Защита конечных устройств
от сложных и целевых атак

Kaspersky EDR Expert

kaspersky активируй будущее

Kaspersky
Endpoint Detection
and Response
Expert

Экспертное решение для защиты вашей инфраструктуры

Kaspersky EDR Expert — мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты, для продвинутого обнаружения, эффективного расследования, проактивного поиска угроз и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств.

Рекомендован для компаний от 1000 узлов

> 400 млн ₽
средний ущерб от успешной кибератаки в корпоративном сегменте

23 дня
среднее время простоя бизнеса из-за атак программ-вымогателей

25%
всех атак относится к APT

Потенциальные последствия киберинцидентов

- Потеря прибыли и упущенные деловые возможности
- Ущерб репутации
- Убытки из-за простоев
- Штрафы и пени

Дополняет платформу для защиты рабочих мест

Kaspersky Security для бизнеса функциями обнаружения, расследования и реагирования, которые значительно повышают уровень безопасности

Может входить в состав платформы Kaspersky Anti Targeted Attack,

создавая решение класса XDR нативного типа

Предоставляет детализированный анализ угроз,

поддерживает автоматическое сравнение результатов внутренних расследований с глобальной репутационной базой Kaspersky Security Network и получение дополнительного контекста от Kaspersky Threat Intelligence

Ваш выбор защиты для устойчивого развития бизнеса

Решения XDR помогают отражать продвинутые атаки значительно быстрее благодаря настроенной автоматизации защитных действий на уровне сети и рабочих мест, доступу к актуальной информации об угрозах и централизованному управлению.

Технология EDR лежит в основе линейки Kaspersky Symphony — Kaspersky Symphony XDR, Kaspersky Symphony XDR Core и Kaspersky Symhony EDR.

Kaspersky Symphony XDR обеспечивает надежную защиту от кибератак, легко встраивается в текущую систему ИБ и помогает соответствовать требованиям законодательства, в том числе за счет встроенного модуля ГосСОПКА.

Сегодняшние вызовы:

Отсутствие прозрачности

для эффективного мониторинга конечных точек. Обнаружение инцидента может занять больше времени просто потому, что бывает очень сложно увидеть и понять, что произошло, как произошло и как это исправить

Использование разных консолей

для детектирования

Отсутствие соответствующих разведданных

Невозможность оперативного анализа угроз и отсутствие четкого представления о тактиках, техниках и процедурах злоумышленников могут препятствовать расследованию и реагированию

С Kaspersky EDR Expert вы сможете:

Эффективно контролировать все конечные точки

Полная прозрачность для ваших специалистов:

- Где возникла угроза
- Как она распространилась
- Какие узлы затронула
- Что именно можно и нужно сделать для предотвращения последствий

Оптимизировать работу команды ИТ-специалистов

Централизованное и автоматизированное разрешение инцидентов в вашей инфраструктуре

Быстро обнаруживать и устранять угрозы

Необработанные данные и вердикты централизованно агрегируются, а возможности расследования расширяются благодаря нашим уникальным индикаторам атак

Kaspersky EDR Expert поможет вашей организации

Повысить эффективность защиты с помощью мощного корпоративного решения по обнаружению инцидентов и реагированию на них

Усилить контроль инфраструктуры рабочих мест и повысить качество обнаружения сложных угроз с помощью продвинутых технологий

Автоматизировать выявление угроз и реагирование на них, не нарушая работу бизнеса

Наладить процессы обнаружения угроз, управления инцидентами и реагирования на них, оптимально распределяя ресурсы

Повысить эффективность внутреннего SOC

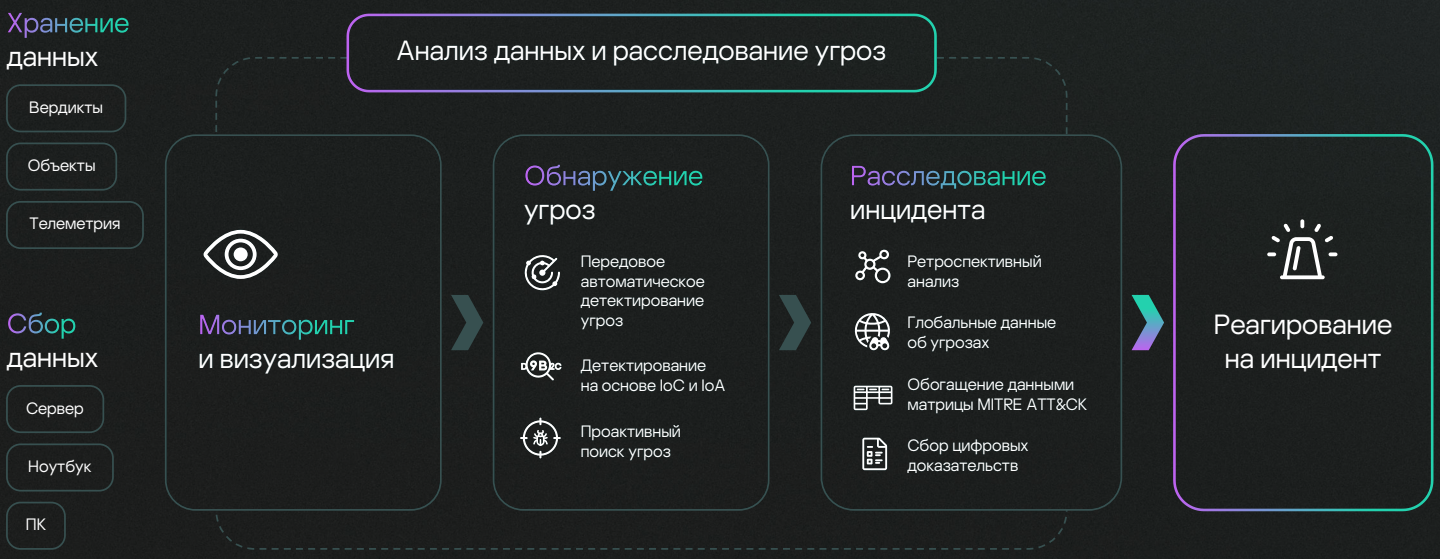
Соответствовать требованиям действующего законодательства

