McAfee Complete Endpoint Threat Protection

Передовые средства защиты от изощренных атак

Для борьбы с угрозами, с которыми сталкивается ваша организация, необходим подробный сбор информации и инструменты, позволяющие принимать меры безопасности и брать под контроль весь жизненный цикл защиты от угроз. Кроме того, эти инструменты должны давать вашим специалистам по безопасности возможность повысить точность принимаемых мер и надежность собираемой информацию о сложных угрозах. McAfee® Complete Endpoint Threat Protection представляет собой набор передовых средств защиты, позволяющих расследовать, сдерживать и отражать угрозы «нулевого дня» и изощренные атаки. Использование базовых средств защиты конечных точек в сочетании с функциями машинного обучения и динамического сдерживания позволяет обнаруживать угрозы «нулевого дня» в режиме почти реального времени, классифицируя и блокируя их еще до того, как они получат возможность заразить ваши системы. Оперативные данные компьютерно-технической экспертизы и отчеты позволяют вам быть в курсе происходящего, помогая перейти от реагирования на инциденты к изучению угроз и укреплению собственной защиты. А поскольку решение создано на базе расширяемой платформы, вы сможете при необходимости без труда добавлять другие передовые средства защиты от сложных угроз, как уже существующих, так и будущих.

Ключевые преимущества

- Технологии машинного обучения и динамического сдерживания позволяют опережать угрозы «нулевого дня», программы-вымогатели и потенциально опасное ПО.
- Автоматизация мер реагирования и анализа позволяет ускорить процесс устранения угроз и избежать снижения производительности труда.
- Централизованная консоль управления позволяет упростить среду, операции развертывания и процессы непрерывного управления.

Автоматизированные средства защиты от сложных угроз

Сложные угрозы необходимо пресекать до того, как они начнут действовать. Именно поэтому McAfee Complete Endpoint Threat Protection включает в себя функцию динамического сдерживания приложений и технологию Real Protect[1]. Функция динамического сдерживания приложений позволяет при обнаружении признаков вредоносного поведения автоматически сдерживать потенциально опасное ПО и подозрительные программы «нулевого дня», предотвращая тем самым заражение систем и снижение производительности

труда пользователей. Используя методы машинного обучения, технология Real Protect может расследовать и классифицировать угрозы, сохраняя собранную информацию для автоматического принятия мер реагирования на угрозы в будущем.

Упрощение системы безопасности

Как известно, сложность — враг эффективности. Теперь вам больше не придется тратить время на управление большим количеством разных специализированных решений с разными интерфейсами и консолями управления. Управление решением McAfee Complete Endpoint Threat Protection осуществляется с помощью одной-единственной консоли: программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™). Наличие единой консоли управления позволяет увеличить скорость развертывания защиты и сократить текущие расходы на управление защитой. 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.

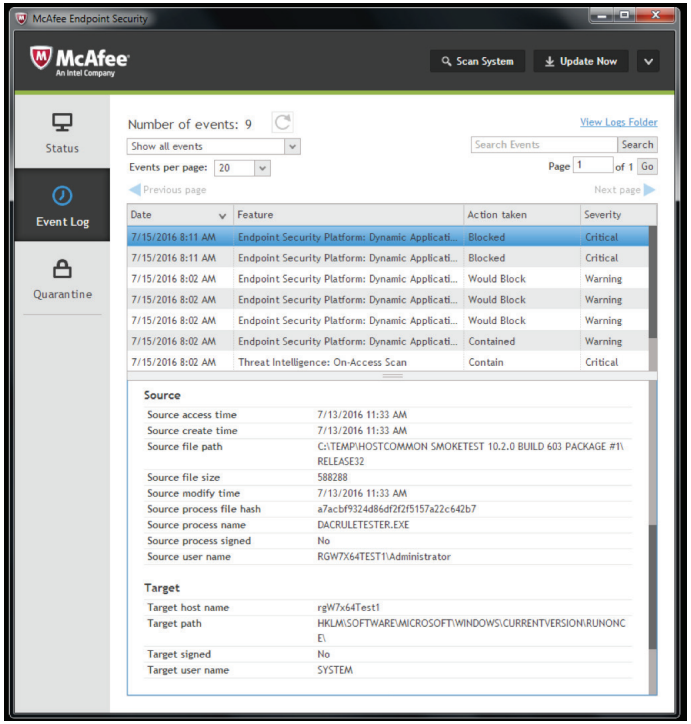

Рис. 1. Технология автоматического сдерживания приложений блокирует и сдерживает угрозы в зависимости от степени их серьезности.

