McAfee Endpoint Security

Специализированная защита для упреждающего управления угрозами и проверенные средства обеспечения безопасности

Защита конечных точек. Что у вас в приоритете?

В современных компаниях вопросами безопасности может заниматься один или несколько отделов. В организациях корпоративного типа за безопасность нередко отвечают сразу несколько отделов: ИТ-администраторы, отдел операций по обеспечению безопасности и др. При выборе платформы для защиты конечных точек ваши главные требования к ее функциям и результатам работы естественным образом зависят от вашей должности в компании, отличаясь от приоритетов других отделов компании.

Используемое вами решение для защиты конечных точек должно соответствовать вашим самым главным приоритетам. Независимо от ваших функциональных обязанностей в компании, решение McAfee® Endpoint Security отвечает вашим конкретным насущным задачам, начиная от предотвращения и поиска угроз до индивидуальной настройки средств защиты. Возможности McAfee® MVISION Insights позволяют приоритизировать конкретные угрозы еще до возникновения атаки. Благодаря решению вы сможете обеспечить своим пользователям бесперебойную работу систем, найти больше возможностей для автоматизации операций и упростить сложные рабочие процессы.

Обеспечение бесперебойной работы и сбора информации об угрозах

McAfee Endpoint Security дает клиентам возможность реагировать на угрозы и управлять жизненным циклом защиты от угроз с помощью средств упреждающей защиты и восстановления систем. Возврат систем в работоспособное состояние осуществляется с помощью функции автоматического отката, позволяющей повысить производительность труда пользователей и администраторов. Благодаря автоматическому откату им не придется тратить рабочее время на ожидание внесения исправлений, на работу по восстановлению систем или на переустановку образов на зараженных системах. Между конечными точками и решением McAfee® MVISION EDR происходит обмен данными о глобальных угрозах и информацией о локальных событиях, получаемой в режиме реального времени. Это позволяет собирать сведения о событиях угроз, обнаруживать и предотвращать угрозы, пытающиеся избежать обнаружения, и сопоставлять их с матрицей MITRE ATT&CK для проведения дальнейших расследований. Для упрощения процессов управления используется консоль централизованного управления, позволяющая выбрать один из трех видов развертывания: локальное, в виде SaaS или в виртуальной среде.

Ключевые преимущества

- **Передовые средства защиты от сложных угроз.** Методы машинного обучения, средства защиты от кражи учетных данных и возможность отката системы к предыдущему состоянию дополняют собой базовые средства защиты, встроенные в настольные и серверные системы под управлением Windows
- **Отсутствие дополнительных сложностей.** Управление технологиями McAfee, политиками для антивирусной программы Защитник Windows и средства Exploit Guard в Защитнике Windows и настройками брандмауэра Windows с помощью единой политики и консоли

