McAfee Endpoint Threat Protection

Набор самых необходимых и эффективных средств для защиты вашей компании по мере ее роста

Нет никаких сомнений в том, что ситуация с угрозами безопасности будет усугубляться. Вы уже знаете, что обеспечение надежной защиты начинается с конечных точек. Однако обеспечить необходимый вам сегодня уровень защиты — задача не из легких. Кроме того, у вас должна быть возможность и в дальнейшем добавлять новые технологии, не прибегая к созданию сложных, изолированных друг от друга защитных операций. McAfee® Endpoint Threat Protection дает вам самые необходимые на сегодняшний день средства защиты и обеспечивает вашу готовность к борьбе со сложными угрозами завтрашнего дня. Решение объединяет в себе средства предотвращения угроз, брандмауэр и средства защиты веб-трафика, электронной почты и устройств. Взаимодействуя друг с другом в режиме реального времени, эти технологии совместными усилиями обеспечивают анализ угроз и защиту от них, блокируя и быстро пресекая атаки до того, как они нанесут ущерб системам или пользователям.

Система взаимодействующих средств защиты конечных точек

Входящие в McAfee Endpoint Threat Protection средства защиты, разработанные с учетом требований интеграции, обмениваются собираемыми в режиме реального времени данными и координируют между собой меры по выявлению и блокированию вредоносных файлов, веб-сайтов и потенциально нежелательных программ, повышая тем самым уровень защиты.

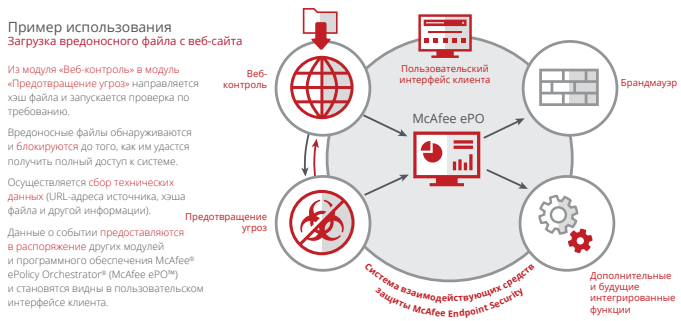

Рис.1. Как взаимодействуют друг с другом средства защиты, включенные в McAfee Endpoint Threat Protection.

Ключевые преимущества

- Использование защитных технологий, основанных на взаимодействии и обмене информацией, повышает общий уровень безопасности.
- Вы сможете по мере необходимости легко брать на вооружение дополнительные защитные функции.
- Централизованное управление, не сказывающиеся на работе пользователей операции сканирования и минимальная нагрузка на системные ресурсы позволяют повысить производительность труда.

Комплексное решение для проблем сегодняшнего и завтрашнего дня

McAfee Endpoint Threat Protection дает возможность заменить развертывания разрозненных специализированных продуктов системой взаимосвязанных и взаимодействующих друг с другом средств защиты, способных благодаря использованию различных защитных технологий обеспечивать безопасность в режиме почти реального времени. Это позволяет не только эффективнее анализировать угрозы, но и дает возможность обмениваться собираемыми компьютерно-техническими данными об угрозах с другими средствами защиты, способствуя тем самым автоматизации защитных средств и помогая им быстрее обнаруживать и блокировать угрозы на других конечных точках и в иных «точках входа».

Кроме того, этот подход допускает большую свободу выбора при развертывании решения. Вы можете установить у себя приобретенный вами продукт в полном объеме и решить, какие функции вы настроите и активируете сейчас, а какие позже. Для последующей активации необходимых вам функций достаточно будет просто внести изменения в политику.

И, наконец, благодаря своей гибкой архитектуре наша система дает вам возможность при необходимости легко брать на вооружение новые, дополнительные технологии защиты. Поэтому у вас всегда будет возможность подключить дополнительные защитные функции, позволяющие бороться с более изощренными угрозами.

Доступная цена без снижения уровня быстродействия

McAfee Endpoint Threat Protection представляет собой расширяемый набор ключевых защитных технологий. Его внедрение не приводит к усложнению операций или снижению уровня быстродействия, а, наоборот, повышает производительность вашего труда и труда ваших пользователей. Так, например, программное обеспечение McAfee ePolicy Orchestrator® (McAfee ePO™), дающее возможность централизовать работу с политиками (развертывание и мониторинг политик, управление политиками) в масштабе всей вашей среды, позволяет повысить эффективность операций. Клиенты, использующие в своих средах несколько разных операционных систем, могут повысить производительность своего труда путем использования межплатформенных политик для Microsoft Windows, Apple Macintosh и Linux. А поскольку компоненты McAfee Endpoint Threat Protection используют общий язык (Data Exchange Layer, DXL), вы получаете возможность оптимизировать процессы взаимодействия технологий и повысить скорость принятия мер реагирования на угрозы, что снизит риски благодаря сокращению «окна уязвимости».

Операции сканирования, никак не сказывающееся на работе пользователей, и оптимизированное потребление памяти и ресурсов процессора позволяют свести к минимуму потери быстродействия систем и повысить производительность труда пользователей. Интуитивно понятный пользовательский интерфейс входит в стандартный набор ПО. Он облегчает вам и вашим пользователям

Поддерживаемые платформы

- Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X версии 10.5 и выше
- 32- и 64-разрядные платформы Linux: RHEL, SUSE, CentOS, OEL, Amazon Linux и последние версии Ubuntu

Серверы:

- Windows Server (2003 SP2 и выше, 2008 SP2 и выше, 2012), Server 2016
- Windows Embedded (Standard 2009, Point of Service 1.1 SP3 и выше)
- Citrix Xen Guest
- Citrix XenApp 5.0 и выше

задачу быстрого получения аналитических данных о сути и целях принятых мер.