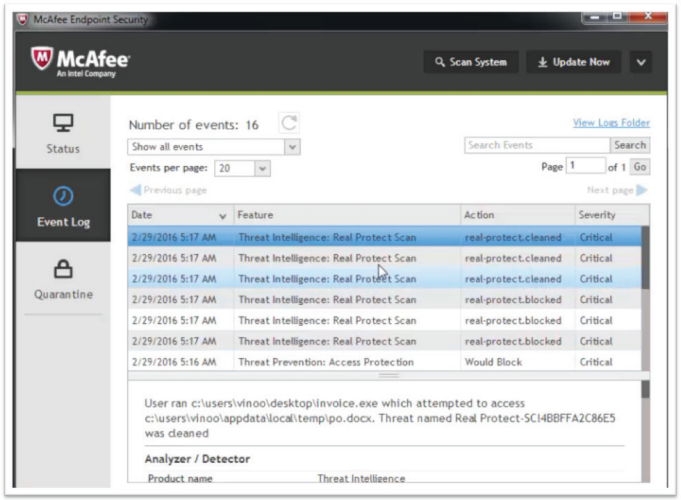

Рис. 2. Используя методы машинного обучения, Real Protect в режиме почти реального времени обнаруживает вредоносные программы «нулевого дня», зачастую необнаруживаемые путем сканирования с использованием сигнатур.

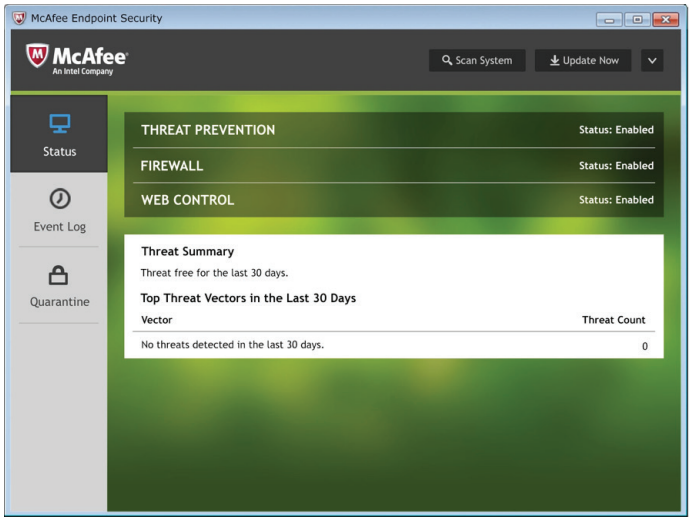

Рис. 3. Интуитивно понятный пользовательский интерфейс упрощает работу администраторов и пользователей.

Гибкая система, созданная для решения проблем сегодняшнего и завтрашнего дня

McAfee Complete Endpoint Threat Protection предоставляет в ваше распоряжение систему взаимосвязанных и взаимодействующих друг с другом средств защиты, способных благодаря использованию большого количества различных защитных технологий обеспечивать безопасность в режиме почти реального времени. Решение позволяет не только эффективнее анализировать угрозы, но и дает возможность предоставлять собираемые компьютерно-технические данные об угрозах в распоряжение других средств защиты, способствуя тем самым их автоматизации. Использование общего уровня связи дает базовым средствам защиты конечных точек возможность обмениваться информацией с передовыми средствами защиты от угроз и тем самым получать более надежные аналитические данные и веские доводы в пользу наличия угроз с момента первого столкновения с ними.

Кроме того, этот подход допускает большую свободу выбора при развертывании решения, так что вы можете установить приобретенный вами сегодня продукт в полном объеме, а потом решить, какие функции вы настроите и активируете сейчас, а какие позже, причем для активации необходимых функций впоследствии достаточно будет просто внести изменения в политику.

