# Kaspersky Endpoint Detection and Response

kaspersky АКТИВИРУЙ БУДУЩЕЕ

**Сегодня киберпреступники используют продвинутые инструменты, которые позволяют им обходить современные средства защиты. Любой отдел вашей компании может подвергнуться атаке, которая нарушит работу бизнеса, снизит его производительность и увеличит операционные расходы.**

**Актуальные проблемы ИТ-безопасности:**

- необходимость ручного разбора и анализа большого числа инцидентов;
- эксплуатация средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей;
- принятие решений без использования средств для наглядного централизованного представления информации;
- выполнение сложных задач в условиях нехватки квалифицированных кадров и экспертизы;
- несоответствие требованиям регулирующих органов и действующего законодательства.

**Kaspersky EDR и ключевые выводы из отчета IDC о безопасности рабочих мест в 2020 году***

- **Слабое решение класса EPP сводит на нет все преимущества EDR-решения**

  «Лаборатория Касперского» предлагает мощную комплексную защиту конечных точек (EPP + EDR) с использованием единого агента, без дополнительных затрат на обслуживание и с минимальным воздействием на производительность рабочих мест

- **Люди и время становятся новым показателем окупаемости EDR-решений**

  «Лаборатория Касперского» применяет высокий уровень автоматизации для решения сложных задач, связанных с процессами обнаружения, расследования и реагирования, высвобождая драгоценное время ваших ИБ-экспертов

- **EDR должен анализировать данные, в том числе те, что находятся за пределами рабочих мест**

  «Лаборатория Касперского» повышает эффективность EDR, добавляя расширенное обнаружение на уровне сети в рамках единого инструмента

# Усиление существующей защиты

Рабочие места по-прежнему остаются основной мишенью злоумышленников и удобными точками входа при проведении кибератак. Чтобы защитить рабочие места и не дать злоумышленникам использовать их для проникновения в инфраструктуру, ИБ-специалистам необходимо осваивать новые способы усиления существующей системы безопасности. Полный цикл защиты рабочих мест, от автоматического блокирования распространенных угроз до быстрого реагирования на сложные инциденты, предполагает использование превентивных технологий наряду с расширенными возможностями защиты.

**Kaspersky Endpoint Detection and Response (EDR)** – это мощная система информационной безопасности, которая предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает их эффективную защиту от сложных угроз и APT-атак.

# Основные преимущества

- Kaspersky EDR дополняет платформу для защиты рабочих мест – **Kaspersky Security для бизнеса**, предлагая мощные функции обнаружения, расследования и реагирования, которые значительно повышают уровень безопасности. Единый агент для автоматической защиты от массовых угроз и расширенной защиты от сложных атак облегчает управление инцидентами и минимизирует дополнительные затраты на обслуживание. Никакой дополнительной нагрузки на рабочие места и никаких дополнительных расходов – только уверенность в том, что ваши конечные устройства и серверы надежно защищены от сложных и целевых атак.

- Kaspersky EDR позволяет сократить время, необходимое для первоначального сбора цифровых улик и анализа телеметрии, что повышает скорость реагирования на инциденты с часов до минут. Решение максимально автоматизирует повседневные задачи по выявлению, приоритизации, расследованию и нейтрализации сложных и APT-угроз. Высокая степень автоматизации в сочетании с удобством использования, повышает уровень вовлеченности ИБ-специалистов и снижает необходимость привлечения дополнительных ресурсов при общем увеличении числа качественно обработанных инцидентов.

- Kaspersky EDR может входить в состав платформы **Kaspersky Anti Targeted Attack (KATA)**, благодаря чему возможности EDR совмещаются с функциями обнаружения продвинутых угроз на уровне сети. ИБ-специалисты получают все необходимые инструменты для многостороннего выявления угроз одновременно на уровне рабочих мест и на сетевом уровне. Решение позволяет эффективно расследовать инциденты, проактивно искать угрозы и быстро и централизованно реагировать на них.

* IDC PERSPECTIVE, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR (Безопасность рабочих мест в 2020 г.: возрождение EPP и предназначение EDR)

