kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky EDR для бизнеса

Оптимальный

Угрозы для бизнеса становятся все сложнее – традиционных средств защиты конечных точек недостаточно, чтобы чувствовать себя в безопасности. Да, конечно, на рынке есть передовые решения класса EDR, но далеко не каждая компания средней величины может позволить себе их использовать – и по финансовым причинам, и по кадровым. Kaspersky EDR для бизнеса Оптимальный содержит упрощенные инструменты класса Endpoint Detection and Response (EDR), которые позволят таким компаниям смягчить ущерб от сложных атак и оперативно на них отреагировать.

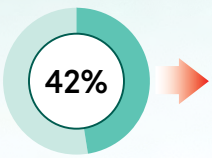
Почему безопасность рабочих мест так важна?

- Это наиболее часто используемая точка входа в инфраструктуру компании – и основная мишень киберпреступников.
- Это основной источник данных, необходимых для эффективного расследования сложных инцидентов безопасности.

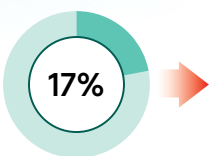
Ключевые выводы из отчета IDC, Endpoint Security 2020

- Слабое решение класса Endpoint Protection Platform (EPP) сведет на нет все преимущества EDR-решения.
- Окупаемость EDR-решения теперь измеряется время- и трудозатратами.

Ключевые результаты исследования SANS 2018, Endpoint Protection and Response



респондентов заявили, что их рабочие места подверглись атакам.



атак охватывало от 10 до 24 рабочих мест; 11% – от 100 до 249 рабочих мест

Расширенная защита рабочих мест

Kaspersky EDR для бизнеса Оптимальный – это новый уровень линейки Kaspersky Security для бизнеса, который включает в себя все возможности уровня Kaspersky Endpoint Security для бизнеса Расширенный и плюс к этому содержит упрощенные инструменты класса EDR для анализа первопричин инцидента и более точного реагирования на события безопасности.

Уровень Расширенный уже предоставляет много возможностей администраторам – это и управление установкой исправлений, и централизованная установка программ, и встроенное шифрование, и разделение прав доступа по ролям. В Kaspersky EDR для бизнеса Оптимальный к этому прибавляется возможность произвести экспресс-анализ инцидента и понять, насколько глубоко он затронул корпоративные системы.

Для работы с инструментами EDR требуется знание основ управления инцидентами, но большинство действий в продукте автоматизировано, поэтому новые инструменты не перегружают ресурсы ИБ-отдела. При этом они значительно повышают эффективность защиты от сложных атак атаками.

Единая консоль управления

Всеми функциями продукта, включая базовые инструменты EDR, можно управлять из единой консоли Kaspersky Security Center, которая дает массу возможностей по гибкой настройке системы защиты. При переходе на следующий уровень новые функции автоматически активируются в консоли, поэтому вам не нужно вновь развертывать продукт в корпоративной сети.

Доступная дополнительно песочница

Вы можете еще больше повысить безопасность рабочих мест, приобретя в дополнение песочницу. Она автоматически анализирует объекты в изолированной среде и блокирует те из них, которые вызывают подозрение.

Основные преимущества

- Полная интеграция технологий классов EDR и EPP в одном продукте.
- Полная интеграция с Kaspersky Sandbox.
- Простое управление из единой консоли.
- Требуются только базовые навыки в области ИБ.
- Низкая стоимость владения.

Технологии EDR становятся доступными: Kaspersky EDR для бизнеса Оптимальный

Kaspersky EDR для бизнеса Оптимальный помогает применить комплексный подход к отслеживанию подозрительной активности, которую стоит воспринимать не как цепочку не связанных на первый взгляд событий, а как целенаправленные злонамеренные действия или попытки скрыть следы преступления.

Вы можете легко развернуть инструменты EDR из консоли **Kaspersky Security Center**, а интуитивно понятный интерфейс упрощает управление безопасностью, позволяет быстрее изучить обнаруженную угрозу и принимать информированные решения о реагировании на инциденты.

Ключевые возможности и преимущества

Помимо мощных функций Kaspersky Security для бизнеса, у решения **Kaspersky EDR для бизнеса Оптимальный** есть следующие преимущества:

- **Автоматическое обнаружение продвинутых угроз и реагирование на них.** Автоматическая защита от продвинутых угроз, в том числе новых и уклоняющихся от обнаружения, бесфайловых атак и атак с использованием легальных инструментов.
- **Визуализация атаки.** Определение пути распространения атаки и автоматическое формирование карточки инцидента упрощает анализ первопричин и позволяет проводить более тщательное расследование.
- **Обнаружение следов угроз.** Решение поддерживает централизованную загрузку индикаторов компрометации из источников аналитических данных об угрозах или баз регулирующих органов для проверки инфраструктуры по запросу или по установленному расписанию.
- **Автоматизированная генерация пользовательских индикаторов угроз и последующих ответных мер.** Решение проверяет инфраструктуру на наличие автоматически созданных индикаторов компрометации и дает возможность применить ответные меры на всех рабочих местах.
- **Быстрое и простое реагирование.** Всего в один клик вы можете применить подходящие ответные меры: поместить файлы на карантин, изолировать отдельный хост, остановить процесс, удалить объект.
- **Углубленный динамический анализ.** Функции EDR можно дополнить песочницей, которая анализирует объекты в изолированной среде. Песочница автоматически применяет ответные меры ко всем рабочим местам.

www.kaspersky.ru