McAfee ePolicy Orchestrator

Централизация работы с информацией о безопасности: сбор, визуализация, обмен и принятие мер

Задачу управления безопасностью осложняет утомительное администрирование большим количеством разных утилит и данных. Это дает противнику преимущество, т. е. больше времени для использования бреши, незаметно возникшей между разными средствами защиты, и для нанесения ущерба. Кроме того, на рынке труда наблюдается нехватка специалистов по кибербезопасности, поэтому для управления сложными системами ИБ их приходится дополнительно обучать. Использование платформы управления McAfee® ePolicy Orchestrator® (McAfee ePO™) позволяет сократить трудозатраты, устранить риск человеческой ошибки и повысить скорость и эффективность управления средствами защиты.

Базовые средства защиты

Начать следует с базовых средств защиты. В основе любой архитектуры безопасности лежит способность отслеживать и контролировать состояние конечных точек и систем. Это — обязательное требование таких отраслевых стандартах конфиденциальности и безопасности, как **CIS Controls** Центра интернет-безопасности (CIS) и **NIST SP 800-53** Национального института стандартов и технологий США (NIST). 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. Управление политиками и принудительное применение политик всех защитных продуктов в масштабе всего предприятия осуществляется из единой консоли, что упрощает задачу управления большим количеством различных продуктов. Эти базовые средства защиты имеют основополагающее значение с точки зрения выполнения нормативно-правовых требований к информационной безопасности.

Подписаться

Проверенное передовое средство управления безопасностью

Консоли McAfee ePO доверяет свыше 30 000 компаний и организаций, использующих ее для управления системой безопасности, оптимизации и автоматизации процессов обеспечения нормативно-правового соответствия и более полного сбора информации о конечных точках, сети и операциях по обеспечению безопасности. В высшей степени масштабируемая архитектура консоли McAfee ePO дает крупным предприятиям возможность управлять сотнями и тысячами узлов из одной-единственной консоли. 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), 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.

Эффективность и консолидация

Результаты **опроса компанией ESG**, показали, что для защиты от миллиардов новых угроз и для управления устройствами в 40 % организаций используется от 10 до 25 утилит, а в 30 % — от 26 до 50 утилит. Такое разнообразие используемых продуктов усложняет работу и, как следствие, увеличивает эксплуатационную выгоду централизованного подхода к управлению всеми операциями от установки продукта до генерирования отчетов. McAfee решает данную задачу с помощью концепции управления безопасностью «Together is Power», которая позволяет консолидировать используемые на предприятии продукты и при этом обеспечить защиту всего многообразия имеющихся активов, сбор информации об угрозах, управление данными из открытых источников и интеграцию сторонних продуктов. McAfee предоставляет централизованный механизм управления и контроля, позволяющий управлять целым рядом защитных продуктов и обеспечивать их нормативно-правовое соответствие. Возможность быстро переходить от продукта к продукту позволяет оперативно находить критически важные данные и принимать предписанные политикой меры. Кроме того, консоль McAfee ePO позволяет инвестировать в технологии следующего поколения и интегрировать их с имеющимися активами в рамках единой системы.

Примерный список продуктов, управляемых с помощью McAfee ePO

Продукты McAfee	Сторонние продукты
McAfee Endpoint Protection (модули предотвращения угроз, веб-контроля и брандмауэра)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
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	

Примеры использования: обеспечение централизованного управления защитными продуктами с помощью консоли McAfee ePO

Продукт и технология	Пример обеспечения централизованного управления	Преимущество
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. Это осуществляется в одном общем интерфейсе управления.	Быстрое сдерживание зараженной конечной точки
McAfee ePO McAfee DLP 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 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. 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
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Развертывание ведущего отраслевого решения Avecto Defendpoint для управления привилегиями, а также управление этим решением, осуществляется из McAfee ePO. Изменения в конфигурацию Avecto Defendpoint вносятся на основе информации о репутации приложений, получаемой из McAfee Threat Intelligence Exchange.	Упрощение работы Не требуется дополнительной инфраструктуры; снижается совокупная стоимость владения Изменения в привилегии доступа вносятся исходя из информации об угрозах
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO направляет в Nexpose список активов. 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.	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.	Сокращается время на обнаружение угроз Блокирование и устранение атак

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

	Интегрированные организации	Неинтегрированные организации
В прошлом году зафиксировали менее пяти случаев нарушения безопасности	78 %	55 %
Обнаруживали угрозы за восемь часов	80 %	54 %

Penn Schoen Berland, 2016 г.

