McAfee Endpoint Protection — Advanced Suite

Защита от атак «нулевого дня» и помощь в обеспечении соответствия законодательным требованиям

Ключевые преимущества

- Защита устройств с Microsoft Windows, Mac и Linux от сетевых и системных угроз, угроз, нацеленных на данные и электронную почту, а также от рисков нарушения соответствия нормативным требованиям
- Объединение усилий по защите конечных точек и данных в едином интегрированном решении от единого производителя, что обеспечивает более надежную защиту при меньших затратах
- Мгновенное повышение уровня защиты благодаря простоте и эффективности централизованного управления и возможности подключать дополнительные средства защиты конечных точек

Наличие в штате мобильных сотрудников плюс все более жесткие нормативные требования могут превратить задачу обеспечения безопасности в настоящий кошмар. Благодаря интегрированной упреждающей системе безопасности, позволяющей бороться с вредоносными программами и атаками «нулевого дня», комплект McAfee® Endpoint Protection — Advanced Suite, входящий в линейку продуктов Intel® Security, защищает как конечные точки при их выводе за пределы корпоративной сети, так и саму сеть при их возвращении. Включенные в него средства предотвращения вторжений обеспечивают защиту настольных компьютеров и ноутбуков от сложных угроз. Централизованное управление на базе политик, поддержка нескольких платформ и функции аудита позволяют обеспечить защиту и нормативно-правовое соответствие всех ваших активов на конечных точках.

Растущая степень изощренности злоумышленников вынуждает специалистов по безопасности налаживать сбор информации о происходящем и внедрять инструменты, необходимые для обнаружения сложных угроз и принятия защитных мер. Очевидно, что любой конечной точке угрожают трудно обнаруживаемые технологии из арсенала современных киберпреступников, однако следует подчеркнуть, что переносные устройства сталкиваются с куда большими угрозами. Работа с ноутбуками часто осуществляется в отелях, кафе и домашних офисах, где отсутствуют традиционные уровни защиты, как например, веб-шлюзы и шлюзы электронной почты, брандмауэры, системы предотвращения сетевых вторжений. В сети, использующей WiFi, любой может прослушивать и получать нечто более ценное, чем просто новости.

Из-за простого отключения от корпоративной сети ПК рискуют пропустить установку пакетов исправлений и других обновлений, что делает их еще более уязвимыми к угрозам «нулевого дня». Указанные пакеты исправлений и другие обновления являются все более и более важными для соблюдения требований законодательных актов. Помимо все более строгих отраслевых нормативных

intel Security

Почему именно Intel Security?

- Процессы администрирования у нас по-настоящему централизованы.
- Встроенные в наши решения механизмы защиты и взаимодействия с конечными точками помогают устранять избыточность, предоставляют возможность для подключения других решений и образуют расширяемую архитектуру, позволяющую масштабировать систему обеспечения безопасности.
- Из всех представленных на рынке решений служба McAfee Global Threat Intelligence дает самый надежный объем информации об угрозах безопасности. Мы видим и защищаем больше, чем кто-либо другой.

требований, ваше руководство, возможно, ожидает от вас, что вы будете управлять распространением конфиденциальных данных, а также использовать Интернет надлежащим образом, находясь как на объекте, так и в пути.

Комплект McAfee Endpoint Protection — Advanced Suite дает вам возможности управления, вооружая разнообразными средствами защиты, контроля соответствия и централизованного управления. Если вы хотите защититься от вирусов, злоумышленников, отправителей нежелательной почты и охотников за данными, если вы хотите избежать нареканий аудиторов, то в нашем решении непрерывной защиты вы найдете превосходное сочетание функциональных возможностей и преимуществ экономии издержек.

Автоматизация и взаимодействие средств защиты

Организациям необходима стратегия защиты от угроз, стратегия обнаружения и устранения уязвимостей, а также механизм обеспечения безопасности, с помощью которого отдельные средства защиты смогут взаимодействовать друг с другом, способствуя быстрому обнаружению целенаправленных атак и реагированию на них. Именно поэтому включенное в комплекте решение McAfee Endpoint Security 10 в режиме реального времени взаимодействует с различными технологиями защиты конечных точек, что дает им возможность анализировать новые и сложные угрозы и совместно принимать меры реагирования, блокируя и быстро пресекая атаки до того, как они нанесут ущерб системам или пользователям. В основе решения лежит механизм, помогающий избавляться от дублирующих технологий и подключать другие решения Intel Security, упрощающие процессы управления и повышающие надежность защиты. В дополнение к этому служба McAfee Global Threat Intelligence (GTI) дает возможность использовать самый крупный из представленных на рынке объемов данных наблюдений и анализа.

Передовая защита от вирусов и нежелательной почты

Наше решение сканирует входящую и исходящую электронную почту с целью перехвата нежелательных сообщений, ненадлежащего содержимого и опасных вирусов. Подозрительные письма отправляются в карантин для предотвращения воздействия на вашу сеть и пользователей со стороны угроз, содержащихся в электронной почте. Модуль антивирусной защиты на сервере электронной почты, предотвращает попадание вредоносных программ в почтовые ящики пользователей.

Защита от угроз «нулевого дня» и уязвимостей

Забудьте об установке внеплановых исправлений! Технологии предотвращения вторжений и противодействия средствам использования уязвимостей защищают настольные компьютеры и ноутбуки от вредоносных программ, блокируют попытки вредоносного кода перехватить управление приложениями и получить повышенные привилегии, а также обеспечивают автоматическое обновление сигнатур, необходимых для защиты настольных компьютеров и ноутбуков от атак Это позволяет вам безопасно устанавливать и тестировать пакеты исправлений по собственному расписанию. Вместе с нашей запатентованной технологией защиты на основе анализа поведения, препятствующей атакам через переполнение буфера, предлагаемый нами продукт включает — по сравнению с другими сопоставимыми продуктами на рынке — защиту от самого широкого спектра опасных системных уязвимостей.