Быстрое обнаружение и устранение сложных угроз

Kaspersky EDR Expert надежно защищает рабочие места и повышает эффективность вашего SOC. Решение обеспечивает сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах для оперативного доступа к ретроспективным данным при расследовании продолжительных атак даже в условиях недоступности рабочих мест, а также вредоносного шифрования или уничтожения данных злоумышленниками.

Расширенные функции обнаружения и расследования на основе уникальных индикаторов атак (IoA), сопоставление с базой знаний тактик и техник злоумышленников MITRE ATT&CK, гибкий инструмент создания запросов и доступ к порталу Kaspersky Threat Intelligence — все это обеспечивает эффективное выявление угроз и быстрое реагирование на инциденты до нанесения ущерба.

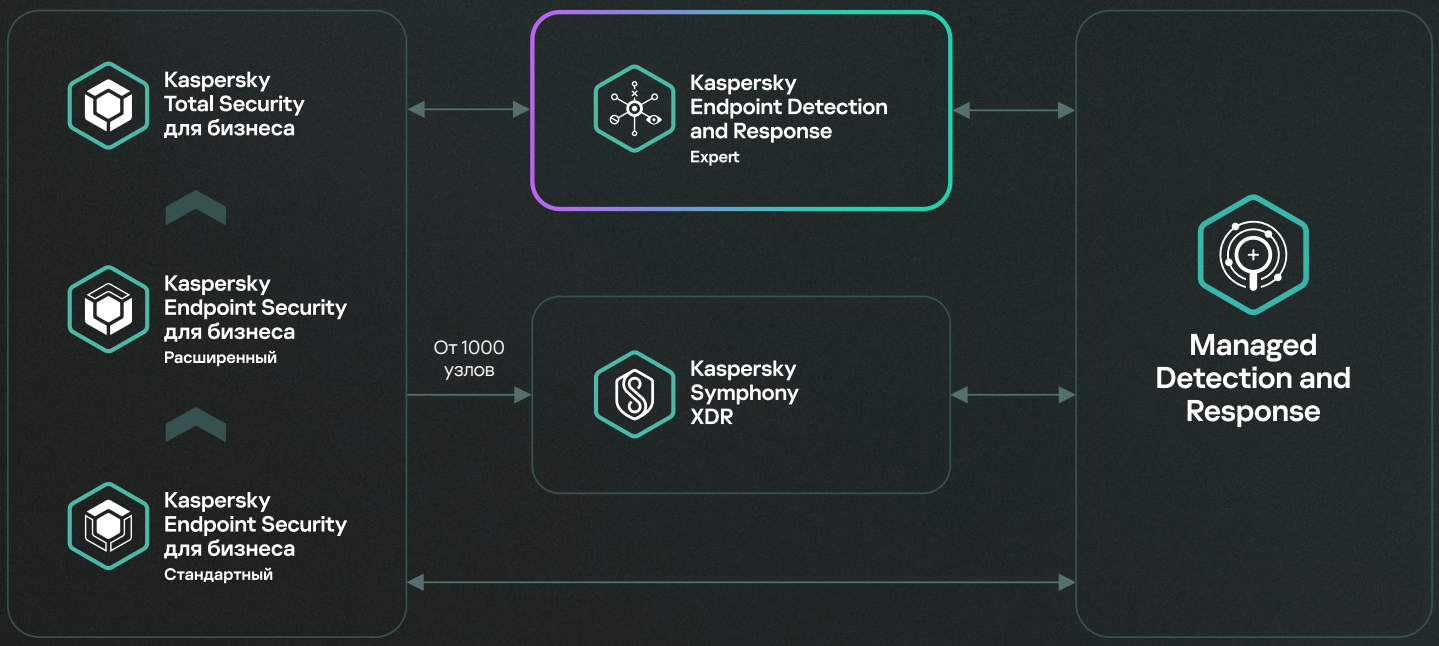
Как работает Kaspersky EDR Expert?



