



McAfee Complete Endpoint Protection — Enterprise

Интеллектуальные и взаимосвязанные средства защиты для всего жизненного цикла угроз

Ключевые преимущества

- Отслеживание и сдерживание «нулевых пациентов» и вредоносных программ, способных обнаруживать «песочницу», позволяет успешно бороться с этими угрозами информационной безопасности без снижения уровня защищенности организации и без нарушения непрерывности ее работы
- Первокласное комплексное решение, включающее в себя несколько уровней защиты: взаимодействующие друг с другом интеллектуальные средства защиты конечных точек, средства предотвращения вторжений и брандмауэр для настольных компьютеров и ноутбуков, функции контроля за устройствами и т. д.

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. Мы предлагаем передовое комплексное, простое в управлении решение для защиты от угроз безопасности, которое использует локальную и глобальную информацию об угрозах для защиты систем и данных от сложных скрытых угроз с помощью средств контроля за приложениями, средств сдерживания и предотвращения вторжений на основе анализа поведения.

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: ПК, Macintosh, компьютеров с Linux, виртуальных машин и др. Решение защищает конечные точки от руткитов, 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 Intel Security, лидер на рынке средств защиты конечных точек.

Защита от сложных угроз

Для защиты от угроз не найти лучшего решения, чем McAfee Complete Endpoint Protection — Enterprise. Наша технология динамического сдерживания приложений обеспечивает защиту систем от новейших форм потенциально опасных программ, «нулевых пациентов», зараженных программами-вымогателями, и других сложных угроз до того, как они получают доступ к системам. Технология исследует поведение предполагаемых угроз, не нарушая безопасность систем. Она даже дает администратору возможность создавать собственные правила управления доступом. Кроме того, легковесность данного решения и отсутствие необходимости подключаться к облаку дают возможность обеспечивать защиту пользователей независимо от того, находятся они в сети организации или вне ее.

Ключевые преимущества (продолжение)

- Единый механизм управления средствами защиты всех ваших конечных точек: систем под управлением Windows, Macintosh и Linux, виртуальных машин
- Сокращение поверхности атак на приложения, экономия времени и усилий при управлении белыми списками
- Подробная информация об угрозах на понятном языке, позволяющая быстро принимать меры по борьбе со сложными угрозами
- Управление рисками за счет возможности направлять ресурсы на те участки, где они больше всего необходимы

Intel Security: лидер отрасли

- Лидер «магического квадранта» в категории поставщиков платформ для защиты конечных точек на протяжении тринадцати лет подряд. (Gartner)¹

Intel Security обеспечивает защиту, быстро обнаруживая и устраняя вредоносные программы благодаря наличию нескольких уровней защиты: взаимодействующих друг с другом интеллектуальных средств защиты конечных точек, средств предотвращения вторжений на настольные компьютеры и ноутбуки, функций контроля за устройствами и т. д. Ведение интеллектуальных белых списков с помощью функции контроля приложений позволяет защитить пользователей от вредоносных приложений и кода, связанных с угрозами «нулевого дня» и постоянными угрозами повышенной сложности (advanced persistent threat — APT).

Больше знайте, больше замечайте и надежнее защищайте свою организацию, используя облачную технологию McAfee Global Threat Intelligence (GTI), которая в режиме реального времени обеспечивает полный сбор информации о новых и возникающих угрозах по всем направлениям, таким как файлы, Интернет, электронная почта и сетевой трафик. McAfee GTI позволяет дополнять информацию о глобальных угрозах данными о локальных угрозах и отражать их при первом появлении. Intel Security имеет самую надежную из имеющихся на рынке служб сбора информации о глобальных угрозах безопасности. Эта служба насчитывает более 100 миллионов датчиков глобальных угроз в более чем 120 странах мира, обрабатывает более 45 миллиардов запросов в день и ежедневно анализирует свыше 1,5 миллиона файлов и 1 миллион URL-адресов.