Подписаться

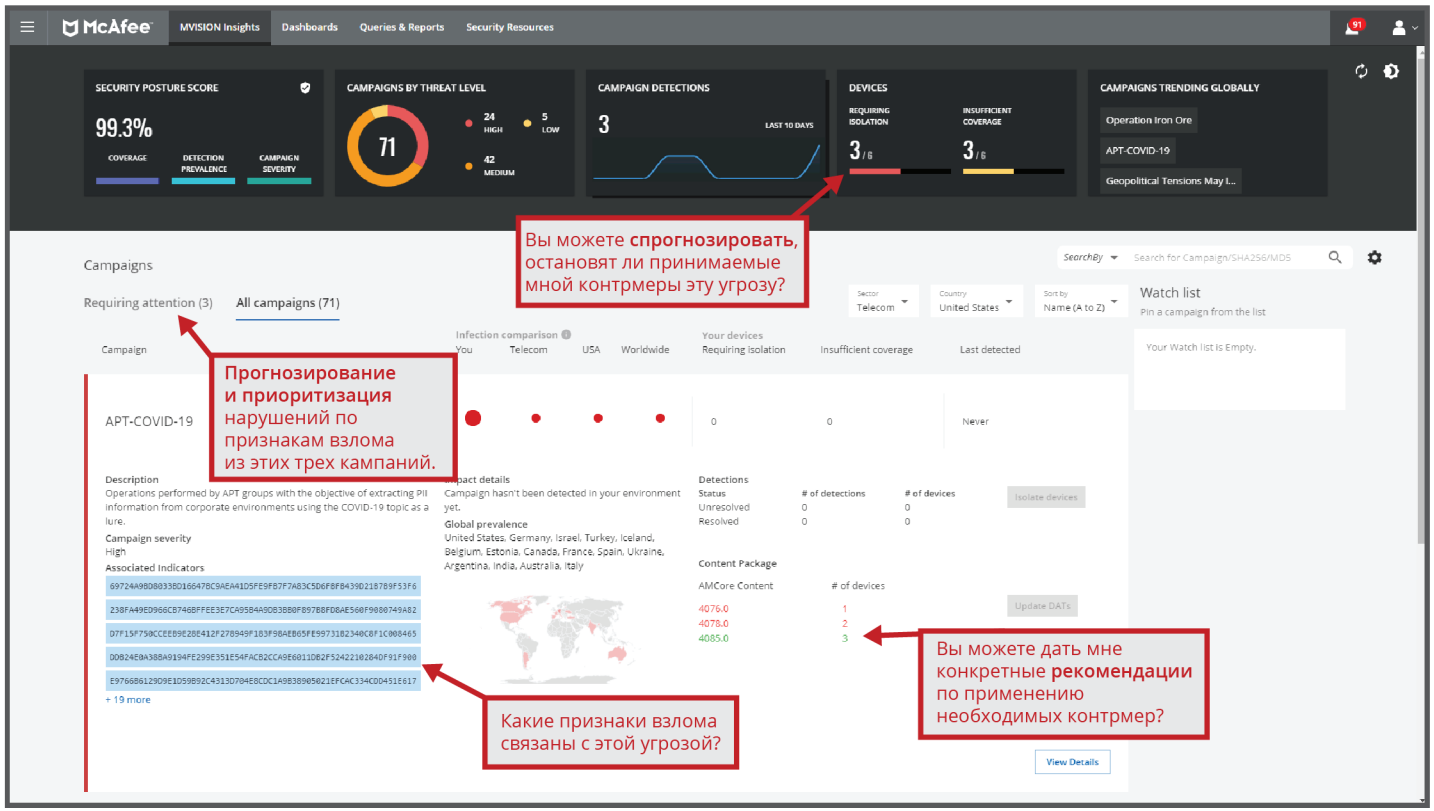

Рис. 1. Панель мониторинга MVISION Insights. (Для эффективной работы MVISION Insights необходимо разрешить сбор и передачу данных телеметрии в решении McAfee Endpoint Security.)

Решение MVISION Insights обеспечивает уникальную возможность сбора информации и управления потенциальным приоритетным угрозам с высокой вероятностью реализации атаки, а также определяет, достаточна ли степень защищенности организации для нейтрализации конкретной угрозы. Тем самым обеспечивается необходимый уровень защиты от критической угрозы, и атака нейтрализуется еще до ее начала.

Организации, использующие MVISION Insights, получают оповещения и уведомления о приоритетных потенциальных угрозах, которые способны реализоваться в зависимости от конкретных отраслей и регионов. Кроме того, решение MVISION Insights предусматривает локальную оценку состояния системы безопасности и ее возможностей для защиты от конкретной угрозы.

Ключевые преимущества (продолжение)

- **MVISION Insights.** Вооружитесь одним из лучших на сегодня решений для сбора информации о конкретных угрозах, чтобы моментально реагировать на потенциально активные кампании, приоритизируя их в зависимости от того, нацелены они на ваш сектор или на ваш регион. MVISION Insights заранее определяет, какие конечные точки могут оказаться незащищенными в ходе таких кампаний, и дает предписывающие рекомендации по повышению эффективности обнаружения угроз. Это единственное решение для защиты конечных точек, обеспечивающее одновременно приоритизирование угроз, прогнозирование атак и рекомендации по контрмерам.

Оно также определяет уязвимые для угрозы конечные точки и дает предписывающие рекомендации по обновлениям. Таким образом усиливается активная работа на опережение злоумышленников, которые могут совершить атаку.

