Семейство продуктов McAfee Endpoint Threat Defense and Response

Обнаружение вредоносного ПО «нулевого дня», защита «нулевого пациента» и борьба со сложными атаками

Для борьбы со все более и более изощренными киберугрозами необходимо новое поколение средств защиты конечных точек. Усугубление ситуации с угрозами безопасности и растущий риск обнаружения неизвестных уязвимостей заставляют организации брать во многом дублирующие друг друга и несвязанные между собой продукты и создавать из них защитные решения, не дающие полного представления о происходящем и отличающиеся чрезмерной сложностью. McAfee решает эту проблему с помощью McAfee® Endpoint Threat Defense и McAfee Endpoint Threat Defense and Response. В обоих этих решениях для обнаружения известных угроз, упреждения новых угроз, исправления уязвимостей и адаптации защиты используются методы статического анализа, анализа поведения и синтеза информации об угрозах. Благодаря открытому, комплексному подходу, в основе которого лежат обмен информацией (о происходящем и об угрозах безопасности) и упрощенные рабочие процессы, объединенные между собой защитные компоненты, работают как единое целое. Взаимосвязанные средства защиты и компьютерно-техническая информация об угрозах, позволяющая сразу принимать конкретные меры реагирования, служат надежной инфраструктурой для быстрой и уверенной классификации угроз и упреждения действий потенциальных злоумышленников.

Ключевые преимущества

- Обнаружение угроз, защита конечных точек и исправление уязвимостей с возможностью упреждающей адаптации средств защиты от вредоносных программ «нулевого дня», потенциально опасного ПО и программ-вымогателей
- Повышение эффективности защиты благодаря динамическому анализу репутации и поведения и использованию методов машинного обучения
- Сведение к минимуму потерь производительности труда пользователей и быстродействия доверенных корпоративных приложений благодаря усовершенствованным средствам защиты

Успешная борьба с вредоносными программами «нулевого дня», потенциально опасным ПО и программами-вымогателями

Динамический и статический анализ угроз с использованием усовершенствованных методов анализа репутации и поведения позволяет обнаруживать потенциальные средства использования уязвимостей и опережать новые угрозы. Синтез и применение информации об угрозах с помощью McAfee Threat Intelligence Exchange позволяют немедленно

блокировать и сдерживать угрозы и мгновенно обновлять информацию о репутации угроз для предотвращения повторных атак.

McAfee Endpoint Threat Defense и McAfee Endpoint Threat Defense and Response обезвреживают вредоносные программы «нулевого дня» путем сравнения признаков демонстрируемого вредоносного поведения с большим набором моделей угроз Real Protect, хранимых в облачной базе данных (в размещенных в США центрах обработки данных). Этот метод классификации угроз на основе анализа поведения используется для искоренения таких активных угроз, которым удалось обойти другие программные средства защиты. Информация об этих угрозах, доступ к которой предоставляется посредством программного обеспечения McAfee ePolicy Orchestrator, позволяет принимать конкретные меры по обнаружению угроз «нулевого дня» и устранению их в режиме реального времени. Использование методов динамического машинного обучения позволяет автоматически совершенствовать средства классификации угроз на основе анализа поведения, обеспечивая тем самым максимальный уровень защиты и эффективности при одновременном уменьшении рисков безопасности.

Сокращение количества событий и более быстрое устранение угроз

Сокращение количества событий безопасности, повышение количества автоматически определяемых угроз, обмен информацией об угрозах и настройка автоматических мер реагирования с использованием упреждающих уведомлений дает вашим сотрудникам возможность сосредоточиться на выполнении наиболее важных задач. Наличие упрощенных рабочих процессов облегчает задачу расследования и устранения угроз, позволяя быстрее обрабатывать события и брать на вооружение дополнительные средства защиты для повышения уровня защищенности в масштабе всей вашей организации.

