McAfee ePolicy Orchestrator

Поддержка для специалистов по безопасности

Задачу управления безопасностью осложняет утомительное администрирование большого количества разных утилит и данных; при этом возможности сбора информации о внешних угрозах зачастую ограничены. Это дает противнику временное преимущество для использования брешей, незаметно возникших между средствами защиты, нанесения большего ущерба. Профессионалов в области кибербезопасности не хватает, поэтому их функции должны ограничиваться лишь управлением сложными средами кибербезопасности. Специалисты должны меньше заниматься реагированием, а больше действовать на упреждение, чтобы всегда быть на шаг впереди противников.

Вашей организации необходимо быстро реагировать на угрозы на всех типах устройств, чтобы свести ущерб к минимуму, а вам — предоставить старшему руководству подтверждение эффективности защиты. Платформа управления McAfee® ePolicy Orchestrator® (McAfee ePO™), доступная локально или в облаке (при двух возможных моделях развертывания: в качестве решения на базе технологии «программное обеспечение как услуга» (SaaS) или «инфраструктура как услуга» (IaaS)), поможет вам снизить трудоемкость и исключить возможность человеческой ошибки. При этом ваши сотрудники, ответственные за управление безопасностью, смогут реагировать на угрозы быстрее и с большей продуктивностью. Уникальным свойством консоли McAfee ePO является McAfee® MVISION Insights — первая технология, позволяющая одновременно в упреждающем режиме приоритизировать угрозы и хакерские кампании, до того как они будут реализованы, спрогнозировать, остановят ли их ваши контрмеры, и предложить конкретные рекомендации по принятию согласованных мер противодействия этой угрозе.

Ключевые преимущества

- Признанное в отрасли решение для централизованного управления значительно упрощает работу благодаря уникальной интегрированной единой панели. Решение может быть размещено в облаке или развернуто локально.
- Проактивный сбор данных для принятия практических мер защиты позволяет опережать злоумышленников.
- Автоматизированные рабочие процессы облегчают задачи администрирования и повышают эффективность.
- Открытая комплексная платформа позволяет интегрировать решения McAfee и более 150 сторонних разработчиков обеспечивая более быстрое и точное реагирование на инциденты.
- Единая система управления безопасностью дает возможность работать с большей частью устройств, представленных на рынке.
- Использует и повышает эффективность встроенных в операционные системы средств защиты, таких как Windows Defender.
- Решение масштабируется, охватывая сотни и тысячи устройств на всем пути от устройства к облаку.

Подписаться

Базовые средства защиты

Давайте начнем с обязательных компонентов. В основе любой архитектуры безопасности лежит способность отслеживать и контролировать состояние защиты устройств и систем. В отраслевых стандартах, таких как «Методы защиты и инструкции по созданию конфигураций защиты» Центра интернет-безопасности (CIS) и «Специальная публикация SP 800-53» Национального института стандартов и технологий (NIST) о мерах обеспечения безопасности и конфиденциальности информации, в качестве обязательного требования подчеркивается необходимость мониторинга и контроля инфраструктур кибербезопасности. Консоль McAfee ePO позволяет собирать критически важную информацию о происходящем, устанавливать политики и автоматизировать процесс принудительного применения политик для обеспечения надлежащего уровня безопасности в масштабе всего предприятия. Теперь вы можете без труда координировать работу многочисленных продуктов, используя для этого интегрированную единую панель для управления политиками и их применения в масштабах всего предприятия. Помимо сбора данных для принятия практических мер реагирования расширение MVISION Insights создает упреждающие рекомендации и обеспечивает возможности для усиления защиты. Эти базовые функции управления защитой имеют основополагающее значение для выполнения нормативно-правовых требований к информационной безопасности.

Проверенное передовое средство управления безопасностью — без сложностей

Консоли McAfee ePO доверяют свыше 36 000 компаний и организаций, использующих ее для управления системой безопасности, оптимизации и автоматизации процессов обеспечения нормативно-правового соответствия и усовершенствованного сбора информации об устройствах, сетях и операциях по обеспечению безопасности в целом. Крупные предприятия полагаются на высокомасштабируемую архитектуру консоли McAfee ePO, позволяющую им управлять сотнями тысяч узлов с помощью единой интегрированной панели. Панель мониторинга позволяет устанавливать приоритеты по устранению рисков и отображает сводную информацию об уровне защищенности всей вашей цифровой среды в одном графическом представлении нового рабочего пространства защиты. Кроме того, благодаря MVISION Insights вы заблаговременно получаете картину самых вероятных для вашей организации внешних угроз, а также предписывающие рекомендации относительно конкретных мер защиты. Эти уникальные возможности совершенствуют систему защиты конечных точек, трансформируя ее из реагирующей в упреждающую, и тем самым облегчая задачу управления безопасностью. Помимо указанного, к вашим услугам имеется библиотека материалов по обеспечению безопасности, в которой вы мгновенно найдете информацию о новейших угрозах и результатах их изучения.

Отраслевые аналитики утверждают, что удобство работы с McAfee ePO служит главной причиной того, что клиенты охотно внедряют у себя продукты McAfee и продолжают работать с нами.

Преимущества интегрированной платформы
Организации, использующие интегрированные платформы, защищены лучше и реагируют на угрозы быстрее, чем их партнеры, не имеющие интегрированных платформ.

Организации с интегрированными платформами

- В прошлом году 78 % организаций зафиксировали менее пяти случаев нарушения безопасности.
- 80 % организаций смогли обнаружить угрозы за восемь часов.

Организации без интегрированных платформ

- В прошлом году только 55 % организаций зафиксировали менее пяти случаев нарушения безопасности.
- Только 54 % организаций смогли обнаружить угрозы за восемь часов.

(Источник: 2016 Penn Schoen Berland)

Администраторы могут подробнее изучить то или иное событие, чтобы получить дополнительные сведения. Сводное представление сокращает время, необходимое для получения и осмысления собранных данных, а также исключает возможность ошибок даже в том случае, если потребуется ручное вмешательство. Консоль McAfee ePO упрощает для администраторов систем ИБ предприятия работу по обслуживанию политик. Кроме того, она позволяет задействовать сторонние данные об угрозах, используя для этого уровень обмена данными Data Exchange Layer (DXL), наш передовой уровень коммуникации. Помимо указанных функций, консоль обеспечивает двунаправленную интеграцию политик с целым рядом продуктов. Такая оптимизация операций позволяет сократить непроизводительные издержки, связанные с обработкой информации и обменом данными, и повысить скорость и точность реагирования.

Центр поддержки предназначен для удобного доступа к информации о продуктах McAfee и обзора состояния сервера McAfee ePO в средах клиентов. Эта информация доступна для локальной консоли McAfee ePO и для консоли McAfee ePO на Amazon Web Services (AWS). Вы можете пользоваться поддержкой и получать уведомления о продуктах в упреждающем режиме, осуществлять поиск в репозиториях контента McAfee и просматривать материалы разделов «Практические рекомендации» и «Инструкции» непосредственно из консоли McAfee ePO. Вы также можете управлять состоянием своей инфраструктуры McAfee ePO, легко выполняя оценку этого состояния, и получать список рекомендуемых шагов по его улучшению.

Эффективная открытая платформа консолидирует инфраструктуру ИТ

Полученные компанией ESG результаты исследования показывают, что для защиты от миллиардов новых угроз и для управления множеством устройств 40 % организаций используют от 10 до 25 утилит, а 30 % — от 26 до 50 утилит. Такое разнообразие используемых продуктов усложняет работу, поэтому эксплуатационная выгода введения централизованного управления всеми операциями (от установки продукта до генерирования отчетов) многократно увеличивается. Более половины организаций отмечает, что интеграция защитных утилит помогла им повысить эффективность работы более чем на 20 % (Источник: данные Института маркетинговых исследований MSI, 2018).

McAfee решает эту задачу за счет использования открытой платформы для управления системой безопасности. Платформа позволяет консолидировать разбухшую ИТ-инфраструктуру и при этом обеспечить защиту всех ваших разнообразных активов. Она поддерживает сбор информации об угрозах, управление данными из открытых источников и интеграцию сторонних продуктов. McAfee предоставляет централизованный механизм контроля, позволяющий управлять целым рядом защитных продуктов и нормативно-правовым соответствием. Возможность быстро переходить от продукта к продукту позволяет аналитикам оперативно находить критически важные данные и принимать предписанные политиками безопасности действия. Кроме того, консоль McAfee ePO позволяет

Экономия времени

Данные Института маркетинговых исследований (MSI, 2018) показывают, что клиенты считают, что смогут экономить до 20 % времени, имея интегрированные инструменты безопасности.

Интеграция в цифрах

- Повышение эффективности инструментов и процессов: 61 %
- Упрощение работы и сокращение объема ручного труда, позволяющее специалистам по безопасности сосредоточиться на задачах, требующих критического мышления: 61 %
- Повышение эффективности сбора информации за счет представления данных в виде шаблонов и в контексте: 58 %
- Оптимизация рабочих процессов для более быстрого реагирования: 57 %

(*Источник: данные Института маркетинговых исследований MSI, 2018)*

инвестировать в технологии следующего поколения и интегрировать их с имеющимися активами в рамках единой системы.

Наша открытая платформа предлагает различные подходы к интеграции (с помощью сценариев, через API-интерфейсы, без API-интерфейсов, а также с минимальными усилиями — через систему обмена сообщениями DXL с открытым исходным кодом), позволяя вам выбрать наиболее соответствующий вашим потребностям вариант, без сложной индивидуальной адаптации или громоздких служб. Благодаря программе McAfee® Security Innovation Alliance мы помогаем ускорять разработку совместимых друг с другом защитных продуктов, упрощаем задачу интеграции таких продуктов в сложные среды клиентов и создаем по-настоящему интегрированную, комплексную экосистему защиты, дающую клиентам возможность получать максимальную отдачу от уже сделанных ими инвестиций в информационную безопасность. Программа McAfee Security Innovation Alliance предлагает средства интеграции с более чем 150 решениями партнеров.

Кроме того, коммуникационный слой DXL взаимодействует с защитными продуктами различных разработчиков, а также с внутренними разработками и решениями с открытым исходным кодом, а также оптимизирует их защитные действия. Благодаря интеграции с Cisco pxGrid и DXL вы получите доступ к любым данным, собираемым 50 дополнительными защитными технологиями. Консоль McAfee ePO является ключевым компонентом управления нашей надежной открытой платформой.

Расширенный набор функций для защиты устройств. Управление встроенными инструментами безопасности

Расширяемая платформа McAfee ePO управляет множеством различных устройств, в том числе устройствами со встроенными средствами защиты. McAfee повышает эффективность защиты и совместно управляет функциями безопасности, уже встроенными в Microsoft Windows 10, обеспечивая оптимизированную защиту и одновременно позволяя организациям использовать собственные возможности системы Microsoft. Консоль McAfee ePO управляет технологией McAfee® MVISION Endpoint, сочетающей в себе расширенные функции машинного обучения, специально настроенные под собственные средства защиты ОС Microsoft, что позволяет избежать сложностей и расходов, возникающих при использовании дополнительной консоли управления. Программное обеспечение McAfee ePO предоставляет единую консоль управления, рассчитанную на совместное использование политик, для устройств под управлением Microsoft Windows 10 и всех устройств в разнородной среде предприятия, обеспечивая тем самым согласованное и простое управление.

Согласованность за счет автоматизации рабочих процессов

Консоль McAfee ePO открывает целый ряд возможностей для гибкого автоматизированного управления, позволяющих быстро и централизованно выявлять уязвимости, изменения уровня защищенности и известные угрозы, управлять ими и реагировать на них. Согласно результатам исследования, проведенного Институтом маркетинговых исследований (MSI) по заказу McAfee в 2018 году, организации ожидают, что смогут экономить приблизительно 25 % времени в день за счет автоматизации воспроизводимых или повторяющихся задач.

С помощью программного обеспечения McAfee ePO вы сможете без труда развертывать и применять политики безопасности, используя единую консоль управления, всего за несколько разворачивающихся логических шагов. Представление в виде единой панели открывает вам доступ к соответствующему контексту в ходе проработки задач. Теперь вы видите каждый шаг и его связь с другими шагами. Это упрощает работу и сводит к минимуму возможность ошибок. Вы сами определяете то, как консоль McAfee ePO будет координировать предупреждения и меры реагирования в зависимости от типа и степени критичности событий безопасности для вашей среды, а также с учетом ваших политик и утилит.

В поддержку операций по разработке и операций по обеспечению безопасности платформа McAfee ePO позволяет создавать автоматизированные рабочие процессы, объединяющие оперативные ресурсы подразделений ИБ и ИТ с целью быстрого устранения проблем. Вы можете использовать консоль McAfee ePO, чтобы инициировать меры по устранению инцидентов с помощью оперативных ресурсов ИТ, например, в виде назначения более строгих политик. Наличие сетевых прикладных программных интерфейсов (API) позволяет сократить объем работы, выполняемой вручную. У вас есть возможность запросить процесс утверждения до выпуска новой или обновленной политики или задачи, что снижает риск ошибок и обеспечивает контроль качества.

В MVISION Insights развертывается автоматизированный рабочий процесс отчетливо упреждающего характера. Общее представление о нем можно описать так: с панели мониторинга MVISION Insights автоматически отправляются предупреждения о внешних и неизвестных угрозах и хакерских кампаниях, которые приоритизируются исходя из анализа событий в конкретной отрасли и географическом регионе. В результате вы получаете прогнозную оценку того, способен ли текущий уровень защищенности вашей организации сдержать конкретную угрозу. Более того, решение предлагают конкретные действия, например обновление DAT-файлов или изолирование.

«McAfee ePO — **одно из самых первых интегрированных средств автоматизации и координации процессов обеспечения безопасности.** <...> Современным специалистам по безопасности необходимо привычное полнофункциональное ePO [ПО McAfee], но в виде упрощенного и эффективного решения... MVISION в виде рабочего пространства на базе SaaS сочетает в себе аналитическую информацию, средства управления политиками и события таким образом, который дает возможность крупным и средним компаниям использовать это решение удобным им способом».

— Фрэнк Дикинсон (Frank Dickinson), вице-президент по исследованиям продуктов обеспечения безопасности, IDC

Распространенные примеры использования

- Возможность планировать генерирование отчетов о соответствии требованиям безопасности с учетом запросов каждого заинтересованного лица позволяет сэкономить время и избавиться от избыточных и трудоемких процессов.
- Возможность работать на упреждение, собирать необходимую информацию о предполагаемых угрозах, получать сведения об их отслеживании в вашей отрасли и в вашем регионе, оценивать способность вашей актуальной системы защиты противостоять угрозам, а при неспособности — получать рекомендации по корректировке, — все это обеспечивает решение MVISION Insights.
- Простая интеграция консоли McAfee ePO в существующие бизнес-процессы и функции при помощи надежного набора интерфейсов прикладного программирования (API) помогает получать больше информации и ускорять рабочие процессы. Так, консоль McAfee ePO интегрируется, с системами обработки заявок, веб-приложениями и порталами самообслуживания.
- Возможность поддерживать необходимый уровень безопасности, развертывая агенты и базирующиеся на технологиях машинного обучения защитные решения. Добавление в корпоративную сеть новых машин выполняется путем синхронизации консоли McAfee ePO и Microsoft Active Directory.

Быстрое устранение угроз и восстановление систем

В платформу McAfee ePO встроен ряд передовых функций, повышающих эффективность сотрудников подразделений ИБ при выполнении работ по устранению угроз и восстановлению нормативно-правового соответствия систем. Функция «Автоматический ответ» консоли McAfee ePO может инициировать то или иное действие в зависимости от произошедшего события. Действия могут быть простыми уведомлениями или утвержденными мерами по восстановлению систем.

Распространенные примеры использования функции «Автоматический ответ»

- Уведомление администраторов о новых угрозах, не выполненных обновлениях или высокоприоритетных ошибках осуществляется по электронной почте или SMS исходя из заданных пороговых значений.
- Применение политик исходя из событий клиента или событий угроз, таких как политика для предотвращения обмена данными с внешним миром в случае возможного нарушения безопасности узла (это позволяет блокировать действия системы команд и управления) или блокирование эксфильтрации данных/передачи данных за пределы организации до тех пор, пока администратор не сбросит политику.

«Программное обеспечение McAfee ePO выгодно выделяется на фоне других решений. Оно служит нам единым центром защиты наших конечных точек. Вся необходимая мне информация, поступающая от всех продуктов McAfee, представлена в одной информационной панели. Простые в использовании панели мониторинга и встроенные функции значительно упрощают все задачи: сбор информации, составление отчетов, развертывание, установку обновлений, обслуживание, принятие решений».

— Кристофер Сачарок (Christopher Sacharok), инженер по информационной безопасности, Computer Sciences Corporation

- Присвоение системам тэгов и выполнение дополнительных задач нацелено на устранение уязвимостей, например, выполнение сканирований памяти по требованию в случае обнаружения угроз.
- Использование зарегистрированных исполняемых файлов применяется для запуска внешних скриптов и команд сервера, таких как создание заявки в службе поддержки или интеграция в другие бизнес-процессы.
- Автоматическое помещение в карантин рабочей нагрузки или контейнера (любого устройства) с более жесткими политиками.

Облачное управление безопасностью

Организациям необходимо упростить и ускорить развертывание решений для защиты от сложных угроз. Многие повышают эффективность работы за счет перехода на облачное управление безопасностью, которое избавляет от необходимости обслуживать локальную инфраструктуру и нести расходы по поддержанию ее доступности. Консоль McAfee ePO может быть установлена из облака в любое время из любой точки мира посредством двух альтернативных вариантов развертывания: программное обеспечение McAfee ePO на AWS или McAfee® MVISION ePO™. В обоих случаях установка и запуск займут менее часа.

- Программное обеспечение McAfee ePO на AWS позволяет организациям использовать многие встроенные функции AWS, например автоматическое масштабирование и службу реляционных баз данных Amazon RDS, избавляя их от необходимости приобретать отдельную базу данных и управлять ею. Это позволяет администраторам сосредоточиться на критически важных задачах по обеспечению безопасности, не отвлекаясь на управление инфраструктурой. Программное обеспечение McAfee ePO на AWS обеспечивает управление решениями McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, DXL и решениями сторонних разработчиков, интегрированными в программное обеспечение McAfee ePO.
- MVISION ePO опирается на преимущества решения McAfee ePO на базе технологии «программное обеспечение как услуга» (SaaS), что значительно упрощает управление платформой, позволяя вам заниматься критически важными задачами по обеспечению безопасности. Обновления платформы выполняются в прозрачном режиме на основе модели непрерывного развертывания. Решение для защиты устройств развертывается автоматически во всех подразделениях предприятия после установки агента, избавляя вас от необходимости выполнять установку или обновления вручную на каждом устройстве и обеспечивая более строгое применение политик для защиты от угроз безопасности. Это позволяет предприятиям управлять решениями McAfee MVISION Endpoint и DXL с помощью единой консоли из любой точки мира.

MVISION ePO помогает вашим устройствам анализировать критически важную информацию, собираемую при помощи решения для управления информацией о безопасности и событиями безопасности (SIEM). Благодаря этому анализу соответствующие данные всегда находятся под рукой у ваших аналитиков, что совершенствует поиск и устранение угроз. Кроме того, существующие клиенты, использующие локальное программное обеспечение McAfee ePO или решение на базе гибридного облака, теперь могут легко и быстро перейти на MVISION ePO и в полной мере воспользоваться многими преимуществами платформы для управления безопасностью на базе технологий SaaS.

Продукты McAfee, управляемые через программное обеспечение McAfee ePO

Продукты McAfee*
McAfee® Endpoint Protection (модули предотвращения угроз, веб-контроля и брандмауэра)
McAfee MVISION Endpoint дополняет Microsoft Windows Defender защитой от сложных угроз (Advanced Threat Protection)
McAfee® MVISION Mobile
McAfee® MVISION Insights
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)
McAfee® Data Loss Prevention (McAfee® DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**Для локально развертываемой версии программного обеспечения McAfee ePO*

Гибкое развертывание

Тип развертывания	Основное преимущество
Локально развертываемая платформа McAfee ePO	Полный контроль данных и набор функций
McAfee ePO на AWS	Избавляет вас от необходимости обслуживать аппаратное обеспечение, необходимое при локальном развертывании
McAfee® MVISION ePO Программное обеспечение как услуга*	Мультиарендное «программное обеспечение как услуга» (SaaS) позволяет полностью отказаться от обслуживания инфраструктуры и установки новых версий

**На McAfee MVISION ePO доступен не весь функционал программного обеспечения McAfee ePO.*

Примеры использования. Как консоль McAfee ePO позволяет централизованно управлять системой безопасности

Продукт и технология	Пример использования	Преимущество
MVISION ePO MVISION Endpoint Microsoft Windows 10	Программное обеспечение McAfee MVISION ePO обеспечивает управление решением McAfee MVISION Endpoint, дополняющим встроенные средства защиты Microsoft Windows 10 инструментами передовой защиты. Вы можете легко обнаруживать сложные угрозы и управлять ими с помощью общей платформы управления и согласованных политик для Microsoft Windows и McAfee Endpoint Security.	Усовершенствованная защита для встроенных средств Microsoft Windows и более эффективное управление, доказавшее свою надежность.
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security обнаруживает на конечной точке известный вредоносный файл. Консоль McAfee ePO вводит в отношении этой конечной точки более строгую политику и помещает ее в карантин. Эти действия выполняются в одном общем интерфейсе управления.	Быстрое сдерживание инфицированных конечных точек
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager обнаруживает на конечной точке значительную эксфильтрацию данных и помечает эту конечную точку в консоли McAfee ePO. Консоль McAfee ePO применяет политики защиты от утечки данных, позволяющие блокировать данные, и информирует пользователя о нарушении нормативно-правовых требований.	Автоматическое принудительное применение политик защиты от утечки данных
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insights	McAfee MVISION Insights предлагает практическую информацию о предполагаемых внешних угрозах с указанием их приоритетов. MVISION Insights обращается к McAfee® MVISION EDR, чтобы получить признаки взлома и выполнить их поиск. Задача состоит в том, чтобы с помощью имеющихся средств проведения расследований установить их наличие в данной среде. Если признаки взлома будут обнаружены, специалисты получат подробную информацию о соответствующей хакерской кампании и о том, какие меры можно предпринять.	Ускоренное расследование и устранение угроз

Примеры интеграции

Продукт и технология	Пример интеграции	Преимущество
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security помечает подозрительный узел. Консоль McAfee ePO может запустить дополнительные проверки. Данная информация с помощью PxGrid и DXL (через консоль McAfee ePO) передается в Cisco ISE. Cisco ISE может изолировать узел до тех пор, пока он не будет признан приемлемым.	Повышенный уровень упреждающей защиты
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO направляет список активов в систему управления уязвимостями Nexpose. Это дает вам возможность с помощью консоли McAfee ePO получать представление об имеющихся рисках и соответствующим образом устанавливать политику. Данные об уязвимостях рассылаются всем разработчикам, подключенным к DXL.	▪ Упрощение работы ▪ Комплексная и надежная система защиты; приоритизация мер по минимизации риска из одной панели управления
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Интеграция способствует двунаправленному обмену информацией об угрозах между сетью и конечными точками в режиме реального времени. События рассылаются всем, кто подключен к DXL. «Программный блейд» Check Point Anti-Bot блокирует трафик, идущий от центров управления бот-сетями, и направляет предупреждения программному обеспечению McAfee ePO, а также передает другим интегрированным защитным решениям сторонних разработчиков обычную информацию DXL. Благодаря такому сбору информации, McAfee автоматически запускает соответствующий восстановительный рабочий процесс для конечных устройств. Check Point и McAfee могут также обнаруживать и предотвращать атаки «нулевого дня» и преобразовывать их в известные атаки вне зависимости от того, исходят ли эти атаки из сети или из конечной точки. Благодаря обмену информацией, критически важной для выполнения поставленных задач, в режиме реального времени интеграция позволяет соответствующим продуктам обнаруживать, блокировать и устранять угрозы в автоматическом режиме.	▪ Сокращается время на обнаружение угроз ▪ Блокирование и устранение атак

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