

McAfee Complete Endpoint Protection — Enterprise

Надежная, быстрая и масштабируемая защита любых устройств от любых угроз

Ключевые преимущества

- Быстрая, первоклассная программно-аппаратная система защиты от сложных и скрытых угроз безопасности сегодняшнего дня
- Объединение средств управления всеми конечными точками, в том числе виртуальными машинами, серверами, ПК и мобильными устройствами
- Сокращение поверхности атак на приложения, экономия времени и усилий при управлении белыми списками
- Возможность устранения уязвимостей в режиме реального времени и заблаговременного блокирования угроз
- Управление рисками за счет возможности направлять ресурсы на те участки, где они больше всего необходимы

Защита конечных точек должна поддерживать, а не замедлять работу предприятий. Защитите свое предприятие и обеспечьте условия для производительной работы персонала! Комплект надежных, простых и быстрых в работе решений McAfee® Complete Endpoint Protection — Enterprise обеспечивает в режиме реального времени сбор информации о состоянии системы безопасности и уровне риска, а также механизмы единого управления. Компания McAfee предлагает самую эффективную защиту от угроз для любых ваших устройств, начиная от серверов и виртуальных машин и заканчивая ПК и мобильными устройствами, — в виде единого, интегрированного и простого в управлении решения. Защита систем и данных от сложных и скрытых угроз осуществляется за счет динамического контроля приложений, предотвращения вторжений на основе анализа поведения, мгновенного анализа рисков, программно-аппаратных средств защиты от руткитов, а также за счет применения технологии глобального сбора информации, охватывающего все направления угроз.

Комплект McAfee Complete Endpoint Protection — Enterprise помогает организациям создать эффективную систему безопасности, начиная с установки под ключ и заканчивая средствами быстрого реагирования на угрозы. Единое комплексное решение обеспечивает защиту всех устройств вашего предприятия: компьютеров ПК, Macintosh, компьютеров с Linux, виртуальных систем, смартфонов, планшетных компьютеров и серверов. Решение защищает конечные точки от руткитов, вредоносных программ для мобильных устройств, направленных атак с использованием веб-сайтов и электронной почты, а также от устойчивых угроз, одновременно упрощая управление средствами защиты и сокращая издержки. Вы получаете полнофункциональную и эффективную систему защиты и управления. Подобную систему защиты предлагает только компания McAfee, лидер на рынке средств защиты конечных точек.

Полная защита

Для защиты от угроз вы не найдете лучшего решения, чем McAfee Complete Endpoint Protection — Enterprise. В ходе недавно проведенного компанией NSS Labs тестирования, решение компании McAfee получило высшие оценки в категории технологий защиты от средств использования уязвимостей и от попыток обхода защиты.

McAfee, единственная среди всех компаний отрасли, предлагает защиту, охватывающую аппаратный и прикладной уровень, тем самым обеспечивая самую действенную защиту. В методике McAfee Deep Defender использованы технологии McAfee и Intel с целью создания передовой защиты на базе программно-аппаратных средств, работающих за пределами операционной системы. По результатам сравнительного тестирования защитных продуктов, проведенного недавно компанией AV-TEST, решение McAfee Deep Defender получило высокую оценку как средство борьбы с такими скрытыми атаками, как руткиты, который проникают глубоко в ядро системы. Ведение динамических белых списков с помощью функции контроля приложений позволяет защитить пользователей от опасных приложений и кода, связанных с угрозами «нулевого дня» и постоянными угрозами повышенной сложности (advanced persistent threat — APT).



Источник: Отчет компании AV-TEST. *Proactive Rootkit Protection Comparison Test* (Сравнительный тест упреждающих средств защиты от руткитов)

Больше знайте, больше замечайте и обеспечивайте более надежную защиту своей организации, используя облачную технологию McAfee Global Threat Intelligence™, которая в режиме реального времени обеспечивает полный сбор информации о новых и возникающих угрозах по всем направлениям угроз, таким как файлы, Интернет, почта и сетевой трафик.

Полное быстроедействие

Целенаправленное сканирование и принятие целенаправленных мер обеспечивает постоянную защиту вашего бизнеса и сводит к минимуму простои. Использование передовых методов «умного» сканирования и управления памятью, оптимизирующих потребление ресурсов ЦП и памяти, обеспечивает превосходный уровень быстрогодействия на всех платформах. При использовании функции контроля

приложений отмечается крайне низкое потребление ресурсов ЦП и памяти, которое достигается за счет отказа от избыточного сканирования и избыточных циклов обновления DAT-файлов.