Быстрое интеллектуальное сканирование

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 быстродействия на всех платформах. Модуль контроля за приложениями McAfee Application Control и его безсигнатурные обновления обеспечивают чрезвычайно низкое потребление ресурсов ЦП и памяти и позволяют избежать слишком частого сканирования и слишком частых циклов обновления DAT-файлов.

Простое развертывание и централизованное управление

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 динамическую модель доверия, McAfee Application Control пополняет белый список динамически, что позволяет обойтись без трудоемкого управления списками приложений.

Сбор информации, управление и реагирование на протяжении всего жизненного цикла угроз

McAfee Complete Endpoint Protection — Enterprise объединяет в себе мощный набор упреждающих средств, способных защитить вас от современных сложных угроз на любом этапе развертывания атаки.

Как работают наши средства защиты от сложных угроз

Технология	Что делает	Результаты ее работы
McAfee Endpoint Security 10	Обеспечивает обмен информацией между большим количеством разных средств защиты от угроз, позволяя обнаруживать казалось бы несвязанные между собой события, являющиеся частью одной целенаправленной атаки.	<ul style="list-style-type: none"> • Функция динамического сдерживания приложений обеспечивает защиту от программ-вымогателей, потенциально опасных программ и «нулевых пациентов» до того, как они получают доступ к системам. • Средства защиты от угроз устанавливаются друг с другом связь и обмениваются информацией о возникающих угрозах. • Используя результаты наблюдений, получаемые из разных источников, адаптивные и интеллектуальные средства сканирования обнаруживают новые виды атак и информируют друг друга об этих атаках в режиме реального времени. • Защита осуществляется на основе информации о локальных и глобальных угрозах. • При обнаружении подозрительных приложений и процессов автоматически принимаются меры реагирования, а информация о них быстро доводится до сведения ответственных лиц и передается другим средствам защиты и международному сообществу экспертов.
McAfee Threat Intelligence Exchange	Предоставляет расширенный объем информации об угрозах, как глобального характера (получаемой из глобальных источников данных и от сторонних поставщиков), так и локального характера (источником которой являются события за текущий и прошлый периоды).	<ul style="list-style-type: none"> • Компоненты защитной инфраструктуры получают дополнительную информацию об опасностях, угрожающих организациям в глобальной сети, собираемую с помощью средств защиты конечных точек, шлюзов и других компонентов защитной инфраструктуры. • Информация об угрозах, собираемая при обнаружении вредоносных программ, посредством Data Exchange Layer за несколько миллисекунд передается на все конечные точки и дает им возможность заблаговременно обеспечить невосприимчивость к угрозам. • Дает возможность менять настройки сбора информации об угрозах (списки сертификатов издателей, хэши файлов, решения о допустимых уровнях риска и т. д.), исходя из потребностей организации.
McAfee Active Response	Расширяет возможности для реагирования на инциденты безопасности благодаря интерактивному и непрерывному сбору и анализу подробной информации в реальном времени.	<ul style="list-style-type: none"> • Автоматически собирает и отслеживает изменения контекста и состояния систем, потенциально являющиеся признаком атаки или признаком наличия временно бездействующих компонентов атаки, и рассылает собранную информацию об угрозах специалистам по анализу, операциям и компьютерно-технической экспертизе. • Дает организации возможность реагировать на изменения в методах проведения атак, автоматизировать сбор данных, рассылку оповещений и порядок реагирования на интересующие объекты, а также подстраивать рабочие процессы под себя. • Постоянно работающие коллекторы срабатывают при обнаружении событий атак и оповещают администраторов и системы о злоумышленных действиях.
McAfee Application Control	Блокирует неразрешенные исполняемые файлы в корпоративных настольных компьютерах и устройствах фиксированного назначения.	<ul style="list-style-type: none"> • Используя динамическую модель доверия и инновационные функции обеспечения безопасности, решение блокирует сложные постоянные угрозы, что позволяет обойтись без обновления сигнатурных баз и трудоемкого управления списками приложений. • Интегрируется с McAfee Global Threat Intelligence, что дает пользователям возможность систематически разрешать известные безвредные приложения и код, а известные и неизвестные вредоносные приложения — блокировать. • Развертывание McAfee Application Control вместе с McAfee Threat Intelligence Exchange позволяет повысить эффективность технологии белых списков с помощью информации о локальных угрозах, дающей возможность мгновенно нейтрализовать неизвестные и целенаправленные вредоносные программы. Взаимодействие McAfee Threat Intelligence Exchange с McAfee Advanced Threat Defense позволяет динамически анализировать поведение неизвестных приложений в изолированной среде («песочнице») и автоматически обеспечивать невосприимчивость всех конечных точек к недавно обнаруженным вредоносным программам.