Для сбора информации об угрозах на разных уровнях взаимодействия в McAfee Endpoint Security используется один-единственный программный агент, что позволяет устранить избыточность, присущую средам, в которых используется большое количество различных специализированных продуктов. В результате достигается комплексный подход к безопасности, исключающий необходимость ручного сопоставления угроз. Информация об угрозах, требующая дальнейшего расследования, автоматически передается специалистам по реагированию на инциденты. Благодаря функции Story Graph данные о событиях угроз

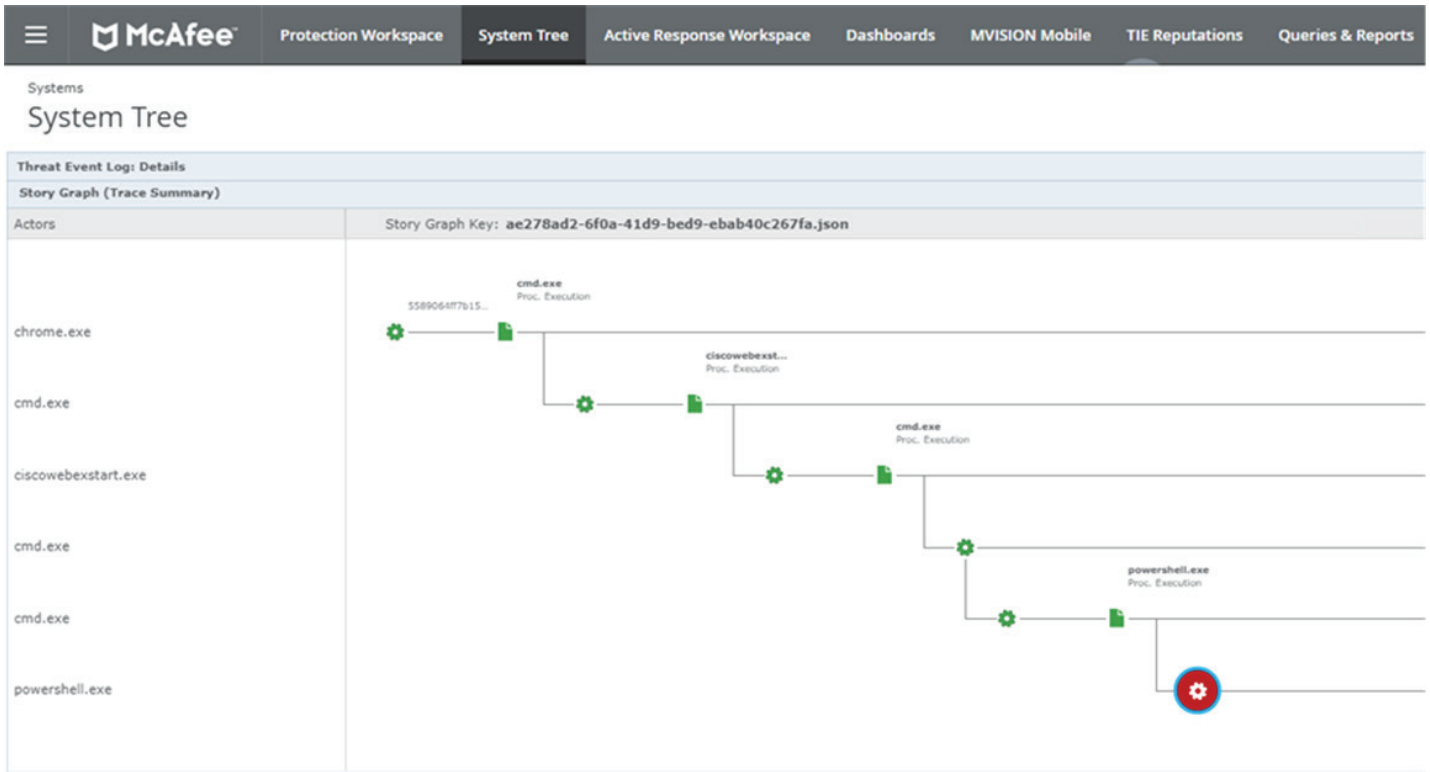

Рис. 2. Story Graph

представляются в простом и наглядном формате, который визуализирует информацию об угрозах и дает администраторам возможность без труда анализировать их и выявлять источники вредоносных объектов.

Автоматизация реагирования и сокращение времени реагирования благодаря интегрированным средствам защиты от сложных угроз

Для защиты от новейших сложных угроз организациям помогут также дополнительные средства защиты от сложных угроз, предлагаемые в рамках интегрированной платформы McAfee Endpoint Security, такие как Dynamic Application Containment (DAC — динамическое сдерживание приложений).[1] Так, например, DAC анализирует потенциально опасное ПО и другие новые вредоносные программы и изолирует их с целью предотвращения заражений.