Встроенный брандмауэр

Встроенный брандмауэр позволяет блокировать незапрашиваемый входящий трафик и контролировать исходящий трафик. Для защиты настольных компьютеров и ноутбуков от бот-сетей, распределенных атак типа «отказ в обслуживании» (DDoS), сложных постоянных угроз (APT) и опасных веб-соединений используется технология

McAfee GTI. Во время запуска системы (т. е. до полной активации всей политики брандмауэра) брандмауэр пропускает только исходящий трафик, повышая тем самым уровень защиты.

Эффективный аудит политик и обеспечение нормативно-правового соответствия

Служба аудита политик, использующая для своих задач агентские модули, сканирует конечные точки и документирует актуальность применяемых политик. Организации могут соотносить свой уровень нормативно-правового соответствия с политиками, рекомендуемыми ISO 27001 и CoBIT, а также с основными отраслевыми стандартами.

Полноценное управление устройствами

Решение предотвращает утечку критически важных данных на съемных носителях, таких как USB-накопители, Apple iPod, Bluetooth-устройства, записываемые компакт-диски и DVD-диски, за пределы компании. Предлагаемые инструменты позволяют отслеживать передачу данных с настольных компьютеров и ноутбуков, а также контролировать ее вне зависимости от направления перемещения пользователей и конфиденциальных данных, даже если пользователи не подключены к корпоративной сети.

Упреждающая веб-защита

Помогает обеспечивать соответствие нормативным требованиям и снижать риск при просмотре веб-страниц, заранее предупреждая пользователей о вредоносных веб-сайтах. Веб-фильтрация на основе узлов позволяет разрешать и блокировать доступ к веб-сайтам, защищая пользователей и обеспечивая соответствие требованиям политики, вне зависимости от того, где и когда они осуществляют просмотр веб-страниц. И последнее: мы предоставляем возможность блокировать приватные URL-адреса и поддерживаем новейшие версии различных веб-браузеров.

Управление, снижающее эксплуатационные затраты

Программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) представляет собой единую централизованную платформу управления безопасностью, которая обеспечивает защиту и снижает эксплуатационные расходы. Кроме того, платформа обеспечивает эффективную работу и дает полный визуальный контроль за состоянием безопасности и уровнем нормативно-правового соответствия.

Платформа позволяет сопоставлять угрозы, атаки и события, связанные с безопасностью конечных точек, сети и данных, а также сопоставлять результаты аудитов состояния нормативного соответствия с целью повышения эффективности защитных действий и подготовки отчетов о соответствии нормативным требованиям. Никакой другой поставщик не может заявить о наличии у него единой интегрированной платформы управления, охватывающей все перечисленные аспекты защиты. ПО McAfee ePO упрощает управление безопасностью.

Скорость и легкость развертывания

Обеспечивайте повышенный уровень защиты без промедления. Благодаря установщику EASI для запуска надежной системы защиты требуется всего четыре щелчка мышью. Интеграция с McAfee ePO дает возможность развертывать средства защиты и управлять ими в рамках единой среды.

Простота миграции

В средах с текущими версиями программного обеспечения McAfee ePO, McAfee® VirusScan® Enterprise и McAfee Agent, перенос имеющихся политик в McAfee Endpoint Security 10 с помощью нашей автоматизированной утилиты занимает не более 20 минут.*

Дополнительная информация

Для получения дополнительной информации посетите страницу **www.mcafee.com/ru/products/endpoint-protection/index.aspx** или позвоните нам по телефону +7 (495) 967 76 20 (основной).

Функция	Назначение
Единая интегрированная платформа управления	Решение McAfee ePO обеспечивает постоянный сбор информации о текущем состоянии безопасности и событиях безопасности, а также прямой доступ к средствам централизованного управления всеми инструментами обеспечения безопасности и соответствия нормативам.
Многоплатформенное развертывание	Обеспечивает защиту от вредоносных программ для всего набора конечных точек (включая операционные системы Macintosh, Linux и Microsoft Windows), используемых мобильным и офисным персоналом.
Управление устройствами	Позволяет выполнять мониторинг и ограничивает копирование данных на съемные устройства и носители во избежание утраты контроля со стороны предприятия.
Средство предотвращения вторжений и встроенный брандмауэр для настольных компьютеров и ноутбуков	Предоставляет защиту от новых уязвимостей «нулевого дня», что сокращает необходимость срочной установки исправлений, управляет приложениями на настольных компьютерах, имеющими доступ в сеть, что дает возможность блокировать сетевые атаки.
Защита от вредоносных программ	Блокирует вирусы, трояны, «червей», рекламные, шпионские и другие потенциально нежелательные программы, занимающиеся кражей конфиденциальных данных и подрывающие производительность труда пользователя.
Защита от нежелательных сообщений	Помогает избавиться от нежелательных сообщений, которые ведут ничего не подозревающих пользователей на сайты, распространяющие вредоносные программы и занимающиеся фишингом.
Веб-контроль с фильтрацией URL-адресов и безопасным поиском	Помогает обеспечивать нормативно-правовое соответствие, заранее предупреждает пользователей о вредоносности открываемых веб-сайтов и защищает пользователей независимо от того, находятся они в корпоративной сети или вне ее.
Безопасность почтового сервера	Защищает ваш сервер электронной почты и перехватывает вредоносные программы до их попадания в папку «Входящие» на компьютере пользователя.
Аудит политик	Обеспечивает тесно интегрированную отчетность о соблюдении нормативных требований стандартов HIPAA, PCI и др.

* Скорость миграции зависит от имеющихся политик и характеристик среды.

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