«McAfee ePolicy Orchestrator — самая мощная из имеющихся в сегодня на рынке платформ управления конечными точками. Этот продукт является базовым средством управления всеми защитными продуктами компании; он обеспечивает тот уровень эффективности и гибкости, который необходим корпоративным клиентам. Защитные функции отличаются широтой охвата и тесной интеграцией друг с другом посредством общего модуля политик и потока информации об угрозах».

— Forrester Wave. Endpoint Security Suites (Комплекты для защиты конечных точек), 2016 г.

Оптимизация работы с помощью расширяемых рабочих процессов

База данных 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. Вы сами определяете то, как консоль McAfee ePO будет направлять 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.

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. С помощью консоли McAfee ePO можно инициировать принятие мер по устранению уязвимостей силами оперативных ИТ-подразделений, например, в виде назначения более строгих политик. Наличие сетевых прикладных программных интерфейсов (API) позволяет сократить объем работы, выполняемой вручную.

Распространенные примеры использования

- Возможность планировать генерирование отчетов о соответствии требованиям безопасности с учетом запросов каждого заинтересованного лица позволяет экономить время и избавиться от избыточных и трудоемких процессов.
- Простая интеграция консоли McAfee ePO в существующие бизнес-процессы и бизнес-функции при помощи набора надежных и простых API-интерфейсов позволяет получать больше информации и ускорять рабочие процессы (например, интеграция с системами управления заявками на устранение неисправностей, с веб-приложениями или с порталами самообслуживания).
- Синхронизация консоли McAfee ePO с Active Directory позволяет развертывать агенты и защитные решения при появлении в корпоративной сети новых систем и тем самым поддерживать необходимый уровень защищенности.

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 управляющего центра) 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 конечной точки с более строгими политиками.

Обеспечение защиты в масштабе всей организации с помощью консоли McAfee ePO

Централизованное управление безопасностью

- Уникальная единая консоль предназначена для централизованного управления и сбора информации о сотнях тысяч узлов в масштабе всего предприятия.
- Открытая система расширенного управления безопасностью систем защищена решениями McAfee и сторонних поставщиков.

Рис. 1. Централизованное управление средствами защиты с помощью консоли McAfee ePO.

- Расширяемая платформа интегрируется с уже имеющейся ИТ-инфраструктурой и использует ее максимально эффективно, снижая эксплуатационные издержки.

Надежное сокращение времени реагирования

- Комплексные представления и аналитическая информация позволяют решать внутренние и внешние проблемы безопасности в упреждающем режиме.

- Быстрое централизованное развертывание обновлений безопасности и описаний вредоносных файлов обеспечивает защиту конечных точек от новейших угроз.
- Сокращение времени реагирования достигается благодаря панелям мониторинга, позволяющим принимать конкретные меры реагирования, а также благодаря усовершенствованным функциям генерирования запросов и отчетов.

Упрощение и оптимизация процессов

- Возможность быстрой установки и запуска реализуется благодаря пошаговой конфигурации, автоматизированным потокам задач управления политиками и стандартным панелям мониторинга.
- Назначение политик по тегам обеспечивает точное применение заданных профилей безопасности к отдельным системам или группам систем исходя из их бизнес-ролей или статуса риска.
- Каталог задач и функции автоматизированного управления способствует оптимизации процессов администрирования и сокращению непроизводительных расходов.
- Управление большим количеством разных продуктов для конечных точек с помощью одного-единственного агента снижает риск конфликтов между конечными точками.

Гибкие возможности масштабирования

- Архитектура корпоративного класса позволяет управлять сотнями тысяч устройств с помощью одного-единственного сервера.
- Поддерживается и зарекомендовала себя в сложных, гетерогенных ИТ-средах.
- Функция корпоративной отчетности помогает получать комплексное представление об уровне защищенности и нормативно-правовом соответствии предприятия.

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

McAfee Together is power.

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