McAfee MVISION Insights

Первое решение для защиты конечных точек, которое динамически повышает уровень защищенности вашей компании, позволяя опережать злоумышленников

Эволюция и темпы распространения киберугроз представляют собой постоянную опасность и критическую проблему для организаций. В условиях нехватки специалистов по безопасности предприятия пытаются решить проблему за счет увеличения бюджетов на обеспечение безопасности, но им все равно не удается поспевать за современными злоумышленниками, постоянно обновляющими свой арсенал инструментов, тактик и методов. Существующие решения используют разрозненные технологии сбора информации, требующие участия человека и ручного вмешательства в процессы защиты. Возможно они и помогают противостоять непосредственным угрозам, однако растущее число и специфика киберугроз вынуждают засыпанные оповещениями об угрозах отделы ИБ неизменно использовать реактивный подход. Платформа сбора данных об угрозах (threat intelligence platform — TIP) может служить базой для большого озера данных об угрозах, но оно требует ручной интеграции и ручного управления жизненным циклом аналитики, что ограничивает возможности для принятия мер и устранения уязвимостей. Системы управления уязвимостями информируют о существующих уязвимостях и степени их серьезности, однако дают ограниченные сведения о том, позволит ли уровень защищенности вашей организации противостоять существующим угрозам в реальных условиях.

Настоящее решение проблемы предлагает McAfee® MVISION Insights, продукт, который собирает информацию об угрозах в режиме реального времени, позволяющую принимать упреждающие меры. Комплексная информация об угрозах, отфильтрованная и проанализированная искусственным интеллектом и человеком, помогает установить приоритеты угроз и хакерских кампаний; при этом наивысший приоритет присваивается тем из них, которые с наибольшей вероятностью будут направлены на вашу организацию. McAfee MVISION Insights точно предсказывает, каким образом угроза повлияет на общий уровень защищенности вашей организации, а также предлагает конкретные рекомендации по оптимизации вашего подхода к обеспечению безопасности.

Основные преимущества

- **Информация о рисках, собираемая миллиардами датчиков.** Информация, получаемая из надежного источника, позволяет в проактивном режиме выявлять потенциальные угрозы вне периметра безопасности вашего предприятия. Приоритеты потенциальных угроз устанавливаются на основе данных по отраслевым вертикалям, географическим регионам и в зависимости от степени защищенности конечных точек в вашей организации.
- **Возможность обнаруживать кампании злоумышленников еще до начала атаки, а также ранжировать уровни риска с помощью единой консоли.** Вы получаете информацию об угрозах, позволяющую принимать конкретные меры реагирования и понимать, насколько уровень защищенности конечных точек в вашей организации способен отразить эти угрозы. Информация также содержит рекомендации по устранению уязвимостей.
- **Сокращение среднего времени обнаружения угроз и реагирования на них.** Решение позволяет оптимизировать рабочие процессы, чтобы ускорить принятие дополнительных мер защиты. С его помощью вы сможете оценивать степень защищенности своих конечных точек и получить рекомендации о внесении необходимых изменений. Время реагирования сокращается при этом с нескольких месяцев до нескольких часов.

Подписаться

Переведите свою систему безопасности на рельсы проактивной защиты!

MVISION Insights предлагает новые функции, встроенные в платформу управления McAfee®, которые уникальным образом согласуют и оптимизируют операции по оценке рисков и угроз, позволяющие в превентивном порядке скорректировать защитные контрмеры и сократить время реагирования, затрачивая при этом меньше ресурсов. Информация о рисках, собираемая миллиардами датчиков, помогает вашему предприятию проанализировать, что именно необходимо сделать для приоритизации мер защиты. Обнаружение и устранение угроз, сокращение времени упреждающего реагирования и значительное снижение рисков — все это можно реализовать с помощью одной консоли.

Реактивные стратегии хотя и служат одним из важных компонентов киберзащиты, но их возможности сводятся лишь к «играм в догонялки» и авралам. Злоумышленники используют инструменты следующего поколения для разработки кампаний, нацеленных на традиционные средства защиты, и испытывают надежность продуктов для реактивной защиты, чтобы выяснить, какими методами можно пробить в них брешь. Организации должны обеспечивать защиту в течение всего жизненного цикла атак, в том числе до их начала и после завершения.