**Kaspersky EDR поможет вашей организации:**

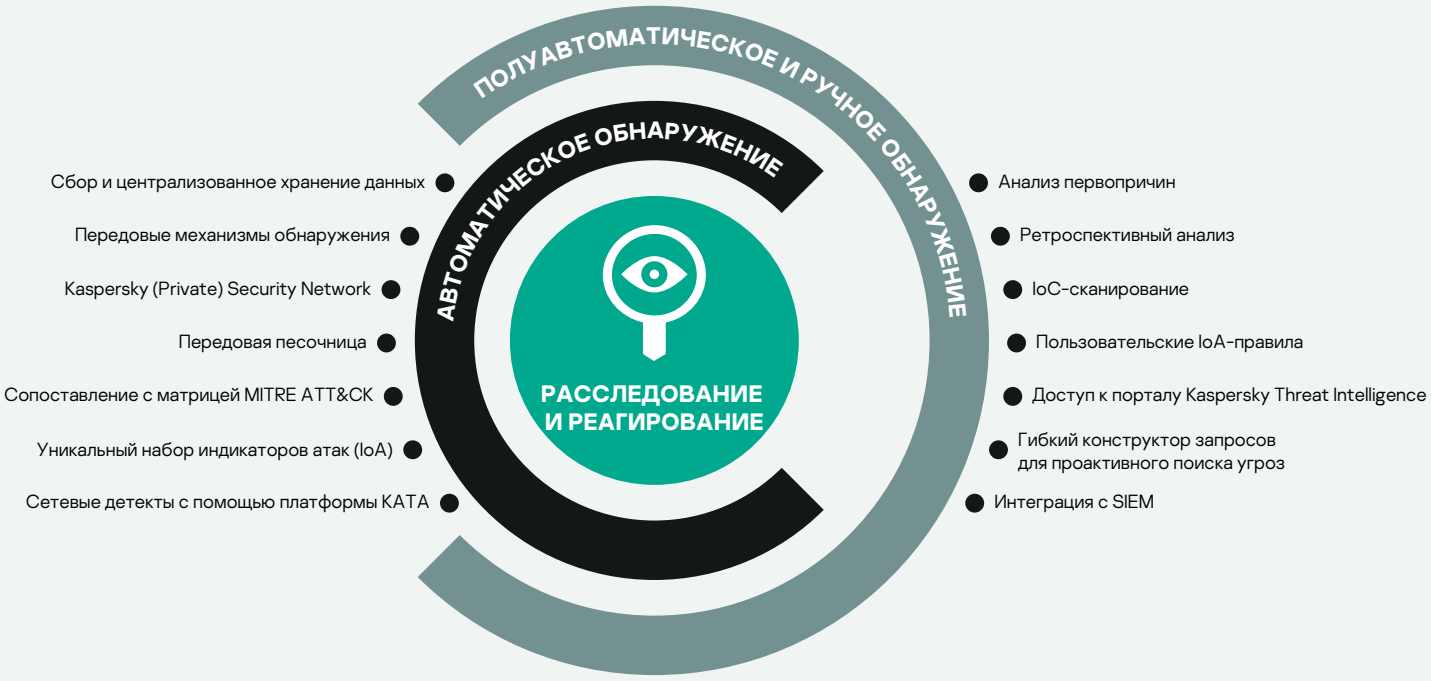
- Повысить эффективность защиты с помощью мощного корпоративного решения по обнаружению инцидентов и реагированию на них
- Усилить контроль инфраструктуры рабочих мест и повысить качество обнаружения сложных угроз с помощью продвинутых технологий
- Автоматизировать выявление угроз и реагирование на них, не нарушая работу бизнеса
- Наладить процессы обнаружения угроз, управления инцидентами и реагирования на них, оптимально распределяя ресурсы
- Повысить эффективность внутреннего центра мониторинга и реагирования (SOC)
- Обеспечить соблюдение требований действующего законодательства, своевременно предоставляя информацию об обнаруженных угрозах регулирующим органам, в строгом соответствии с требованиями российского законодательства по обеспечению безопасности критической информационной инфраструктуры (КИИ)

# Быстрое обнаружение и устранение сложных угроз

**Kaspersky EDR предлагает надежную защиту рабочих мест и повышает эффективность вашего SOC. Решение обеспечивает сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах, что позволяет обеспечить оперативный доступ к ретроспективным данным при расследовании продолжительных атак, даже в условиях недоступности рабочих мест, а также зашифровки или уничтожения данных злоумышленниками. Расширенные функции 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, позволяя предотвратить возможный ущерб.**

## Варианты использования

- **Поиск следов действующей атаки по всей сети**
- **Быстрое обнаружение вторжений и устранение их последствий до причинения серьезного ущерба**
- **Быстрое расследование и централизованное управление инцидентами для тысяч рабочих мест в рамках единого отлаженного рабочего процесса**
- **Интеграция с вашей SIEM-системой для сопоставления уведомлений от других источников с активностью на рабочих местах**
- **Проверка уведомлений о возможных угрозах, обнаруженных другими защитными решениями**
- **Автоматизация рутинных операций для высвобождения ресурсов сотрудников и максимально оперативного рассмотрения всех уведомлений**




**«Лаборатория Касперского» получила высокую награду Gartner Peer Insights Customers' Choice в категории EDR-решений**

«Лаборатория Касперского» вошла в список шести лучших мировых разработчиков EDR-решений рейтинга Gartner Peer Insights Customers' Choice в 2020 году.

Наши результаты:

- Самый высокий рейтинг (4.9 / 5.0) среди всех EDR-поставщиков.
- 98% клиентов рекомендуют решение Kaspersky EDR.

MITRE | ATT&CK®

**Качество обнаружения подтверждено оценкой MITRE ATT&CK**

Мы осознаем важность анализа тактик, техник и процедур при расследовании сложных инцидентов и понимаем, какую значимую роль играет база знаний MITRE ATT&CK на современном рынке кибербезопасности.

Поэтому:

- Решение Kaspersky EDR сопоставляет события с базой знаний тактик и техник злоумышленников MITRE ATT&CK, что позволяет проводить глубокий анализ сложных угроз и оперативно реагировать на них.
- Решение Kaspersky EDR приняло участие в тестировании MITRE ATT&CK (Раунд 2) и продемонстрировало высокую эффективность обнаружения ключевых техник, применяемых злоумышленниками в ходе современных целевых атак.

**Узнать больше:** kaspersky.com/MITRE

# Ценность Kaspersky EDR 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**

## Для еще более высокого уровня безопасности – Kaspersky Managed Detection and Response

**В дополнение к Kaspersky EDR вы можете подключить сервис постоянной защиты от кибератак Kaspersky Managed Detection and Response. Он обеспечивает круглосуточный мониторинг системы безопасности, позволяет обнаруживать и приоритизировать инциденты, а также помогает оперативно и точно на них реагировать. Благодаря этому ваши специалисты по ИБ могут сфокусироваться на решении тех задач, которые действительно требуют их участия.**

Подробная информация о Kaspersky EDR:

kaspersky.ru/enterprise-security/endpoint-detection-response-edr

**www.kaspersky.ru**