Защиту от сложных угроз обеспечивает также технология Real Protect, позволяющая обнаруживать вредоносное ПО «нулевого дня» и оптимизировать процессы обнаружения угроз путем классификации поведения вредоносных программ с помощью методов машинного обучения. Классификация поведения без использования сигнатур выполняется в облаке и отличается низким ресурсопотреблением на клиентском компьютере, причем обнаружение угроз происходит в режиме почти реального времени. Получаемую аналитическую информацию можно использовать для создания признаков атаки и признаков взлома. Из конкретных областей применения аналитической информации можно назвать обнаружение угроз в межузловом трафике, выявление «нулевых пациентов», атрибуцию угроз, проведение компьютерно-технических экспертиз и устранение уязвимостей. Кроме того, со временем скорость анализа, проводимого с помощью Real Protect, увеличивается, потому что механизм классификации поведения автоматически совершенствуется, а набор правил, позволяющих выявлять похожие атаки путем анализа кода (как статического, так и во время выполнения), пополняется.

Наконец, когда реальность угрозы подтверждается, клиент восстанавливает конечную точку, откатывая ее к последней рабочей конфигурации. Это позволяет без промедления предотвратить заражение конечной точки и сэкономить время администраторов ИБ.

Интеллектуальная защита конечных точек позволяет отслеживать действия злоумышленников в реальном времени

Чем лучше информация об угрозах, тем лучше результаты. Обмениваясь (в режиме реального времени) полученной в ходе наблюдений информацией с большим количеством подключенных к нему технологий для защиты конечных точек, McAfee Endpoint Security обеспечивает взаимодействие этих технологий и ускоряет процесс выявления случаев подозрительного поведения, обеспечивает более эффективную координацию разных средств защиты и повышает уровень защищенности от целенаправленных атак и угроз «нулевого дня». Сбор таких данных, как хэш файла,

URL-адрес источника, события AMSI и PowerShell, и передача их не только на другие средства защиты, но и на клиентский интерфейс и интерфейс управления, помогает пользователям определять характер атак и снабжать администраторов практически применимой информацией об угрозах для проведения компьютерно-технической экспертизы.

Кроме того, благодаря технологии McAfee® Threat Intelligence Exchange адаптивные средства защиты получают возможность взаимодействовать с другими решениями McAfee: шлюзами, изолированными средами («песочницами»), нашим решением для управления информацией о безопасности и событиями безопасности (SIEM) и др. Сбор и распространение информации об угрозах на локальном и глобальном уровне, а также внутри сообщества специалистов по информационной безопасности сокращает время между атакой, ее обнаружением и сдерживанием с нескольких недель или месяцев до нескольких миллисекунд.

Развернутая в сочетании с технологией McAfee® Global Threat Intelligence (McAfee® GTI) платформа McAfee Endpoint Security получает возможность через облако в режиме реального времени осуществлять мониторинг всего спектра новых и только появляющихся угроз по всем векторам (файлы, Интернет, сообщения и сети) и принимать меры реагирования. Повышение эффективности существующей системы отслеживания конечных точек и управления ими путем задействования информации о локальных и глобальных угрозах дает возможность мгновенно нейтрализовать неизвестное и целенаправленное вредоносное ПО. Меры, принимаемые в автоматическом режиме против подозрительных приложений и процессов, способствуют быстрой эскалации инцидентов для реагирования на новые и только появляющиеся виды атак. Одновременно с этим информация передается на другие средства защиты и глобальному сообществу специалистов по информационной безопасности.

Клиенты, использующие DAC и Real Protect, получают аналитическую информацию о более сложных угрозах и их поведении. Так, например, DAC предоставляет информацию о заблокированных приложениях и о том, к чему они пытаются получить доступ: к реестру, к памяти или к другим ресурсам.

Тем организациям, которым для поиска вредоносных программ и реагирования на инциденты нужна аналитическая информация о связанных с угрозами процессах на конечных точках, Real Protect предоставляет информацию о признанных вредоносными разновидностях поведения, а также результаты классификации угроз. Особенно эффективно эту информацию можно использовать для выявления вредоносных файлов, пытающихся избежать обнаружения с помощью таких методов обхода защиты, как упаковка, шифрование и эксплуатация благонадежных приложений.

Надежная и эффективная защита помогает своевременно принимать меры реагирования

Эффективность интеллектуальных средств защиты может быть сведена на нет низкой скоростью сканирования, долгим процессом установки или сложностью в управлении. Для экономии рабочего времени пользователей в McAfee Endpoint Security используется общий уровень обслуживания и наш новый модуль защиты от вредоносного ПО, помогающий сократить объем ресурсов и энергопотребления, необходимый для работы систем пользователей. Сканирование конечных точек не влияет на производительность труда пользователей, поскольку выполняется только в режиме простоя устройства и автоматически возобновляется после его перезагрузки или выключения.

Адаптивный характер процесса сканирования помогает также снизить нагрузку на ЦП: поняв, какие процессы и источники являются надежными, модуль сканирования ограничивается только теми процессами, которые кажутся подозрительными или имеют неизвестные источники. В McAfee Endpoint Security имеется встроенный брандмауэр, с помощью McAfee GTI обеспечивающий защиту конечных точек от бот-сетей, распределенных атак типа «отказ в обслуживании» (DDoS), сложных постоянных угроз (APT) и опасных веб-подключений.

Облегчение работы за счет снижения сложности и повышения срока эксплуатации защитных продуктов

Из-за стремительного роста числа защитных продуктов с частично совпадающими функциями и отдельными консолями управления многим организациям оказывается непросто составить точную картину потенциальных атак. В случае McAfee Endpoint Security надежность защиты в долгосрочной перспективе обеспечивается за счет открытой и расширяемой платформы, служащей фундаментом для централизованного управления как уже имеющимися, так и будущими решениями для защиты конечных точек. Для обеспечения взаимодействия с уже приобретенными организацией техническими решениями на данной платформе используется уровень обмена данными Data Exchange Layer. Его интегрированная архитектура легко объединяется с другими продуктами McAfee, что сокращает число оставшихся брешей в защите, несовместимых технологий и избыточность. Снижение эксплуатационных расходов и упрощение процессов управления стимулирует рост производительности.

Для еще большего упрощения работы можно использовать программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™), позволяющее осуществлять мониторинг происходящего, развертывание средств защиты и управление конечными точками из единой консоли. Наличие настраиваемых представлений и эффективных рабочих процессов на понятном языке позволяет быстро оценивать уровень защищенности, выявлять зараженные устройства и снижать риски путем помещения систем в карантин, прекращения вредоносных процессов или блокирования попыток эксфильтрации данных. Кроме того, решение позволяет централизованно управлять всеми конечными точками, другими технологиями McAfee и более чем 130 защитными решениями сторонних поставщиков.

Функция	Назначение
Упреждающее обнаружение угроз и реагирование на них (MVISION Insights)	▪ Заблаговременно обнаруживает потенциальные угрозы в зависимости от конкретных отраслей и регионов. ▪ Выполняет локальную оценку уровня защищенности от потенциальной угрозы и предлагает корректирующие рекомендации с целью его повышения. ▪ Позволяет опережать злоумышленников путем принятия защитных мер еще до возникновения атаки.
Real Protect	▪ Модуль классификации поведения с помощью методов машинного обучения позволяет обнаруживать угрозы «нулевого дня» в режиме почти реального времени и получать информацию об угрозах для принятия конкретных мер реагирования. ▪ Автоматически совершенствует механизм классификации поведенческих признаков, позволяющий определять угрозы по поведению и добавлять правила для выявления схожих атак в будущем.
Защита конечных точек от целенаправленных атак	▪ Модуль защиты конечных точек позволяет сократить разрыв между обнаружением угрозы и ее сдерживанием с нескольких дней до нескольких миллисекунд. ▪ Собирая информацию об угрозах из разных источников, McAfee Threat Intelligence Exchange дает компонентам системы безопасности возможность мгновенно обмениваться информацией о новых и сложных многоэтапных атаках. ▪ Регистрация событий с помощью AMSI и PowerShell позволяет обнаруживать и отражать бесфайловые атаки и атаки, проводимые с использованием сценариев.
Интеллектуальное, адаптивное сканирование	▪ Повышает уровень производительности и быстродействия благодаря отказу от сканирования надежных процессов и приоритизации подозрительных процессов и приложений. ▪ Адаптивные функции поведенческого сканирования позволяют осуществлять мониторинг происходящего, выявлять угрозы и при обнаружении подозрительной активности передавать эту информацию на следующий уровень.
Устранение угроз путем отката	▪ Устранение угроз путем отката автоматически отменяет изменения, внесенные вредоносными программами, и возвращает системы в их последнее работоспособное состояние, поддерживая тем самым производительность труда пользователей.

