабах предприятия
- Повышение уровня защиты и сокращение стоимости владения за счет динамических белых списков
- Эффективный контроль за доступом к приложениям с помощью централизованной платформы управления, имеющейся в программном продукте McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Сокращение количества циклов установки исправлений благодаря использованию белых списков и передовой технологии защиты памяти
- Обеспечение защиты на подключенных и отключенных серверах, виртуальных машинах (VM), конечных точках и устройствах с фиксированными функциями, таких как торговые терминалы
- Автоматический допуск нового ПО, добавленного с помощью разрешенного процесса

McAfee Application Control обеспечивает полную защиту от нежелательных приложений и кода, блокируя сложные угрозы и не требуя обновления сигнатур. Решение дает вам стабильные инструменты для допуска известных безвредных программ, блокирования известных и неизвестных вредоносных программ и правильного администрирования новых программ. Наша динамическая модель доверия на основе белых списков позволяет сокращать издержки путем отказа от дорогостоящей обработки белых списков вручную.

Один список. Никакого гадания.

Чтобы обнаружить относящиеся к приложению файлы и работать с ними, не нужно быть детективом. Разработанная нами функция инвентаризации приложений группирует все двоичные файлы (EXE, DLL, драйверы и сценарии), находящиеся в любой точке вашей компании, по приложениям и поставщикам, отображая их в интуитивно понятном иерархическом формате. Для классификации приложений используются следующие категории: известные «хорошие» (well-known), неизвестные (unknown) и известные «плохие» (known-bad). Кроме того, вы можете легко проводить поиск по интересующим вас параметрам, таким как приложения, добавленные на текущей неделе, несертифицированные двоичные файлы, файлы с неизвестной репутацией, системы с устаревшими версиями Adobe Reader и т. д. Это позволяет быстро выявлять уязвимости и подтверждать нормативно-правовое соответствие лицензий на программное обеспечение.

Помогите пользователям стать частью решения

Благодаря McAfee Application Control у ИТ-специалистов есть много способов предоставить пользователям возможность устанавливать новые приложения.

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.

intel Security

Ключевые преимущества (продолжение)

- Возможность распознавать политики доверенных средств установки обновлений до развертывания белых списков на предприятии
- Гибкая работа пользователей настольных ПК достигается за счет предоставления им права самостоятельно разрешать новые приложения
- Поддержка эффективной работы пользователей и быстродействия сервера благодаря использованию экономичного решения
- Простая возможность обеспечения защиты неподдерживаемых устаревших систем, таких как Microsoft Windows NT, Microsoft Windows 2000 и Microsoft Windows XP
- Возможность интеграции с консолью McAfee ePO с целью централизации управления ИТ

Поддерживаемые платформы

Microsoft Windows (32- и 64-разрядные версии)

- Встроенные системы: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8, 8.1 Industry
- Серверные ОС: 2008, 2008 R2, 2012, 2012 R2
- Рабочие станции: Vista, 7, 8, 8.1

Linux

- RHEL/CentOS 5, 6
- SUSE/openSUSE 10, 11
- OEL 5, 6
- Ubuntu 12.04

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 программное обеспечение McAfee Application Control с McAfee Host Intrusion Prevention, McAfee Firewall и другими продуктами McAfee для управления безопасностью и риском. Кроме того, простую одношаговую установку и обновление развертывания McAfee Application Control можно выполнять из системного центра Microsoft System Center. При этом к программному обеспечению McAfee ePO можно легко подключить продукты партнеров по McAfee Security Innovation Alliance, а также ваши собственные управляющие приложения.

Рис. 1. Помимо настольных компьютеров и серверов программное обеспечение McAfee Application Control обеспечивает защиту устройств с фиксированными функциями, что позволяет значительно сократить риск потребителя.

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.

Эффективные встроенные рекомендации

Программное обеспечение McAfee Application Control имеет интерфейс рекомендаций, предлагающий новые политики установки обновлений на основе наблюдения за приложениями, запускаемыми на конечных точках. Это превосходный способ управления исключениями, сгенерированными заблокированными приложениями. Вы можете сначала просто просмотреть все исключения и информацию о заблокированных приложениях, а затем либо допустить файл и включить его в белый список, либо проигнорировать его, если данное приложение должно быть заблокировано.

Рис. 2. Безопасный процесс обновлений

Экономия системных ресурсов и эксплуатационных расходов

McAfee Application Control является программным решением с низким потреблением ресурсов:

- Легкость настройки и низкие расходы на запуск и эксплуатацию
- Незначительный объем используемой памяти
- Процесс сканирования файлов не снижает быстродействие системы
- Поддержка изолированного и автономного режимов
- Не требует обновления сигнатур

Защита устаревших систем

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, в деле обеспечения их защиты вы можете полностью положиться на McAfee Application Control.

Минимизация работы по установке исправлений и защита памяти

Использование McAfee Application Control в сочетании с McAfee Host Intrusion Prevention позволяет изолировать трафик приложений, находящихся в сером списке. Эта проверенная контрмера позволяет откладывать развертывание пакета исправлений до следующего планового цикла установки исправлений. Также McAfee Application Control обеспечивает защиту включенных в белый список приложений от атак методом переполнения буфера памяти на 32-разрядных и 64-разрядных версиях Windows.

Интергарция с McAfee GTI — интеллигентный способ борьбы с глобальными угрозами

McAfee GTI — это уникальная 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 в McAfee Application Control для определения репутации всех файлов в вашей вычислительной среде и их классификации на «хорошие», «плохие» и «неизвестные». Возможность отслеживать репутацию файлов с помощью GTI распространяется как на защищенные изолированные среды, так и на инфраструктуры с сетевым подключением. Интеграция с технологией McAfee GTI позволит вам с уверенностью выявлять случаи непреднамеренного включения вредоносных программ в белые списки.

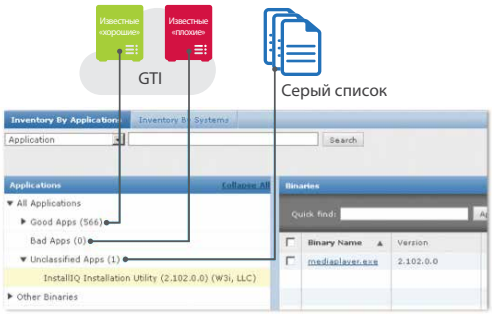

Рис. 3. McAfee Global Threat Intelligence проводит непрерывный мониторинг репутации файлов и отправителей, позволяя автоматически блокировать известные «плохие» файлы и помещать в серые списки те файлы, репутация которых не известна.

Последующие действия

Программное обеспечение McAfee Application Control — эффективный способ блокировать несанкционированные приложения и вредоносный код на серверах, корпоративных рабочих станциях и устройствах с фиксированными функциями. Централизованно управляемое решение на основе белых списков использует динамическую модель доверия и инновационные функции обеспечения безопасности, блокируя постоянные угрозы повышенной сложности, что позволяет обойтись без обновления сигнатурных баз и трудоемкого управления списками приложений. McAfee Application Control дает возможность защитить системы от неизвестных постоянных угроз повышенной сложности с помощью централизованно управляемых белых списков приложений.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com

61338ds_mac_0914_fnl_ETMG