Жизненный цикл атаки

Рис. 1. Типичный жизненный цикл атаки

Сбор данных и практически полезная аналитическая информация об угрозах дают вам в конечном итоге возможность выстроить наиболее эффективную стратегию киберзащиты от наиболее вероятных угроз и укрепляют уверенность в применяемых вами средствах защиты. Рассмотрим, как McAfee MVISION Insights справляется с этой задачей.

- **Решение помогает сократить число «мертвых зон» и повышает уровень ситуационной осведомленности.** Еще до начала действия угрозы вы точно знаете, смогут ли ей противостоять ваши меры защиты. MVISION Insights в проактивном режиме отслеживает и приоритизирует локальные и глобальные угрозы, которые, по прогнозам, могут быть реализованы в отношении вашего предприятия.

MVISION Insights дает ответы на вопросы, связанные с рисками для конечных точек

- Подвергаетесь ли вы риску? Каков в настоящее время уровень незащищенности?
- Как вы устанавливаете приоритеты атак, которые могут быть направлены на вашу организацию? Как вы узнаете о них? В чем заключается ваш процесс анализа?
- Как вы узнаете об угрозах, которые не были реализованы в отношении вашей организации, но остаются вероятными?
- Даже если бы у вас была платформа сбора данных об угрозах, каким образом вы бы определяли приоритеты всех атак в базе данных этой платформы?
- Как вы узнаете об угрозах, которые были реализованы в отношении ваших коллег?
- Насколько распространена данная угроза в вашей отрасли и в вашем регионе?
- Как имеющаяся у вас на сегодня система защиты справляется с этой угрозой?
- Насколько вы уверены в полноте картины угроз, имеющейся в вашем распоряжении, и почему?

- **Анализ угроз методами машинного обучения.** Благодаря этой функции вы сможете определить, как будет вести себя именно ваша система безопасности при атаках, а также получить рекомендации о том, какие упреждающие меры защиты можно быстро и легко внедрить, чтобы блокировать эти атаки.
- **Автоматическое обнаружение глобальных угроз, которых вы не замечали.** MVISION Insights использует гиганстское озеро информации об угрозах безопасности, поступающей от более чем миллиона датчиков.