Упреждающая веб-защита	▪ Модуль упреждающей защиты веб-трафика с функциями веб-защиты и фильтрации для обеспечения безопасного просмотра веб-сайтов на конечных точках.
Динамическое сдерживание приложений	▪ Функция динамического сдерживания приложений обеспечивает защиту от программ-вымогателей и потенциально опасных программ, а также помогает выявлять «нулевых пациентов».[2]
Блокирование агрессивных сетевых атак	▪ На основе оценок репутации, получаемых с помощью McAfee GTI, встроенный брандмауэр обеспечивает защиту конечных точек от бот-сетей, DDoS-атак, сложных постоянных угроз и подозрительных веб-подключений. ▪ Во время запуска системы брандмауэр пропускает только исходящий трафик, обеспечивая тем самым защиту конечных точек, находящихся за пределами корпоративной сети.
Story Graph	▪ Дает администраторам возможность быстро определить местонахождение, причину и продолжительность заражения, чтобы проанализировать угрозу и быстрее принять меры реагирования.
Централизованное управление (платформа McAfee ePO) с несколькими вариантами развертывания	▪ Эта по-настоящему централизованная платформа управления позволяет обеспечить более полный сбор информации о происходящем, упростить операции, повысить производительность труда ИТ-подразделений, объединить процессы ИБ и снизить затраты.
Открытая, расширяемая платформа для защиты конечных точек	▪ Интегрированная архитектура дает средствам защиты конечных точек возможность взаимодействовать друг с другом и обмениваться информацией с целью обеспечения более надежной защиты. ▪ Способствует снижению эксплуатационных расходов за счет устранения избыточности и оптимизации процессов. ▪ Легко интегрируется с другими продуктами McAfee и продуктами сторонних поставщиков, сокращая бреши в защите.

Таблица 1. Основные функции и их назначение.

Лишить киберугрозы преимущества первого удара

McAfee Endpoint Security дает сегодняшним специалистам по ИБ все необходимое для того, чтобы лишить злоумышленников преимущества первого удара: набор интеллектуальных, взаимодействующих друг с другом средств защиты и платформу для упрощения сложных сред. Высокие показатели надежности, быстродействия и эффективности обнаружения угроз, подтвержденные результатами независимых тестов, позволяют организациям защитить своих пользователей, повысить производительность труда и обрести уверенность в собственной защищенности.

Компания McAfee, лидер на рынке безопасности конечных точек, предлагает полный спектр решений для обеспечения эшелонированной обороны и упреждающей защиты, сочетающих в себе надежные средства защиты и эффективную систему управления, которые позволяют специалистам по безопасности выявлять больше угроз, делая это быстрее и затрачивая меньше ресурсов.

Простота миграции

В средах с текущими версиями программного обеспечения McAfee ePO, McAfee VirusScan® Enterprise и McAfee® Agent перенос имеющихся политик в McAfee Endpoint Security с помощью нашей автоматизированной утилиты занимает не более 20 минут.[3]

Кроме того, McAfee Endpoint Security даст вам следующие преимущества:

- производительность труда пользователей не снижается при сканировании;
- более точные данные компьютерно-технической экспертизы, представляемые в наглядном формате Story Graph, позволяют быстро разобраться в ситуации и упрощают проведение расследований с целью ужесточения ваших политик безопасности;
- функция отката автоматически отменяет внесенные вредоносными программами изменения и поддерживает системы в работоспособном состоянии;
- благодаря MVISION Insights вы сможете получать упреждающую информацию о приоритетных потенциальных угрозах, а также предписывающие рекомендации по настройке мер противодействия им;
- меньшее количество используемых агентов и отказ от сканирований помогают сократить объем вводимых вручную данных;
- взаимодействие средств защиты позволяет эффективнее бороться со сложными угрозами;
- к вашим услугам платформа нового поколения, легко интегрируемая с другими нашими решениями для защиты от сложных угроз и EDR-решениями (Endpoint Detection and Response — обнаружение угроз и реагирование на инциденты на конечных точках).

Дополнительная информация

С дополнительной информацией о McAfee Endpoint Security можно ознакомиться здесь.

С дополнительной информацией о McAfee Endpoint Security как о решении, дополняющем собой другие продукты McAfee, можно ознакомиться по следующим ссылкам:

- MVISION Endpoint
- Семейство продуктов MVISION
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. Функция включена в большинство комплектов решений McAfee для защиты конечных точек. За дополнительной информацией просим вас обращаться к вашему торговому представителю.
2. См. предыдущую сноску.
3. Скорость миграции зависит от имеющихся политик и характеристик среды.

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