Взаимосвязанные компоненты посредством McAfee Data Exchange Layer автоматически обмениваются между собой важной информацией, необходимой для обеспечения безопасности. McAfee Threat Intelligence дает вам возможность синтезировать комплексную информацию об угрозах в масштабе всей вашей экосистемы безопасности, используя для этого McAfee Global Threat Intelligence и другие, сторонние источники данных, и сразу же рассылать эту информацию на другие компоненты с целью автоматической адаптации защиты.

- Повышение скорости реагирования и количества устраняемых угроз благодаря обмену информацией об угрозах в масштабе всей вашей экосистемы безопасности
- Оптимизация расследования и разрешения инцидентов благодаря централизации рабочих процессов и наличию единой консоли управления в виде программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™)

Защита «нулевого пациента»

Вы сможете обнаруживать вредоносные программы «нулевого дня» и лишать их возможности вносить изменения в конечные точки. Модуль динамического сдерживания приложений следит за поведением потенциально вредоносного ПО и препятствует попыткам внести вредоносные изменения, чтобы эффективно блокировать средства использования уязвимостей до их реализации. Вы сможете защитить конечные точки в пределах и за пределами сети, и сдерживать вредоносное поведение с помощью средств защиты, работающих незаметно для пользователей.

Оптимизация процессов обеспечения безопасности с целью масштабирования и адаптации защиты

Для оптимизации процессов принудительного применения политик, расследования инцидентов и устранения угроз используется программное обеспечение McAfee ePO — единая централизованная консоль управления, позволяющая отслеживать происходящее во всех системах, быстро оценивать степень их защищенности и обеспечивать защиту в режиме реального времени. Наличие централизованных рабочих процессов и возможность одним щелчком мыши устранять проблемы на одной конечной точке или во всей инфраструктуре позволяют сократить затраты на мониторинг конечных точек, поиск данных и принятие мер реагирования. Используя методы машинного обучения, McAfee Endpoint Threat Defense и McAfee Endpoint Threat Defense and Response совершенствуют модели классификации поведения и мгновенно рассылают информацию об угрозах на все защитные компоненты, благодаря чему эти компоненты получают возможность бороться с новыми угрозами как единая, взаимосвязанная система. Вы сможете предотвращать повторные атаки и сдерживать потенциальные угрозы с помощью готового набора вариантов действий, позволяющего высвободить ресурсы ИТ-персонала и дать ему возможность заняться другими приоритетными задачами по управлению безопасностью.

Обнаружение, приоритизация и отражение сложных атак

McAfee Endpoint Threat Defense and Response помогает определять происхождение, масштаб и последствия атаки. Благодаря технологии McAfee Active Response решение дает возможность отслеживать, что происходит на всех конечных точках в вашей инфраструктуре, причем как в текущем, так и в ретроспективном временно́м представлении. Выявление и приоритизация признаков атаки на основе надежных контекстных данных позволяет повысить скорость реагирования.

ЛИСТ ДАННЫХ ДЛЯ СЕМЕЙСТВА ПРОДУКТОВ

Точное, быстрое и динамичное выслеживание угроз в упреждающем режиме позволяет эффективно бороться с любыми угрозами независимо от того, как они себя ведут: активно распространяются, дожидаются удобного момента или удаляют следы своих действий, чтобы избежать обнаружения. Отслеживание происходящего и контроль на основе собираемой информации позволяют точно выявлять системы, в которых пытаются закрепиться угрозы безопасности, и дает вашим специалистам по экстренному реагированию возможность сразу же принимать меры по сдерживанию и устранению угроз, сокращая «окно уязвимости» с нескольких месяцев до нескольких минут или даже миллисекунд.