И, наконец, благодаря своей гибкой архитектуре наша система дает вам возможность при необходимости брать на вооружение новые, дополнительные технологии защиты.

Поддерживаемые платформы

- Microsoft 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 на базе Linux: последние версии RHEL, SUSE, CentOS, OEL, Amazon Linux и Ubuntu

Серверы:

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

Рис. 4. Принцип построения клиента McAfee для защиты конечных точек.

Компонент	Преимущество	Преимущества для клиентов	Дифференциация
Динамическое сдерживание приложений	Обеспечивает безопасность «нулевого пациента», лишая потенциально опасное ПО возможности вносить злонамеренные изменения в конечные точки.	▪ Повышение уровня защиты без снижения производительности труда пользователей и быстродействия доверенных приложений. ▪ Сокращение временного интервала между обнаружением атаки и ее сдерживанием — с минимальным ручным вмешательством. ▪ Защита «нулевого пациента» и предотвращение заражения сети.	▪ Работает как с подключением к Интернету, так и без подключения; не требует поступления данных и аналитической информации извне. ▪ Работает незаметно для пользователя. ▪ Режим наблюдения позволяет мгновенно собирать информацию об угрозах, пытающихся использовать потенциальные уязвимости внутри среды.
Real Protect	Классифицируя поведение файлов с помощью методов машинного обучения, блокирует угрозы «нулевого дня» еще до того, как они смогут запуститься в системе, а также останавливает уже запущенные угрозы, которым удалось обойти предыдущие средства обнаружения.	▪ Упрощение борьбы с вредоносными программами «нулевого дня», включая такие труднообнаружимые объекты, как программы-вымогатели. ▪ Автоматическое разоблачение, анализ и устранение угроз без необходимости ручного вмешательства. ▪ Адаптация защиты путем использования автоматизированных средств классификации угроз и инфраструктуры взаимосвязанных средств защиты.	▪ Обнаруживает вредоносное ПО, которое можно выявить только путем динамического анализа поведения. Глубокая интеграция позволяет в режиме реального времени обмениваться новыми данными о репутации и повышать эффективность работы всех защитных компонентов.
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, анализа поведения и проверки файлов при доступе. ▪ Возможность обеспечить защиту настольных компьютеров и серверов на любых системах Windows, Mac и Linux упрощает процедуры настройки политик и процессы развертывания. ▪ Отказ от проверки доверенных процессов и приоритизация подозрительных процессов позволяют повысить уровень быстродействия.	Многоуровневое средство защиты от вредоносного ПО, взаимодействующее со средствами веб-защиты и брандмауэром повышает эффективность анализа и предотвращает угрозы.
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 путем разрешения или запрета доступа к тем или иным веб-сайтам. ▪ Надежно предотвращает загрузку опасных файлов, блокируя их до совершения загрузки.	Обеспечивает защиту на платформах Windows и Mac и в разных браузерах.
Data Exchange Layer	Обеспечивает взаимосвязанность средств защиты, позволяющую интегрировать между собой продукты McAfee и продукты сторонних производителей, а также оптимизировать обмен информацией между ними.	▪ Снижение риска и сокращение времени реагирования посредством интеграции. ▪ Позволяет снизить накладные расходы на администрирование и обслуживающий персонал. ▪ Позволяет оптимизировать процессы и получить практические рекомендации.	Обеспечивает обмен важнейшей информацией об угрозах между средствами защиты.
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.	▪ Подтвержденную эффективность достигается за счет объединения и упрощения рабочих процессов защиты. ▪ 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. ▪ Интуитивно понятные панели мониторинга и отчеты позволяют сократить временной интервал 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 Complete Endpoint Threat Protection можно получить по адресу **www.mcafee.com/ru/products/complete-endpoint-threat-protection.aspx**.

1. Решение включает в себя размещенные центры обработки данных, расположенные в США и используемые для проверки репутации файлов и хранения данных, необходимых для обнаружения подозрительных файлов. Функция динамического сдерживания приложений лучше всего работает при наличии подключения к облаку, но это не является обязательным условием. Для использования функций динамического сдерживания приложений и Real Protect в полном объеме необходим доступ к облаку и действующая поддержка, причем в таком случае на них распространяются Условия предоставления облачных служб.

McAfee Together is power.

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