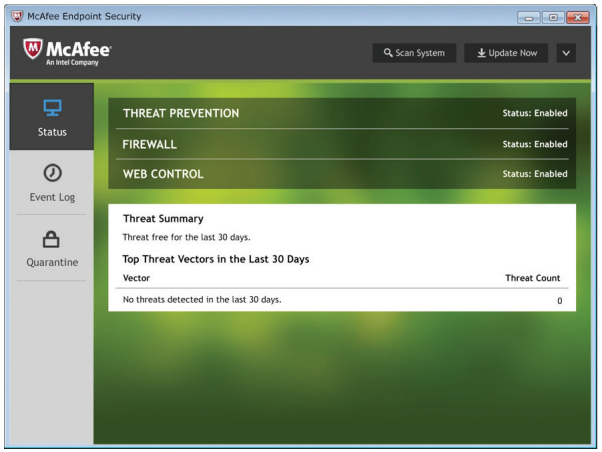

Рис.2. Интуитивно понятный пользовательский интерфейс упрощает работу администраторов и пользователей.

Компонент	Преимущество	Преимущества для клиентов	Дифференциация
Предотвращение угроз	Комплексное средство защиты, быстро обнаруживающее, блокирующее и устраняющее вредоносные программы благодаря наличию нескольких уровней защиты.	▪ Останавливает известные и неизвестные вредоносные программы с помощью методов эвристического анализа и проверки файлов при доступе. ▪ Обеспечивая защиту на платформах Windows, Mac и Linux, упрощает политики и развертывание. ▪ Отказ от проверки доверенных процессов и приоритизация подозрительных процессов позволяют повысить уровень быстродействия.	Многоуровневое средство защиты от вредоносного ПО, взаимодействующее и обменивающееся информацией со средствами веб-защиты и брандмауэром с целью повышения эффективности анализа и автоматизации процесса применения правил для блокирования потенциальных угроз.
Встроенный брандмауэр	Защищает конечные точки от бот-сетей, распределенных атак по типу «отказ в обслуживании» (DDoS), ненадежных исполняемых файлов, сложных постоянных угроз и опасных веб-подключений.	▪ Обеспечивает защиту пользователей и сохранение производительности труда путем принудительного применения ваших политик. ▪ Обеспечивает сохранность пропускной способности путем блокирования нежелательных входящих подключений и контроля над исходящими запросами. ▪ Предупреждает пользователя о доверенных сетях и исполняемых файлах, а также об опасных файлах и подключениях.	Привязка политик к используемым приложениям и местонахождению пользователей позволяет обеспечить защиту ноутбуков и настольных компьютеров, особенно в случае их нахождения за пределами корпоративной сети.

Компонент	Преимущество	Преимущества для клиентов	Дифференциация
Веб-контроль	Включает в себя средства веб-защиты и фильтрации для обеспечения безопасного посещения веб-сайтов на конечных точках.	▪ Снижает риск и обеспечивает нормативно-правовое соответствие, предупреждая пользователей о вредоносных веб-сайтах до посещения этих веб-сайтов. ▪ Предотвращает угрозы безопасности и спады производительности труда, разрешая или блокируя опасные и ненадлежащие веб-сайты. ▪ Надежно предотвращает загрузку опасных файлов, блокируя их до совершения загрузки.	Обеспечивает защиту на платформах Windows, Mac, Linux и в разных браузерах с использованием данных, поступающих от McAfee Global Threat Intelligence.
Data Exchange Layer	Обеспечивает взаимосвязанность средств защиты, позволяющую интегрировать между собой продукты McAfee и продукты сторонних производителей, а также оптимизировать обмен информацией между ними.	▪ Интеграция ведет к снижению риска и сокращению времени реагирования. ▪ Позволяет снизить накладные расходы на администрирование и обслуживающий персонал. ▪ Позволяет оптимизировать процессы и получить практические рекомендации.	▪ Обеспечивает обмен важнейшей информацией об угрозах между защитными продуктами. ▪ Мгновенно рассылает информацию об угрозе, собранную на «нулевом пациенте», всем остальным конечным точкам с целью предотвратить заражение и усилить защиту.
Управление с помощью McAfee ePO	В высшей степени масштабируемая, гибкая и автоматизированная платформа для централизованного управления политиками безопасности позволяет выявлять проблемы безопасности и принимать меры реагирования.	▪ Объединение и упрощение рабочих процессов обеспечения безопасности гарантированно ведет к повышению их эффективности. ▪ Больше информации и свободы действий для уверенного принятия мер безопасности. ▪ К вашим услугам быстро развертываемый и легко управляемый единый агент с настраиваемым механизмом применения политик. ▪ Возможность использовать динамические и автоматизированные запросы, панели мониторинга и меры реагирования позволяет сократить время между выявлением угрозы и реагированием на нее.	▪ Наличие единой консоли позволяет повысить эффективность контроля, снизить расходы и ускорить процессы управления операциями по обеспечению безопасности. ▪ Зарекомендовавший себя высококлассный интерфейс пользуется широким отраслевым признанием. ▪ На перетаскиваемых панелях мониторинга отображается информация, собираемая в масштабах всей огромной экосистемы безопасности. ▪ Открытый характер платформы позволяет быстро внедрять инновации в области ИБ.

Дополнительная информация

Дополнительную информацию о преимуществах McAfee Endpoint Threat Protection можно получить по адресу **www.mcafee.com/ru/products/endpoint-threat-protection.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru