

McAfee Application Control

Снижение риска несанкционированного использования приложений и усиленный контроль за конечными точками

Компаниям часто бывает трудно предупредить отклонение поведения рабочих станций и серверов от корпоративных стандартов. Пользователи могут несанкционированно устанавливать приложения, которые создают опасность заражения вредоносными программами, проблемы для службы технической поддержки или риск нарушения лицензий на программное обеспечение. Благодаря своей передовой технологии «белого списка», McAfee® Application Control гарантирует, что на серверах и в конечных точках выполняются только доверенные приложения, и допускает обновление программного обеспечения исключительно из авторизованных источников. Это обеспечивает ИТ-персоналу максимальную прозрачность и контроль за конечными информационными ресурсами, а также помогает гарантировать соблюдение лицензионных соглашений. Кроме того, когда компания хочет продлить срок службы систем с фиксированными функциями (устаревшие машины Microsoft Windows NT или машины с ограниченными ресурсами памяти), Application Control создает дополнительный уровень защиты без ущерба для производительности системы.

Основные преимущества

- Повышенная прозрачность и управляемость приложений в конечных точках и на серверах
- Расширение возможностей систем с фиксированными функциями
- Низкая стоимость владения, поскольку динамический «белый список» исключает ручной труд при администрировании баз данных, правил и обновлений
- Программное решение с низким уровнем нагрузки, которое прозрачно работает в конечных точках
- Повышение уровня надежности систем и обеспечение непрерывности бизнеса
- Хорошо подходит для кассовых терминалов на предприятиях розничной торговли, устройств обработки изображений в здравоохранении, а также для устаревших систем с фиксированными функциями на базе Microsoft Windows NT и Windows 2000

Сегодня ИТ-подразделения, располагая меньшими ресурсами, вынуждены выполнять повышенные требования в отношении соблюдения правил безопасности, рабочих процедур и нормативов на удаленных рабочих местах и серверах. Конечные пользователи могут непреднамеренно занести программное обеспечение, которое представляет опасность для предприятия. Организациям всех размеров необходим эффективный способ стандартизации рабочих станций и серверов без снижения производительности труда конечных пользователей, чтобы они гарантированно применяли только утвержденное программное обеспечение.

Предотвращение использования неавторизованных приложений

McAfee Application Control дополняет традиционные решения безопасности, позволяя ИТ-подразделению разрешать установку только утвержденного программного обеспечения и легко блокировать неавторизованные или уязвимые приложения, которые представляют

опасность для серверов и рабочих станций — без какой-либо дополнительной нагрузки на ресурсы системы.

Наша технология доверительной модели на основе «динамического белого списка» исключает ручные и дорогостоящие операции поддержки, характерные для других технологий с использованием «белого списка», так как не требует никаких баз данных, правил или обновлений.

Эффективность работы в контролируемой среде

ИТ-подразделения могут применять гибкую корпоративную политику безопасности, гарантирующую, что доверенные приложения можно по мере необходимости безопасно развертывать на рабочих станциях и серверах из репозитория или принудительно устанавливать стандартные образы систем. Централизованное управление ИТ снижает накладные расходы при сохранении высокого уровня безопасности и непрерывности бизнеса.

Спецификации

Операционные системы (ОС)

- Microsoft Windows NT
- Microsoft Windows 2000/2003/2008
- Microsoft Windows XP/Vista
- Microsoft Windows XPE
- Microsoft Windows XP/Vista (64-bit)
- Microsoft Windows 2003/2008 (64-bit)
- Microsoft Windows CE 6.0
- Linux RHEL 3/4/5
- CentOS 4/5
- SuSE EL 9/10
- Oracle EL 5
- Solaris 8/9/10

Гипервизоры VMware

- ESX 3.0.x/3i/3.5
- Virtual Center
- VMware Server 2.0



Рисунок 1. McAfee Application Control распространяет уровень защиты на устройства с фиксированными функциями, такие как киоски, POS-терминалы, а также на унаследованные платформы, экспоненциально снижая риск для заказчика

Усиление контроля над системами с фиксированными функциями

В регулируемых отраслях, таких как розничная торговля и здравоохранение, или на ответственных объектах инфраструктуры важную роль играют устройства типа кассовых терминалов (POS) или устаревшие системы Microsoft Windows NT, в которых часто хранятся конфиденциальные данные.