Панель мониторинга MVISION Insights

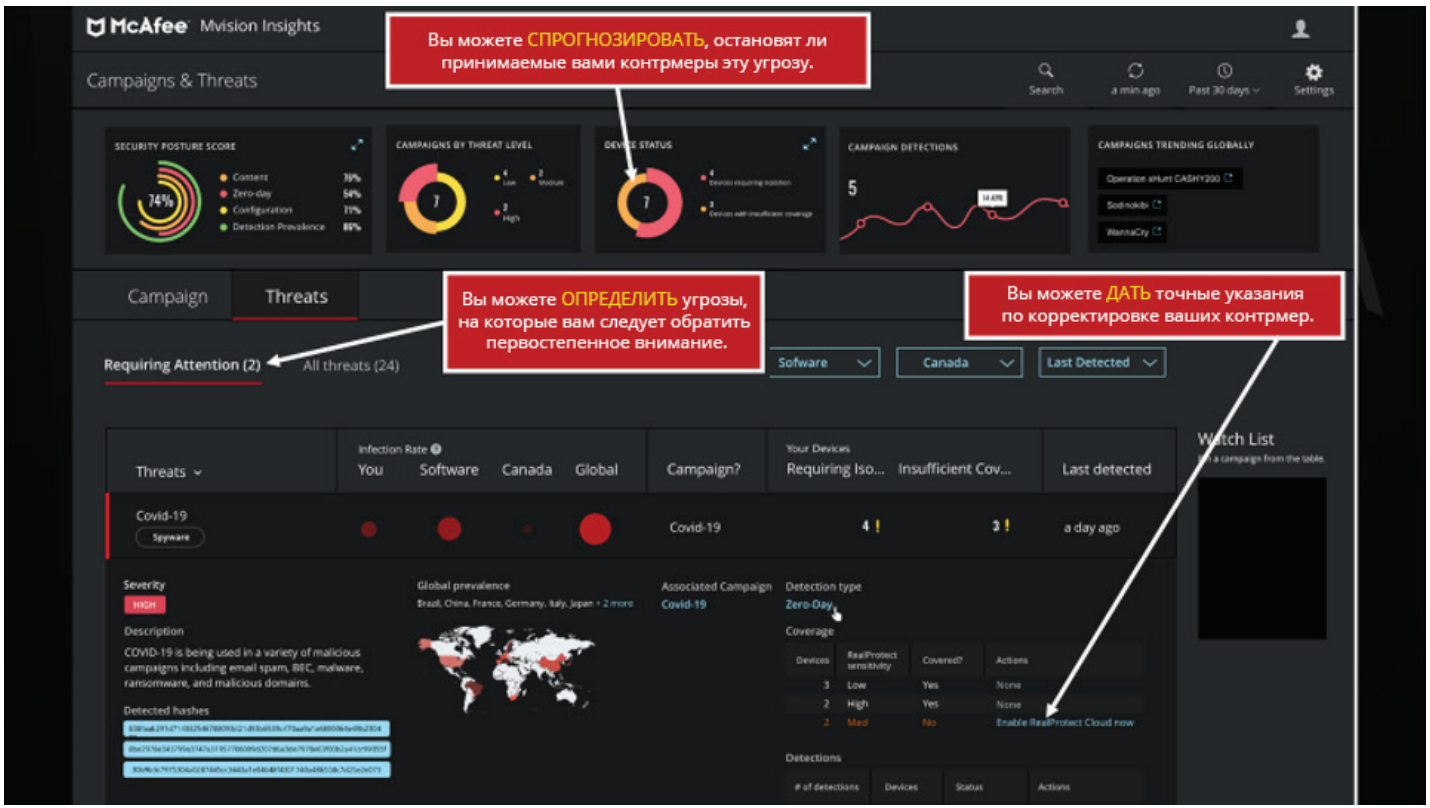

Рис. 2. Пример панели мониторинга MVISION Insights.