Примечание. McAfee Threat Intelligence Exchange, McAfee Active Response и McAfee Advanced Threat Defense представляют собой отдельные модули, которые клиенты при желании могут приобрести в дополнение к решениям McAfee Endpoint Protection.

Интегрированная архитектура Intel Security

Комплект McAfee Complete Endpoint Protection — Enterprise помогает оптимизировать уровень безопасности и риска, а также сократить издержки и повысить динамичность вашего бизнеса. Использование комплексного механизма

обеспечения безопасности и расширяемой архитектуры взаимодействующих между собой конечных точек позволяет устранить избыточность и тем самым упростить процессы управления и повысить эффективность реагирования на инциденты. Кроме того, это дает возможность централизовать управление, сократить

накладные расходы на обеспечение безопасности и заложить основу для текущего и будущего развития. Оптимизация и автоматизация процессов защиты и управления инцидентами безопасности позволяет сократить расходы на обеспечение безопасности и количество неэффективных операций. Благодаря возможности в режиме реального времени управлять средствами

защиты и собирать информацию об угрозах в глобальном масштабе Intel Security 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 Endpoint Security

- Обмен информацией с несколькими технологиями защиты конечных точек в режиме реального времени дает возможность анализировать новые и сложные угрозы и совместно с другими технологиями принимать меры реагирования, блокируя и быстро пресекая атаки до того, как они нанесут ущерб системам или пользователям
- Передовой продукт корпоративного класса для защиты от вредоносных программ, имеющий встроенные функции защиты от угроз «нулевого дня»
- Легко интегрируется с дополнительными средствами защиты от сложных угроз, такими как McAfee Active Response

Динамическое сдерживание приложений

- Надежно анализирует поведение и обеспечивает сдерживание таких угроз, как потенциально опасные программы, программы-вымогатели, «нулевые пациенты» и др., не требуя подключения к облаку

Контроль за приложениями

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

Средство предотвращения вторжений и брандмауэр для настольных компьютеров и ноутбуков

- Защита от неизвестных угроз, угроз «нулевого дня» и новых уязвимостей
- Сокращение потребности в срочной установке исправлений
- Возможность индивидуальной настройки средств защиты позволяет предотвращать случаи использования уязвимостей, атаки на память и попытки повышения уровня привилегий

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
- Мы предлагаем самую надежную из имеющихся на рынке служб сбора информации о глобальных угрозах безопасности, насчитывающую более 100 миллионов датчиков глобальных угроз в более чем 120 странах мира и позволяющую нам собирать больше информации и обеспечивать более надежную защиту

Веб-защита и защита систем обмена сообщениями

Веб-контроль с фильтрацией URL-адресов и безопасным поиском

- Предупреждение пользователей перед посещением вредоносных веб-сайтов сокращает уровень риска и обеспечивает соблюдение нормативно-правовых требований
- Применение политик посещения веб-страниц путем разрешения или блокирования 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

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
- Упрощение процессов управления защитой в средах с разными ОС с помощью кросс-платформенных политик



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

1. Первый отчет был опубликован в 2002 г. Раньше в наименованиях категорий фигурировало словосочетание «магический квадрант» среди поставщиков антивирусов корпоративного уровня.