С точки зрения расхода ресурсов ЦП или памяти McAfee Application Control представляет собой идеальное решение для распространения уровня защиты на такие системы с фиксированными функциями. Оно занимает мало памяти и не влияет на производительность системы, требует очень низких затрат на установку и обслуживание и столь же эффективно при работе в автономном режиме, без доступа к сети.

Пристальный, централизованный контроль за POS-терминалами

После проверки POS-терминала на выполнение исходных условий в целях защиты целостности данных и доступности систем можно заблокировать несанкционированную установку программ и внесение изменений в эти системы.

Безопасные медицинские устройства

Уникальное сочетание малого потребления ресурсов с динамическим «белым списком» помогает уменьшить число инцидентов с устройствами отображения информации, вызванных несанкционированным внесением изменений. Защита критически важной инфраструктуры

Предотвратив несанкционированную загрузку или исполнение программного обеспечения, можно защитить от кибератак критически важные устройства и серверы на таких объектах, как электростанции и системы и диспетчерского управления и сбора данных (SCADA).

Динамический «белый список» на базе доверительной модели

Используя модель надежного источника, McAfee Application Control исключает необходимость для ИТ-администраторов вести списки авторизованных приложений вручную. К работе допускается только авторизованное ПО, и это никак нельзя изменить.



Рисунок 2. Безопасная процедура внесения изменений

Основные характеристики

- Автоматически принимает новое программное обеспечение, добавляемое посредством авторизованного процесса
- Предотвращает выполнение любого несанкционированного программного обеспечения, сценариев и динамических библиотек (DLL), а также защищает от эксплоитов в оперативной памяти
- Легко поддерживает существующие процессы внесения изменений как в подсоединенные к сети, так и в автономно работающие серверы и конечные точки
- Администраторы с физическим или удаленным доступом к машине не могут обойти защиту
- Централизованное управление еще больше уменьшает нагрузку на ИТ-персонал
- McAfee Application Control – это программное решение, которое требует очень мало издержек на обслуживание
- Простая установка и низкие первоначальные и текущие накладные расходы
- Минимальная нагрузка на процессор и менее 10 Мбайт используемой оперативной памяти
- Отсутствие сканирования каких-либо системных файлов, которое могло бы повлиять на производительность системы
- Работает в автономном режиме, без подключения к сети

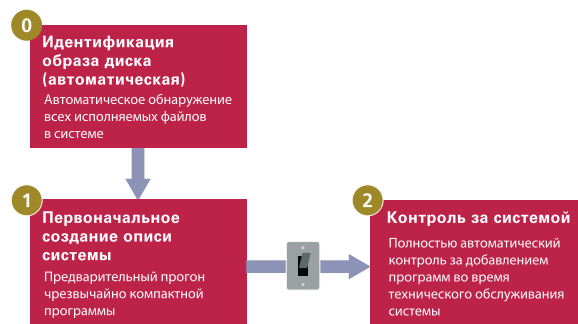


Рисунок 3. Как работает динамический «белый список».

Интеграция и совместимость с решениями McAfee

McAfee Application Control бесшовно интегрируется с McAfee Change Control, обеспечивая более строгое соблюдение корпоративной ИТ-политики. Система Change Control предотвращает внесение изменений и следит за целостностью системы в режиме реального времени, минимизируя отклонения от корпоративных стандартов.

Заказчики McAfee Total Protection for Endpoint получают также преимущества расширенного управления конечными точками и серверами. Application Control дополняет защиту на основе поведения и сигнатур, обеспечиваемую системой McAfee Host Intrusion Prevention, исключая из корпоративной среды несанкционированное программное обеспечение.

McAfee Application Control работает в сетях с различной топологией и с различными конфигурациями межсетевого экрана.