Оценка рисков

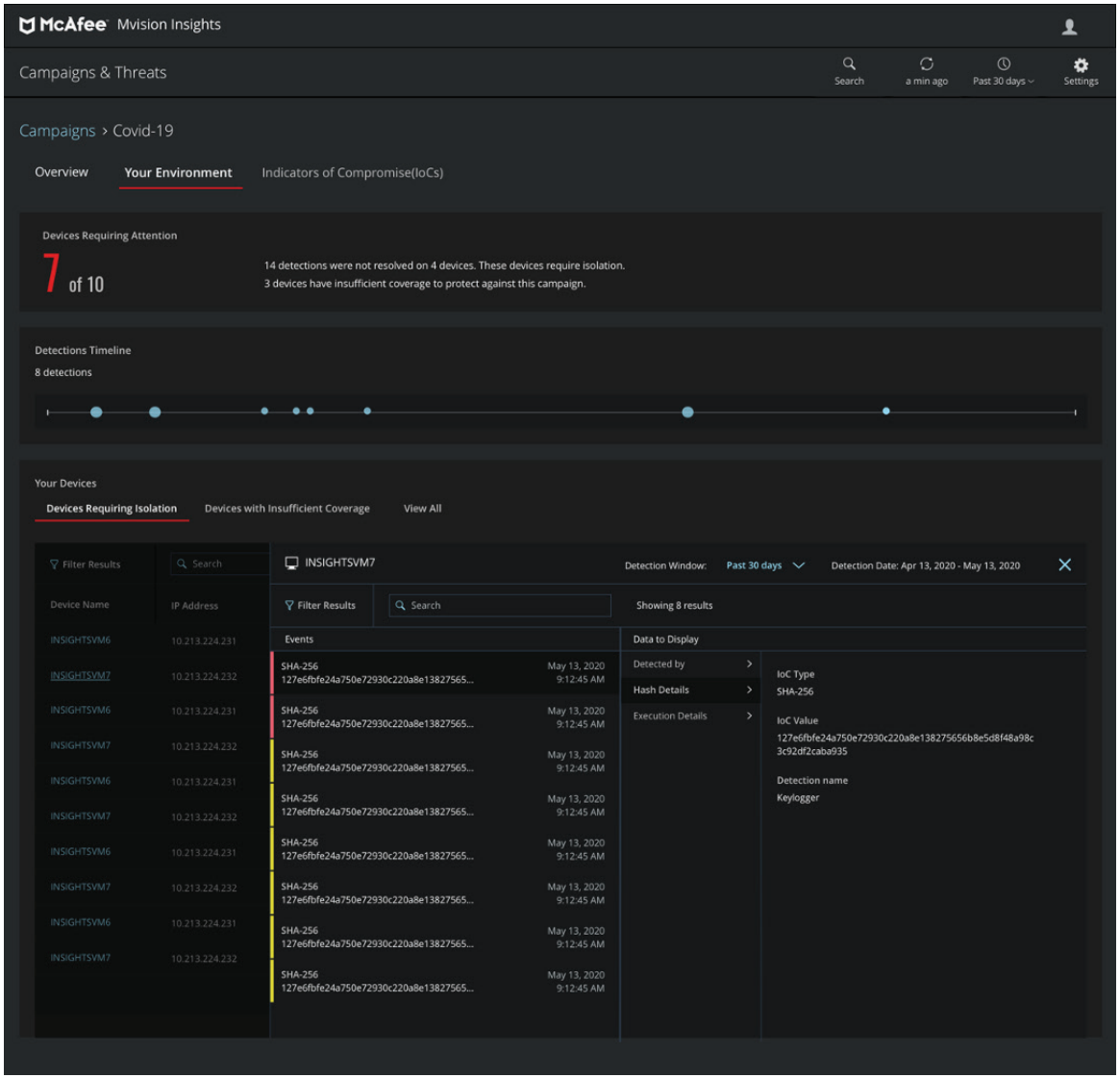

Рис. 3. Панель демонстрирует, каким компонентам вашей среды следует уделить внимание, чтобы отразить угрозы в упреждающем режиме.

Значительное сокращение времени обнаружения и реагирования

Благодаря предписывающим рекомендациям и автоматизации мер реагирования MVISION Insights помогает вашему предприятию сделать следующий важный упреждающий шаг на пути к изменению вашей уникальной среды и устранению угроз. Автоматизация повышает эффективность защиты от внешних атак за счет автоматического анализа и сопоставления внешних угроз, а также упреждающей защиты от них до начала атаки.

- **Сокращение среднего времени обнаружения угроз и реагирования на них с нескольких месяцев до нескольких минут.** Совместная работа человека и машины (использование методов глубокого обучения и машинного обучения) и расширенные возможности анализа позволяют просеивать огромные объемы данных и получать точную и конкретную информацию о происходящем. Расширенные возможности обнаружения угроз в превентивном порядке сокращают время реагирования и значительно снижают риск.
- **Улучшение отношения сигнал-шум при обнаружении признаков угроз.** Усовершенствованные средства анализа позволяют расширить диапазон обнаруживаемых угроз и понимать смысл получаемых предупреждений. При анализе угроз MVISION Insights может легко переключаться на McAfee® MVISION EDR для поиска дополнительной контекстной информации, например признаков взлома, и для сокращения длительности циклов расследования.
- **Информация об угрозах представлена в понятной форме, с указанием приоритетов и действенности рекомендованных мер.** Реагирование согласно рекомендациям, составленным с учетом проанализированной и приоритизированной информации об угрозах повышают уровень возможностей даже начинающих аналитиков. Интегрированная консоль помогает ускорить и упростить процесс реагирования: вносить изменения в конфигурацию, изолировать зараженные устройства, обновлть политику или переключаться на систему обнаружения и реагирования на конечных точках (EDR).

Расширение возможностей специалистов SOC

Специалисты по безопасности перегружены огромным объемом собираемой информации, которую им приходится анализировать для защиты своих сред. Недостаток ресурсов и времени тормозит анализ угроз и эффективности мер защиты. Совместная работа человека и машины расширяет возможности анализа (независимо от уровня квалификации аналитиков), позволяя просеивать огромные объемы данных и представлять их в виде информации для принятия конкретных мер реагирования. MVISION Insights дает вашему предприятию возможность преодолеть дефицит квалифицированного персонала и расширить возможности специалистов центра управления безопасностью (SOC). Вооруженные более качественной информаций специалисты по безопасности принимают более обоснованные решения.

- Анализ информации, полученной с помощью системы сбора данных MVISION Insights, позволяет отделам ИБ модифицировать систему защиты с учетом специфики предприятия и максимально укрепить ее. В результате вы сможете обеспечить оптимальную защиту при прежней численности и квалификации персонала. MVISION Insights передает аналитику более целенаправленного характера в систему MVISION EDR, что позволяет сократить длительность цикла расследования и получить знания и ресурсы, необходимые для выполнения расследований. Аналитики могут быстрее и эффективнее установить уровень риска и первопричину инцидента.
- Решение помогает руководителям служб ИТ-безопасности получить максимальную отдачу от персонала и продуктов, освобождая аналитиков ИБ от рутинных задач и позволяя даже младшим сотрудникам отделов работать намного эффективнее. Организации могут добиться сокращения времени, связанного с управлением безопасностью. Решение позволяет оптимизировать рабочие процессы, чтобы ускорить принятие дополнительных мер защиты.
- Автоматизация процессов обнаружения, реагирования и защиты от приоритизированных угроз в превентивном режиме с помощью единой консоли избавляет аналитиков от необходимости постоянно переключаться между задачами. MVISION Insights накапливает и анализирует необходимые элементы данных и практические рекомендации в единой консоли, предоставляя их аналитикам ИБ в нужный момент.

