kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Endpoint Detection and Respose Optimum

Глубинная защита рабочих мест с возможностями мгновенного автоматического реагирования и простого причинно-следственного анализа

Вызовы

На протяжении 2019 г. **91%** всех организаций столкнулись с кибератаками; каждая десятая стала жертвой целевой атаки[1]

Сложные угрозы приводят к простоям

Времена незатейливых вредоносных программ давно прошли. Киберугрозы стали гораздо изощреннее, они дольше остаются незамеченными, вызывая перебои в работе и нанося бизнесу крупный ущерб.

Атаки становятся дешевле и доступнее

Сложные угрозы стали значительно дешевле в реализации, злоумышленники используют их все чаще. Организации, полагавшие, что их эта проблема не затронет, теперь должны всерьез задуматься о защите.

Трудно найти ресурсы

Ситуацию усугубляет нехватка ресурсов, самые важные из которых – время и дефицит на рынке труда квалифицированных ИБ-специалистов.

Решение

«Слабое решение класса Endpoint Protection Platform (EPP) сведет на нет все преимущества EDR-решения»[2]

«Окупаемость EDR-решения теперь измеряется время- и трудозатратами»[2]

Kaspersky Endpoint Detection and Response Optimum (KEDR Optimum) с возможностями улучшенного обнаружения угроз, упрощенного расследования и автоматического реагирования поможет вам защититься от сложных и продвинутых угроз. Решение доступно в рамках линейки продуктов для комплексной защиты рабочих мест Kaspersky Security для бизнеса.

Инструменты для расследования

Решение предоставляет полные и наглядные данные о событиях безопасности, простые инструменты для расследования и возможности автоматического реагирования. С их помощью вы сможете не только обнаружить угрозу, но и определить ее истинные происхождение и масштаб, а также оперативно среагировать на неё, минимизировав бизнес-потери.

Настоящая глубинная защита

Решение сочетает простой в использовании набор автоматизированных инструментов для обнаружения угроз и реагирования на них с надежной защитой рабочих мест и улучшенными технологиями обнаружения Kaspersky Security для бизнеса.

Повышение эффективности

Благодаря простому централизованному управлению и высокому уровню автоматизации вы сможете сэкономить время, оптимизировать загрузку администраторов и сократить расходы на IT-ресурсы. Управление ведется из единой консоли, размещенной локально или в облаке[3].

Ключевые преимущества

- Защитите себя от продвинутых и сложных угроз, которые встречаются все чаще и становятся все опаснее
- Экономьте время и ресурсы благодаря простым автоматизированным инструментам
- Определяйте масштаб распространения сложной угрозы в вашей сети
- Узнайте первопричину угрозы: выясните, как она проникла в вашу систему
- Предотвратите дальнейший ущерб благодаря быстрому автоматическому реагированию

Примеры использования EDR

Получите ответы на важные вопросы

- Каков контекст оповещения об инциденте?
- Что уже было сделано в связи с этим оповещением?
- Активна ли обнаруженная угроза до сих пор?
- Атакованы ли другие хосты?
- По какому вектору развивалась атака?
- Какова истинная первопричина угрозы?

Точно определите масштаб угрозы

Как только вы узнали о риске глобальной угрозы (например, если регулирующий орган требует выполнить проверку на наличие определенного индикатора компрометации), вы можете:

- Импортировать индикаторы компрометации из доверенных источников и запускать периодические проверки на наличие признаков атаки
- Тщательно расследовать инцидент, сгенерировать индикаторы компрометации на основе обнаруженных угроз и запустить сканирование во всей сети, чтобы выяснить, не затронуты ли другие хосты

Мгновенно реагируйте на активные угрозы

- Автоматически помещайте на карантин файлы, ассоциированные со сложными угрозами, на всех рабочих местах
- Автоматически изолируйте зараженные хосты сразу по факту обнаружения индикатора компрометации, ассоциированного с быстро распространяющейся угрозой
- Предотвратите запуск вредоносного файла и его распространение по сети во время проведения расследования

[1] По данным глобального исследования рисков информационной безопасности (The Kaspersky Lab Global IT Risk Report), «Лаборатория Касперского», 2019 г

[2] Отчет IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDRs (Безопасность рабочих мест в 2020 г: возрождение EPP и предназначение EDR), Doc № US45794219, 2020 г.

Основные преимущества

Точное определение масштаба угрозы

Просматривайте оповещения о событиях на рабочих местах и анализируйте их, чтобы определить истинный масштаб распространения угрозы. Это поможет полностью ликвидировать последствия инцидентов, не оставляя на компьютерах никаких следов прошедшей атаки.

Экономия времени и ресурсов

Комфортное управление из единой консоли доступно как локально, так и в облаке, и сочетается с простыми сценариями EDR и инструментами контроля, такими как визуализация дерева событий, поиск индикаторов компрометации и возможности реагирования. Чтобы освоить решение, вам не потребуется много времени.

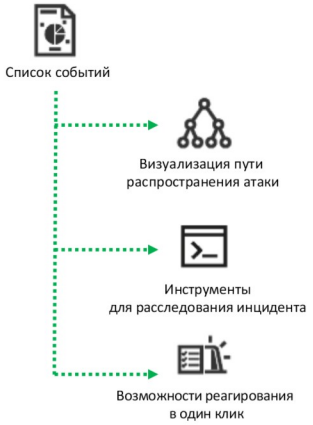
Укрепите вашу защиту

Вы можете использовать Kasperky EDR Optimum совместно с Kaspersky Sandbox и получить комплексное интегрированное решение класса Endpoint Security, обеспечивающее простую, эффективную и автоматизированную многоуровневую защиту от обычных, сложных и маскирующихся угроз.

Анализируйте данные оповещений

Kaspersky EDR Optimum предоставляет больше информации об инцидентах и помогает установить связи между отдельными событиями благодаря визуализации пути распространения атаки.

Благодаря проверке на импортированные или сгенерированные индикаторы компрометации вы можете следить за состоянием всех хостов в сети.



Оперативно принимайте ответные меры

Вы можете настроить автоматическое реагирование на угрозы, обнаруженные на рабочих местах, на базе проверок на индикаторы компрометации или моментально реагировать на инциденты сразу при их обнаружении, выбирая ответные меры в один клик.

Возможности реагирования включают изоляцию хоста, помещение файла на карантин, запуск проверки хоста и предотвращение выполнения файла.

Также рекомендуем

Kaspersky Endpoint Detection and Response Expert

Признанное EDR-решение экспертного уровня, идеально подходит для крупных IT-организаций с мощной ИБ-службой или командой SOC. Оно позволит досконально разобраться в самых изощренных продвинутых и целевых атаках. Решение использует улучшенные технологии обнаружения и активный поиск угроз, предоставляя пользователю функциональные возможности расследования и централизованного реагирования на инциденты.
https://www.kaspersky.ru/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Полностью управляемый сервис кибербезопасности, предоставляющий индивидуально настраиваемые возможности обнаружения, приоритизации, расследования и реагирования. Аналитические инструменты разработаны на основе более чем 20-летнего опыта в сфере исследования угроз. Вы получаете все основные преимущества собственного SOC без необходимости создавать его.
https://www.kaspersky.ru/enterprise-security/managed-detection-and-response

Подробную информацию о Kaspersky Endpoint Detection and Response Optimum смотрите на странице
http://www.kaspersky.ru/enterprise-security/edr-security-software-solution

www.kaspersky.ru