Усильте безопасность вашей организации с уникальными возможностями Kaspersky EDR Expert

Глубокая интеграция с Kaspersky Endpoint Security	Автоматический анализ подозрительных событий, собираемых с конечных узлов пользователей. Создание собственных правил детектирования угроз по событиям антивирусного движка.
Единый агент KEDR Expert	Развертывание и использование функционала агента EDR для сбора событий ОС и ПО в составе установленного антивирусного решения одного производителя на одном ПК.
Детектирование угроз	Уникальные IoA правила от центра экспертизы «Лаборатории Касперского». Запуск проверки по YARA-правилам на конечных точках (ОЗУ, указанные директории, локальные диски и точки автозапуска (autorun-область) по расписанию и по требованию. Возможность загрузки файлов типа Open IoC.
Расследование и реагирование	Сбор данных компьютерной криминалистики для расследования инцидента через стандартные задачи (дамп памяти процесса, получить ключ реестра, получить метафайлы NTFS, получить список процессов, получить список точек автозапуска, получить список файлов). Реагирование на инцидент посредством выполнения стандартных задач (выполнить программу/скрипт, управление службами, изоляция рабочей станции от сети, операции с карантином, возможность автоматически реагировать на вердикты технологии «песочница» и др.).
Интеграция с KSN/KPSN для проверки репутации файлов и URL-адресов в реальном времени	Подключение к приватной копии или к публичной общемировой репутационной базе производителя решения.
Встроенный компонент **Sandbox** в составе решения	Автоматическая отправка файлов в компонент «Песочница» с защищаемых рабочих станций и создание правила блокировки запуска вредоносных файлов при получении вердикта. Неограниченное количество инсталляций компонентов Central Node и Sandbox.
Запросы в KTL, интеграция с Kaspersky Threat Lookup	Получение расширенного контекста по обнаруженному IOC при запросе аналитика в онлайн базу знаний.
Возможности без использования решений класса SIEM от производителя	Создание собственных поисковых запросов в базу данных телеметрии через веб-интерфейс системы для осуществления процессов поиска угроз. Написание собственных правил обнаружения инцидентов. Визуализация графа активности ВПО на защищаемой рабочей станции.
Механизм **самозащиты** агента	Настройка механизмов защиты агента от отключения и деструктивного воздействия со стороны пользователя на рабочей станции.

Повысьте уровень защиты вашей организации



Дополнительные возможности

Kaspersky EDR Expert Plus

Kaspersky Endpoint Detection and Response Expert + Kaspersky Endpoint Security для бизнеса Расширенный

Мировое признание и доказанная эффективность

Продукты «Лаборатории Касперского» регулярно получают высокую оценку независимых экспертов. Наши решения удостоены многочисленных наград, а их эффективность подтверждена ведущими аналитиками.

AV-TEST

Независимая лаборатория AV-Comparatives протестировала Kaspersky EDR Expert и присвоила статус стратегического лидера

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Результат тестирования решения в трехлетнем цикле тестов не был превзойден: в 9 из 12 тестов был показан 100% уровень детектирования нулевой уровень ложных срабатываний

SE Labs AAA Enterprise Advanced Security EDR Detection

SE Labs протестировала эффективность Kaspersky EDR Expert против широкого спектра кибератак и присвоила решениям рейтинг AAA

MITRE ENGENUITY | ATT&CK® Evaluations

Качество обнаружения подтверждено оценкой MITRE ATT&CK. Решение Kaspersky EDR Expert прошло тестирование MITRE ATT&CK (Раунд 2), показав высокую эффективность обнаружения ключевых техник, применяемых на основных этапах проведения современных целевых атак

Соответствие требованиям регуляторов

KEDR Expert сертифицирован как средство обнаружения вторжений (СОВ уровня узла) по 4 уровню доверия, средство антивирусной защиты 4 класса защиты, средство контроля съемных машинных носителей информации 4 класса защиты.

Решение также имеет сертификаты ФСБ и Минобороны.

Ценность Kaspersky EDR Expert для вашего бизнеса

Устранение брешей в системе безопасности и быстрое обнаружение атак

Автоматизация рутинных задач по обнаружению угроз и принятию ответных мер

Освобождение ресурсов ИТ и ИБ для решения более важных задач

Ускорение выявления угроз и принятия ответных мер

Повышение эффективности анализа угроз и реагирования на инциденты

Обеспечение соответствия требованиям регулирующих органов

Узнайте, как мы помогаем компаниям, похожим на вашу

Россия и страны СНГ

Промышленность

НОРНИКЕЛЬ — Подробнее

ФОСАГРО — Подробнее

KUMTOR — Подробнее

Финансы

МКБ — Подробнее

KICB KYRGYZ INVESTMENT AND CREDIT BANK — Подробнее

БЕЛАРУСКІ НАРОДНЫ БАНК — Подробнее

Розничная торговля

МАГНИТ — Подробнее

ИТ и телеком

hh — Подробнее

MTC RED — Подробнее

Транспорт

БЧ — Подробнее

Зарубежные заказчики

Государственные структуры

قطر QATAR
اللجنة الأولمبية القطرية Qatar Olympic Committee — Подробнее

AGP — Подробнее

Kaspersky Endpoint Detection and Response Expert

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее