

McAfee ePolicy Orchestrator

Поддержка для специалистов по безопасности

Задачу управления безопасностью усложняет утомительное администрирование большим количеством разных утилит и данных. Это дает противнику преимущество, а именно больше времени для использования брешей, незаметно возникших между средствами защиты, для нанесения большего ущерба. Профессионалов в области кибербезопасности не хватает, поэтому ваша задача состоит в том, чтобы упростить их действия при координации сложных сред кибербезопасности.

Вашей организации необходимо быстро реагировать на угрозы на всех типах устройств, чтобы свести ущерб к минимуму, а вашему руководству требуется подтверждение эффективности защиты. Платформа управления McAfee® ePolicy Orchestrator® (McAfee ePO™), доступная локально или в облаке, поможет вам снизить трудоемкость и исключить риск ошибки, связанной с человеческим фактором, а ваши сотрудники, ответственные за управление безопасностью, смогут реагировать на угрозы быстрее и с большей продуктивностью.

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, подчеркивается необходимость мониторинга и контроля инфраструктур кибербезопасности в качестве обязательного требования. Консоль McAfee ePO позволяет собирать критически важную информацию о происходящем, устанавливать политики и автоматизировать процесс принудительного применения политик для обеспечения надлежащего уровня безопасности

Ключевые преимущества

- Признанное в отрасли централизованное управление с помощью уникальной интегрированной единой панели значительно упрощает работу и осуществляется как из облака, так или локально.
- Автоматизированные рабочие процессы облегчают задачи администрирования и повышают эффективность.
- Открытая комплексная платформа позволяет интегрировать решения McAfee и более 150 сторонних поставщиков, обеспечивая более быстрое и точное реагирование на инциденты.
- Единая система управления безопасностью позволяет работать с большей частью устройств, представленных на рынке.
- Использует и повышает эффективность встроенных в операционные системы средств защиты, таких как Windows Defender.

Подписаться



ЛИСТ ДАННЫХ

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. Эти базовые функции управления защитой имеют основополагающее значение с точки зрения выполнения нормативно-правовых требований к информационной безопасности.

Проверенное передовое средство управления безопасностью — без сложностей

Консоли McAfee ePO доверяет свыше 36 000 компаний и организаций, использующих ее для управления системой безопасности, оптимизации и автоматизации процессов обеспечения нормативно-правового соответствия и более полного сбора информации об устройствах, сетях и операциях по обеспечению безопасности. Крупные предприятия полагаются на высокомасштабируемую архитектуру консоли McAfee ePO, позволяющую им управлять сотнями тысяч узлов с помощью единой интегрированной панели. Панель мониторинга позволяет установить приоритеты задач, связанных с рисками, и отображает сводную информацию об уровне защищенности всей вашей цифровой среды в одном графическом представлении нового рабочего пространства защиты.

Для получения дополнительной информации администраторы могут изучить определенные события более подробно. Сводное представление сокращает время, необходимое для создания отчетов и анализа имеющейся информации,

а также исключает риск ошибок даже в случае, если потребуется ручное вмешательство. Консоль McAfee ePO предоставляет администратору систем ИБ предприятия возможность упростить процесс обслуживания политик, задействовать сторонние данные об угрозах, используя для этого уровень обмена данными [Data Exchange Layer \(DXL\)](#), наш передовой уровень коммуникации, и обеспечить 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.

Эффективная открытая платформа консолидирует инфраструктуру ИТ

Полученные [компанией ESG](#) результаты исследования показывают, что для защиты от миллиардов новых угроз и для управления устройствами 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 отмечают, что интеграция защитных утилит помогла им повысить эффективность работы более чем на 20 % (см. опубликованное в 2018 году исследование Института маркетинговых исследований — MSI). McAfee решает эту задачу за счет использования открытой платформы для

Ключевые преимущества (продолжение)

- Решение масштабируется, охватывая сотни и тысячи устройств на всем пути от устройства к облаку.
-

Отраслевые аналитики утверждают, что клиенты внедряют у себя продукты McAfee и продолжают работать с McAfee благодаря удобству работы с программным обеспечением McAfee ePO.

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 обнаруживали угрозы за восемь часов.

ЛИСТ ДАННЫХ

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 действия. Кроме того, консоль McAfee ePO позволяет инвестировать в технологии следующего поколения и интегрировать их с имеющимися активами в рамках единой среды.

Наша открытая платформа предлагает разные подходы к интеграции (выполнение сценариев, API-интерфейсы, отсутствие API-интерфейсов и минимальные усилия при использовании системы обмена сообщениями DXL с открытым исходным кодом), позволяя вам выбрать наилучший из них, соответствующий вашим потребностям, 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 Data Exchange Layer (DXL) взаимодействует с защитными продуктами разных поставщиков 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. 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. Программное обеспечение McAfee ePO управляет технологией McAfee® MVISION Endpoint, сочетающей в себе расширенные функции машинного обучения, специально настроенные под собственные средства защиты ОС Microsoft, и в то же время позволяет избежать сложностей и расходов, возникающих при использовании дополнительной консоли управления.