Полная простота

Всего четыре щелчка мышью и 20 минут времени — и защита создана. Программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) позволяет в режиме реального времени централизованно управлять политиками на всех устройствах и получать всю необходимую информацию через единую панель управления. Real Time for McAfee ePO предоставляет вашим специалистам по безопасности мгновенный доступ к критически важным данным и таким образом скорость их реагирования на инциденты безопасности возрастает в десятки и тысячи раз.

McAfee. Лидер отрасли

- Начиная с 2007 года компания неизменно присутствует в сегменте лидеров «магического квадранта» в категории производителей платформ для защиты конечных точек. (Gartner)
- Последние четыре года компания включается в сегмент лидеров «магического квадранта» в категории производителей средств защиты данных на мобильных устройствах. (Gartner)
- Первое место по результатам тестирования продуктов для защиты от средств использования уязвимостей и атак с использованием методов обхода защиты. (NSS Labs)
- Решение McAfee продемонстрировало наилучший показатель блокирования угроз, а общий показатель защиты от средств использования уязвимостей составил 97 %. (NSS Labs)
- Показатель 100 % в сравнительном тестировании средств предупреждающей защиты от руткитов «нулевого дня» и скрытых атак на ядро. (AV-TEST)

Анатомия атаки

Фазы атаки	Как комплект McAfee Complete Endpoint Protection — Enterprise обеспечивает вашу защиту
Подготовительная фаза атаки Упреждающие меры сокращают поверхность атак и число уязвимостей.	<ul style="list-style-type: none"> Мгновенный сбор информации о степени защищенности ваших конечных точек дает вам возможность легко и эффективно сокращать поверхность атак. Приоритизация рисков осуществляется на основе обновляемой в режиме реального времени информации об угрозах, степени серьезности угроз и имеющихся мерах противодействия.
Первый контакт Вредоносная программа вступает в контакт с ничего не подозревающими пользователями, как правило, посредством вредоносного веб-сайта. К другим точкам доступа относятся съемные носители, незапрашиваемые сообщения с сайтов социальных медиа, а также незащищенные беспроводные сети.	<ul style="list-style-type: none"> Использование средств веб-защиты и фильтрация содержимого веб-сайтов снижают вероятность попутной загрузки вредоносного ПО. Механизм контроля устройств блокирует попытки использования несанкционированных носителей информации, которые могут быть заражены вредоносными программами. Механизм анализа репутации сетевых подключений блокирует атаки бот-сетей, атаки типа «отказ в обслуживании» и вредоносный трафик. Функция защиты мобильных устройств от вредоносных программ блокирует попытки взлома смартфонов и планшетных компьютеров.
Локальное исполнение На атакуемом компьютере запускается вредоносный код, целью которого является использование уязвимостей, имеющихся в приложениях или в самой операционной системе. Если вредоносной программе удается обойти функции защиты, то она получает возможность записать свой код на диск.	<ul style="list-style-type: none"> Программно-аппаратные средства защиты, работающие ниже уровня ОС, блокируют руткиты уровня ядра и уровня загрузки. Функция предотвращения вторжений на узел блокирует средства использования уязвимостей и экранирует неустранимые уязвимости. Механизм динамического контроля приложений разрешает устанавливать только известные файлы и приложения с хорошей репутацией на основе динамических белых списков. Функция сканирования при доступе осуществляет мониторинг памяти и сетевого трафика. Защищенный контейнер для мобильной электронной почты обеспечивает безопасность корпоративных данных на устройствах.
Закрепление присутствия Вредоносный код спрятан в системе и закрепляется в ней; таким образом он может «пережить» перезапуск системы и остаться скрытым от средств защиты и от пользователя.	<ul style="list-style-type: none"> Традиционные средства борьбы с вирусами и вредоносными программами. Защита от руткитов и других скрытых атак обеспечивается с помощью программно-аппаратных средств. Функция предотвращения вторжений на узел обеспечивает защиту узла во время запуска и при работе в автономном режиме.
Вредоносные действия Цель атаки достигнута. Это может быть и кража идентификационных данных, и похищение интеллектуальной собственности, и банковское мошенничество.	<ul style="list-style-type: none"> Использование установленных на узлах межсетевых экранов позволяет блокировать подключения к известным вредоносным бот-сетям и сокращать объем утечек конфиденциальных данных. Использование белых списков лишает вредоносные программы возможности вносить изменения в известные файлы приложений с хорошей репутацией, и запуск вредоносного кода становится невозможным.

