



McAfee Complete Endpoint Protection — Enterprise

Надежная, быстрая и масштабируемая защита любых устройств от любых угроз

Ключевые преимущества

- Высококласная, комплексная, многоуровневая защита, включающая передовые средства защиты от вредоносных программ, предотвращение вторжений на узел, контроль за устройствами, шифрование и т. д.
- Объединение средств управления всеми конечными точками — от виртуальных машин и серверов до ПК и мобильных устройств
- Сокращение поверхности атак на приложения, экономия времени и усилий при управлении белыми списками
- Возможность устранения уязвимостей и заблаговременного блокирования угроз в режиме реального времени
- 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, 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. Такую систему предлагает только компания McAfee — лидер на рынке средств защиты конечных точек.

Полная защита

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

Предлагаемое McAfee решение быстро обнаруживает, блокирует и устраняет вредоносные программы благодаря наличию нескольких уровней защиты, таких как передовые средства защиты от вредоносных программ, предотвращение вторжений

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 входит 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)

на узел, контроль за устройствами, установленный на узле брандмауэр, шифрование и т. д. 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).

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, таким как файлы, Интернет, почта и сетевой трафик.

Полное быстроедействие

Целенаправленное сканирование и принятие целенаправленных мер обеспечивает постоянную защиту вашего бизнеса и сводит простои к минимуму. 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.

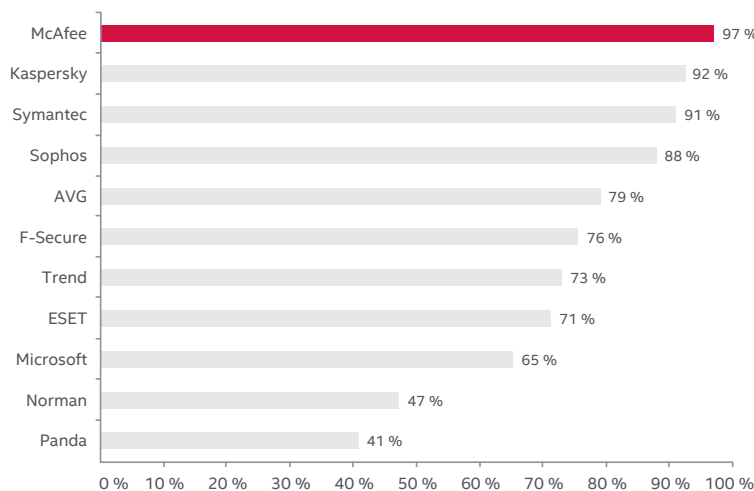


Рис. 1. Суммарные показатели блокирования угроз (включая альтернативные векторы атак)
 Источник: Отчет NSS Labs: *Corporate AV / EPP Comparative Analysis* (Сравнительный анализ корпоративных продуктов для защиты от вирусов и попыток обхода защиты), 2013 г.

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.

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.

Защита конечных точек во всех фазах развертывания вредоносной атаки

McAfee Complete Endpoint Protection — Enterprise объединяет в себе мощный набор упреждающих средств, способных защитить вас от современных сложных угроз на любом этапе развертывания атаки. Ниже показано, как наше решение минимизирует риск, на примере типичных сценариев атак.

Анатомия атаки

Фазы атаки	Как комплект McAfee Complete Endpoint Protection — Enterprise обеспечивает вашу защиту
<p>Подготовительная фаза атаки Упреждающие меры сокращают поверхность атак и число уязвимостей.</p>	<ul style="list-style-type: none"> Мгновенный сбор информации о степени защищенности ваших конечных точек дает возможность легко и эффективно сокращать поверхность атак.
<p>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 неправильно сконфигурированные или незащищенные беспроводные сети.</p>	<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.
<p>Локальное выполнение кода На атакуемом компьютере запускается вредоносный код, целью которого является использование уязвимостей, имеющихся в приложениях или в самой операционной системе. Если вредоносной программе удастся обойти функции защиты, то она получает возможность записать свой код на диск.</p>	<ul style="list-style-type: none"> 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.
<p>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.</p>	<ul style="list-style-type: none"> Традиционные средства борьбы с вирусами и вредоносными программами. Функция предотвращения вторжений на узел обеспечивает защиту узла во время запуска и при работе в автономном режиме.
<p>Вредоносные действия Цель атаки достигнута. Это может быть кража идентификационных данных, и похищение интеллектуальной собственности, и банковское мошенничество.</p>	<ul style="list-style-type: none"> Использование установленных на узлах брандмауэров 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 и исключая неэффективные операции. Благодаря возможности в режиме реального времени управлять средствами защиты и собирать информацию об угрозах в глобальном масштабе McAfee помогает быстро и легко обнаруживать и приоритизировать угрозы, а также устранять риски, угрожающие вашему бизнесу. Более подробная информация находится на сайте 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)

McAfee VirusScan® Enterprise

- Передовой продукт корпоративного класса для защиты от вредоносных программ, имеющий встроенные функции защиты от угроз «нулевого дня»

Динамический контроль приложений

- Блокирование установки и запуска нежелательных приложений и вредоносных программ с минимальным воздействием на производительность систем, пользователей и администраторов

Система предотвращения вторжений на узлы и брандмауэр для конечных точек

- Защита от неизвестных угроз, угроз «нулевого дня» и новых уязвимостей
- Сокращение потребности в срочной установке исправлений

Технология Global Threat Intelligence

- Обеспечение защиты от новых и возникающих угроз по всем направлениям, благодаря информации, собираемой в режиме реального времени миллионами датчиков, установленных по всему миру

Веб-защита и защита систем обмена сообщениями

McAfee SiteAdvisor® с функцией фильтрации URL-адресов

- 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

- Защита сервера электронной почты и перехват вредоносных программ 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

- Защита мобильных устройств, данных и сетей
- Простая инициализация и деинициализация учетных записей

Защита данных

Контроль устройств

- Предотвращение утечки конфиденциальных данных путем ограничения использования съемных носителей

Управление

McAfee ePO

- Управление политиками и нормативно-правовым соответствием, составление отчетов с помощью единой централизованной консоли



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

Intel и логотип Intel являются зарегистрированными товарными знаками Intel Corporation в США и/или других странах. McAfee, логотип McAfee, ePolicy Orchestrator, McAfee ePO и SiteAdvisor являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright © 2014 McAfee, Inc. 61570ds_complete-ep-protection-ent_1214