Подробная аналитическая информация

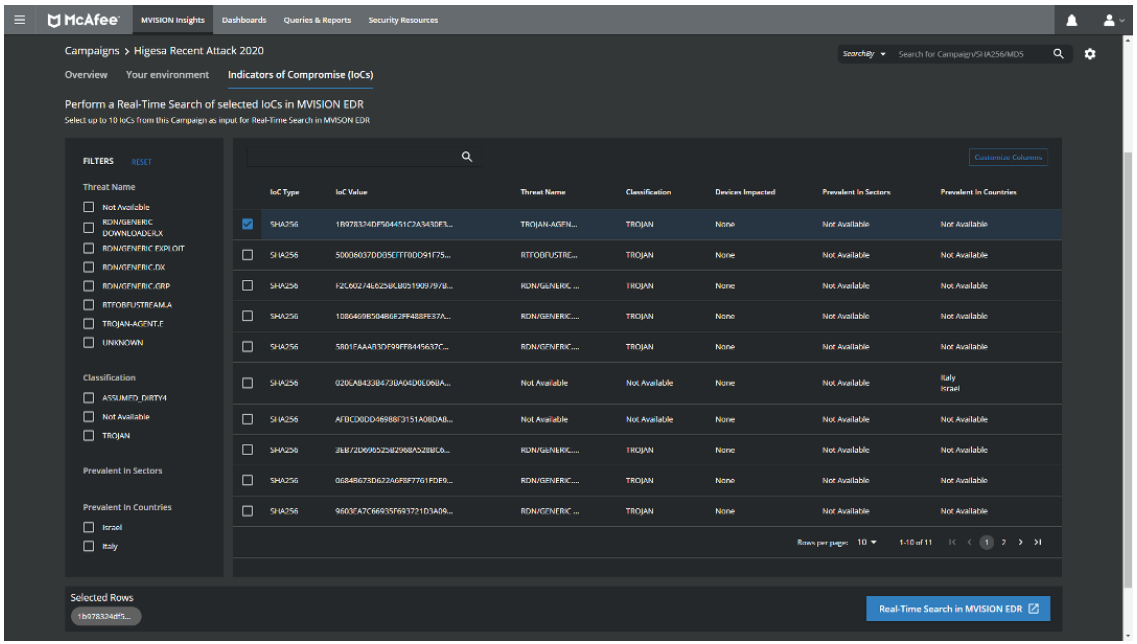

Рис. 4. Анализируйте ситуацию глубже, чтобы понять события, связанные с угрозами, и определить свои возможности по защите вашей организации.

Требования относительно использования MVISION Insights

MVISION Insights работает под управлением McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (локально и на базе IaaS) и McAfee® MVISION ePO™ (SaaS). Решение оптимизировано для использования с нашей новейшей технологией защиты конечных точек — McAfee® Endpoint Security и McAfee® Agent. Для эффективной работы MVISION Insights необходимо разрешить сбор и передачу данных телеметрии в решении McAfee Endpoint Security.

Примеры использования решения клиентами

Проблема	Решение	Результат
Являюсь ли я объектом атаки? **Это новый вариант кампании?**	▪ Оценка угрозы, исходящей от известной кампании. ▪ Выборочный ретроспективный анализ атак. ▪ Создание отчетов по сравнительной эффективности защиты. ▪ Ретроспективный анализ атак на пользователя по признакам взлома.	Ответ на вопрос: Подвергаюсь ли я риску?
Способна ли текущая конфигурация защиты защитить меня?	▪ Проверка состояния локальной защиты.	Оценка текущего состояния моей защиты.
Что конкретно мне необходимо изменить, чтобы обеспечить защиту?	▪ Проверка состояния локальной защиты.	Предписывающие рекомендации относительно конкретных действий
Можно ли изолировать угрозу с помощью других моих функций безопасности?	▪ Опубликовать данные для изоляции или сдерживания угрозы другими функциями безопасности.	Отправка данных о сдерживающих действиях другим функциям безопасности для дальнейшего снижения риска (через DXL).

Дополнительная информация

Для получения подробной информации посетите наш сайт www.mcafee.com/ru.

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