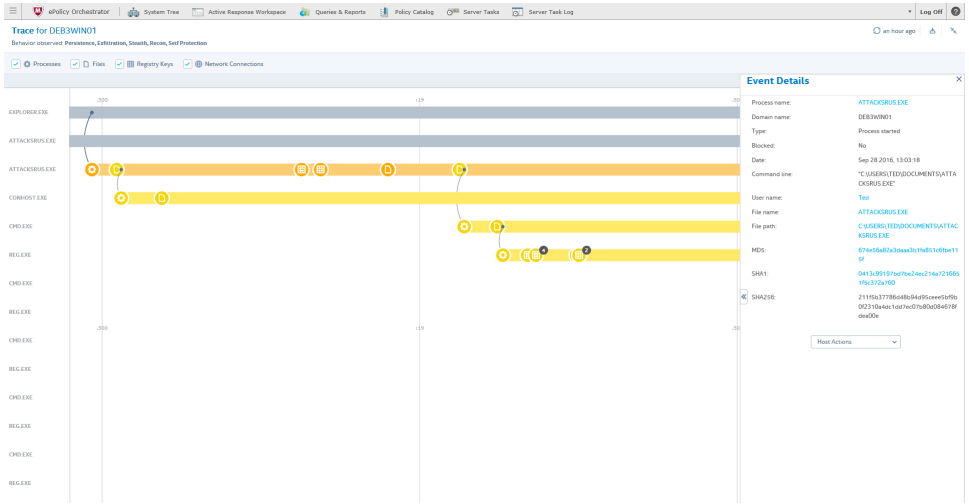

Рис. 1. Рабочая панель с информацией об угрозах позволяет отслеживать происхождение и поведение подозрительных инцидентов для более быстрого принятия мер реагирования.

Функциональные возможности семейства продуктов McAfee Endpoint Threat Defense and Response

Компонент	Преимущество	Преимущества для клиентов	Дифференциация	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Динамическое сдерживание приложений[1]	Обеспечивает безопасность «нулевого пациента», лишая потенциально опасное ПО возможности вносить изменения в конечные точки в пределах и за пределами сети.	▪ Анализ потенциальных угроз без нарушения безопасности «нулевого пациента». ▪ Повышение уровня защиты без снижения производительности труда конечных пользователей и быстродействия доверенных приложений. ▪ Сокращение временно́го интервала между обнаружением атаки и ее сдерживанием при минимальном ручном вмешательстве. ▪ Защита «нулевого пациента» и сохранение производительности конечных точек, изолирование сети от заражений.	▪ Являясь неотъемлемой частью инфраструктуры McAfee, позволяет обеспечить оптимальный уровень защиты и эффективности. ▪ 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.	√	√

ЛИСТ ДАННЫХ ДЛЯ СЕМЕЙСТВА ПРОДУКТОВ

Компонент	Преимущество	Преимущества для клиентов	Дифференциация	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Real Protect	Классифицируя поведение файлов с помощью методов машинного обучения, блокирует вредоносное ПО «нулевого дня» еще до того, как оно сможет запуститься в системе, а также останавливает активные 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.	▪ Статический и динамический анализ поведения обеспечивает более надежную защиту, чем при одноэтапных подходах. ▪ 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.	√	√
McAfee Threat Intelligence Exchange	Связывает между собой защитные компоненты, чтобы они могли обмениваться контекстной информацией, собирать информацию о происходящем и осуществлять контроль в масштабах всей организации с целью адаптивной защиты от угроз.	▪ Возможность выявлять угрозы на «нулевом пациенте» и мгновенно делиться информацией со всей системой безопасности для предотвращения повторного заражения. ▪ Снижение совокупной стоимости владения и повышение эффективности защиты конечных точек. ▪ Взаимосвязь защитных компонентов позволяет создать замкнутую систему защиты, когда независимые технологии обеспечения безопасности начинают работать как единая скоординированная система.	▪ Синтез каналов McAfee Global Threat Intelligence, сторонней и локально собираемой информации об угрозах. ▪ Определение надежности/ненадежности на основе локальной или сторонней информации об угрозах. ▪ Мгновенная передача информации о репутации угроз между продуктами для защиты конечных точек, веб-трафика, сети и облака. ▪ Возможность генерировать подробные отчеты с информацией об угрозах, позволяющие принимать конкретные меры реагирования и адаптировать средства защиты.	√	√
McAfee 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. ▪ Позволяет снизить накладные расходы на администрирование и обслуживающий персонал. ▪ Оптимизация процессов и практические рекомендации.	▪ Обмен информацией об угрозах между всеми защитными продуктами. ▪ Мгновенная рассылка информации об угрозе, собранной на «нулевом пациенте», всем остальным конечным точкам с целью предотвратить заражение и усилить защиту.	√	√