McAfee Security Connected

Комплект McAfee Complete Endpoint Protection — Enterprise помогает оптимизировать уровень безопасности и риска, а также сократить издержки и повысить динамичность вашего бизнеса. С помощью разработанной компанией McAfee концепции Security Connected вы можете оптимизировать и автоматизировать процессы обеспечения защиты и управления инцидентами безопасности, тем самым сокращая расходы на обеспечение безопасности

Используя функцию динамического контроля приложений, пользователи могут устанавливать новое программное обеспечение, соблюдая требования авторизованных процессов, что позволяет избежать разочарований и задержек, связанных с ведением белых списков вручную. В комплект также включен инструмент McAfee Risk Advisor, который поможет вам легко управлять рисками и расставлять приоритеты при защите ваших самых важных активов. Приоритизация защиты от новых угроз осуществляется на основе анализа того, каким угрозам подвержены те или иные активы и имеются ли у вас соответствующие средства защиты.

Защита конечных точек во всех фазах развертывания вредоносной атаки

McAfee Complete Endpoint Protection — Enterprise объединяет в себе мощный набор предупреждающих средств, способных защитить вас от современных сложных угроз на любом этапе развертывания атаки. Здесь мы расскажем о способах снижения риска на примере типичных сценариев атак.

и исключая неэффективные операции. Благодаря возможности в режиме реального времени управлять средствами защиты, а также благодаря глобальному сбору информации об угрозах, McAfee помогает быстро и легко обнаруживать и приоритизировать угрозы, а также устранять риски, угрожающие вашему бизнесу. Получить подробную информацию можно, посетив страницу www.mcafee.com/ru/products/complete-endpoint-protection-enterprise.aspx.

Основные преимущества комплекта McAfee Complete Endpoint Protection — Enterprise

Защита от вредоносных программ (ПК, Macintosh, компьютеры с Linux, виртуальные машины, серверы)	
McAfee Deep Defender <ul style="list-style-type: none">• Блокирует руткиты и скрытые атаки с помощью функций защиты, работающих ниже уровня операционной системы.	•
Динамический контроль приложений <ul style="list-style-type: none">• Блокируют установку и запуск нежелательных приложений и вредоносных программ, минимальным образом сказываясь на производительности систем, пользователей и администраторов.	•
Система предотвращения вторжений на узлы и сетевой экран для конечных точек <ul style="list-style-type: none">• Защищает от неизвестных угроз «нулевого дня» и новых уязвимостей.• Сокращает потребность в срочной установке исправлений.	•
Global Threat Intelligence <ul style="list-style-type: none">• Обеспечивает защиту от новых и недавно появившихся угроз по всем направлениям, благодаря информации, собираемой в режиме реального времени миллионами датчиков, которые установлены по всему миру.	•
Веб-защита и защита систем обмена сообщениями	
McAfee SiteAdvisor® с функцией фильтрации URL-адресов <ul style="list-style-type: none">• Предупреждение пользователей перед посещением вредоносных веб-сайтов сокращает уровень риска и обеспечивает соблюдение нормативно-правовых требований.• Разрешение или запрет доступа к веб-сайтам.	•
Средство защиты от вредоносных программ и нежелательных сообщений для электронной почты <ul style="list-style-type: none">• Защищает сервер электронной почты и перехватывает вредоносные программы до их попадания в папку «Входящие» на компьютере пользователя.• Обнаружение, удаление и блокирование вредоносных программ на серверах Microsoft Exchange и Lotus Domino с помощью McAfee GroupShield.	•
Безопасность мобильных устройств	
Управление мобильными устройствами и средствами защиты от вредоносных программ для мобильных устройств <ul style="list-style-type: none">• Защита мобильных устройств, данных и сетей.• Простая инициализация и деинициализация учетных записей.	•
Защита данных	
Контроль устройств <ul style="list-style-type: none">• Предотвращает утечку конфиденциальных данных путем ограничения использования съемных носителей.	•
Управление и оценка рисков	
McAfee ePO и Real Time for McAfee ePO <ul style="list-style-type: none">• Управление политиками и нормативно-правовым соответствием, составление отчетов с помощью единой централизованной консоли.• Мгновенное получение информации и немедленное принятие мер по корректировке состояния защиты конечных точек.	•
Оценка рисков <ul style="list-style-type: none">• Анализ и приоритизация рисков позволяют определить уязвимость тех или иных критически важных активов к конкретным угрозам.• Мгновенное эффективное сопоставление данных о возникающих угрозах позволяет быстро определять, приняты ли необходимые меры защиты.• Сокращается количество времени, затрачиваемого на установку исправлений и диагностирование проблем.	•