Организации без интегрированных платформ

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

Источник: Penn Schoen Berland, 2016 г.

Экономия времени

Недавнее исследование Института маркетинговых исследований (MSI), опубликованное в 2018 году, показывает, что клиенты считают, что смогут сэкономить 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: Исследование MSI за 2018 год

ЛИСТ ДАННЫХ

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 согласованность и простоту действий.

Согласованность через автоматизацию рабочих процессов

Программное обеспечение McAfee ePO открывает целый ряд возможностей для гибкого автоматизированного управления, позволяющих быстро выявлять уязвимости, изменения уровня защищенности и известные угрозы, управлять ими и реагировать на них из одной-единственной консоли. Исследование, проведенное Институтом маркетинговых исследований (MSI) по заказу McAfee в 2018 году, говорит о том, что 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 с легкостью разворачивать и применять политики безопасности, используя единую панель 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 риск 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 в зависимости от ваших политик и утилит. Для поддержки 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 систем эксплуатации 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.

Распространенные примеры использования

- Возможность планировать генерирование отчетов о соответствии требованиям безопасности с учетом запросов каждого заинтересованного лица экономит время и избавляет от избыточных и трудоемких процессов.
- 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. Эта консоль интегрируется, например, с системами обработки заявок, веб-приложениями и порталами самообслуживания.

ЛИСТ ДАННЫХ

- Поддерживайте необходимый уровень безопасности, развертывая агенты или базирующиеся на технологиях машинного обучения защитные решения. При появлении в корпоративной сети новых систем они добавляются в систему путем синхронизация 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» 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.

- Присвоение системам тэгов и выполнение дополнительных задач нацелено на устранение уязвимостей, например, сканирования 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 и нести расходы по поддержанию доступности локальной инфраструктуры. Программное обеспечение McAfee ePO может быть установлено из облака в любое время из любой точки мира посредством двух альтернативных вариантов развертывания: программное обеспечение McAfee ePO на Amazon Web Services (AWS) или McAfee MVISION ePO. В обоих случаях установка и запуск займут менее часа.

«McAfee ePO — одно из самых первых интегрированных средств автоматизации и координации процессов обеспечения безопасности. ... современным специалистам по безопасности необходим привычный полнофункциональный ePO, 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 удобно использовать это решение».

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

ЛИСТ ДАННЫХ

- 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 управляет решениями McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, Data Exchange Layer и решениями сторонних поставщиков, интегрированными в программное обеспечение McAfee.
- McAfee® MVISION ePO опирается на преимущества решения McAfee ePO на базе технологии «программное обеспечение как услуга» (SaaS). Это 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 Data Exchange Layer с помощью единой консоли из любой точки мира. McAfee MVISION ePO позволяет 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.

Продукты McAfee, управляемые через McAfee ePO

Продукты McAfee*
McAfee® Endpoint Protection (модули предотвращения угроз, веб-контроля и брандмауэра)
McAfee MVISION Endpoint дополняет Windows Defender защитой от сложных угроз (Advanced Threat Protection)
McAfee® MVISION Mobile
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 McAfee ePO

«Программное обеспечение McAfee ePO выгодно выделяется на фоне других решений. Оно служит нам „единым центром“ защиты наших конечных точек. Вся необходимая мне информация обо всех продуктах McAfee видна мне 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

ЛИСТ ДАННЫХ

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, что требуется при локальном развертывании
McAfee MVISION ePO Программное обеспечение ePO 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 ePO

Примеры использования. Как консоль позволяет централизованно управлять системой безопасности

Продукт и технология	Пример использования	Преимущество
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	Программное обеспечение McAfee MVISION ePO управляет 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. Платформа объединяет встроенные средства 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. Выполняются эти действия 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 потери данных, позволяющие блокировать данные, и информирует пользователя о нарушении нормативно-правовых требований.	Автоматическое принудительное применение политики защиты от потери данных

Примеры интеграции

Продукт и технология	Пример комплексного использования решений	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. Посредством PxGrid и DXL (через консоль McAfee ePO) данная информация 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 поставщикам, подключенным к DXL.	<ul style="list-style-type: none"> ▪ 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 двустороннему 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 передает программному обеспечению McAfee ePO, а также другим интегрированным защитным решениям сторонних поставщиков предупреждения по общим вопросам 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.	<ul style="list-style-type: none"> ▪ Сокращается время на обнаружение угроз ▪ Блокирование и устранение атак

Функции и преимущества технологий McAfee зависят от конфигурации системы и могут потребовать активации аппаратного обеспечения, программного обеспечения или услуги. Ни одна компьютерная система не может быть полностью защищенной.

McAfee не контролирует и не проверяет результаты тестов производительности или веб-сайты третьих сторон, на которые имеются ссылки в настоящем документе. Рекомендуем вам самостоятельно посетить указанные веб-сайты и проверить, являются ли эти результаты точными.



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

McAfee, логотип McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2018 McAfee, LLC. 3952_0718
ИЮЛЬ 2018 г.