ЛИСТ ДАННЫХ ДЛЯ СЕМЕЙСТВА ПРОДУКТОВ

Компонент	Преимущество	Преимущества для клиентов	Дифференциация	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Платформа управления 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. ▪ Централизованный сбор информации обо всех системах, позволяющий оценивать степень их защищенности в режиме реального времени. ▪ К вашим услугам быстро развертываемое и легко управляемое защитное решение McAfee с настраиваемым механизмом применения политик. ▪ Сокращение временного интервала между выявлением угрозы и реагированием на нее благодаря использованию динамических автоматизированных запросов, панелей мониторинга и мер реагирования.	▪ Детальный контроль, снижение расходов и ускорение процессов управления операциями по обеспечению безопасности благодаря наличию единой консоли. ▪ Наличие перетаскиваемых панелей мониторинга позволяет лучше отслеживать происходящее в масштабах всей экосистемы в режиме реального времени. ▪ Наличие пакетов средств разработки (SDK) для открытой платформы позволяет быстро внедрять новые инновационные технологии в сфере ИБ.	√	√
McAfee Active Response	Позволяет отображать информацию об угрозах в упреждающем режиме, генерировать временны́е графики, анализировать текущие и архивные данные и обнаруживать угрозы с возможностью немедленно принимать меры и адаптировать средства защиты.	▪ Быстрый поиск информации в текущих и архивных данных для определения полного масштаба атаки, повышения скорости расследований и сокращения времени, необходимого для принятия мер реагирования. ▪ Автоматизация мер реагирования на угрозы и обеспечение постоянно актуальной защиты без ручного вмешательства. ▪ Приоритизация угроз с высоким приоритетом. ▪ Средства непрерывного мониторинга и настраиваемые коллекторы позволяют осуществлять глубокий поиск признаков не только таких атак, которые запущены или временно бездействуют, но и тех, которые были уже удалены.	▪ Мгновенная видимость неизвестных попыток использования уязвимостей и случаев опасного поведения в среде, не обнаруженных ранее с помощью защитных технологий. ▪ Возможность изучать временны́е графики событий на каждой конечной точке и встроенный поиск по всем конечным точкам в режиме реального времени для выявления угроз безопасности. ▪ Возможность одним щелчком мыши обеспечивать защиту, исправлять уязвимости и адаптировать средства защиты, заменив целый ряд разных инструментов и этапов одной-единственной операцией.		√

Спецификации

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Поддерживаемые платформы:	**Поддерживаемые платформы:**
▪ Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary	▪ Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary
▪ Mac OS X версии 10.5 и выше	▪ RedHat 6.5
▪ Linux: RHEL, SUSE, CentOS, OEL, Amazon Linux и последние версии Ubuntu	▪ CentOS 6.5
Серверы:	▪ Windows Server 2008, 2012, 2016
▪ 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	

1. McAfee Endpoint Threat Defense and Response включает в себя размещенные центры обработки данных, расположенные в США и используемые для аутентификации заказчиков, проверки репутации файлов и хранения данных, необходимых для обнаружения и выслеживания подозрительных файлов. Функция динамического сдерживания приложений лучше всего работает при наличии подключения к облаку, но это не является обязательным условием. Для использования возможностей McAfee Active Response, модуля 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.

Дополнительная информация

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

Дополнительную информацию о преимуществах McAfee Endpoint Threat Defense and Response можно получить по адресу **www.mcafee.com/ru/products/endpoint-threat-defense-response.aspx.**

McAfee Together is power.

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