



Максимальная защита  
в едином решении

# Kaspersky Anti Targeted Attack

Kaspersky EDR Expert

# Ваш выбор защиты

для устойчивого  
развития бизнеса



## «Лаборатория Касперского» позволяет организациям:

Внедрить единую надежную систему защиты корпоративной инфраструктуры от сложных атак.

Снизить нагрузку на службу информационной безопасности.

Оптимизировать затраты на процесс расследования и реагирования на комплексные инциденты.

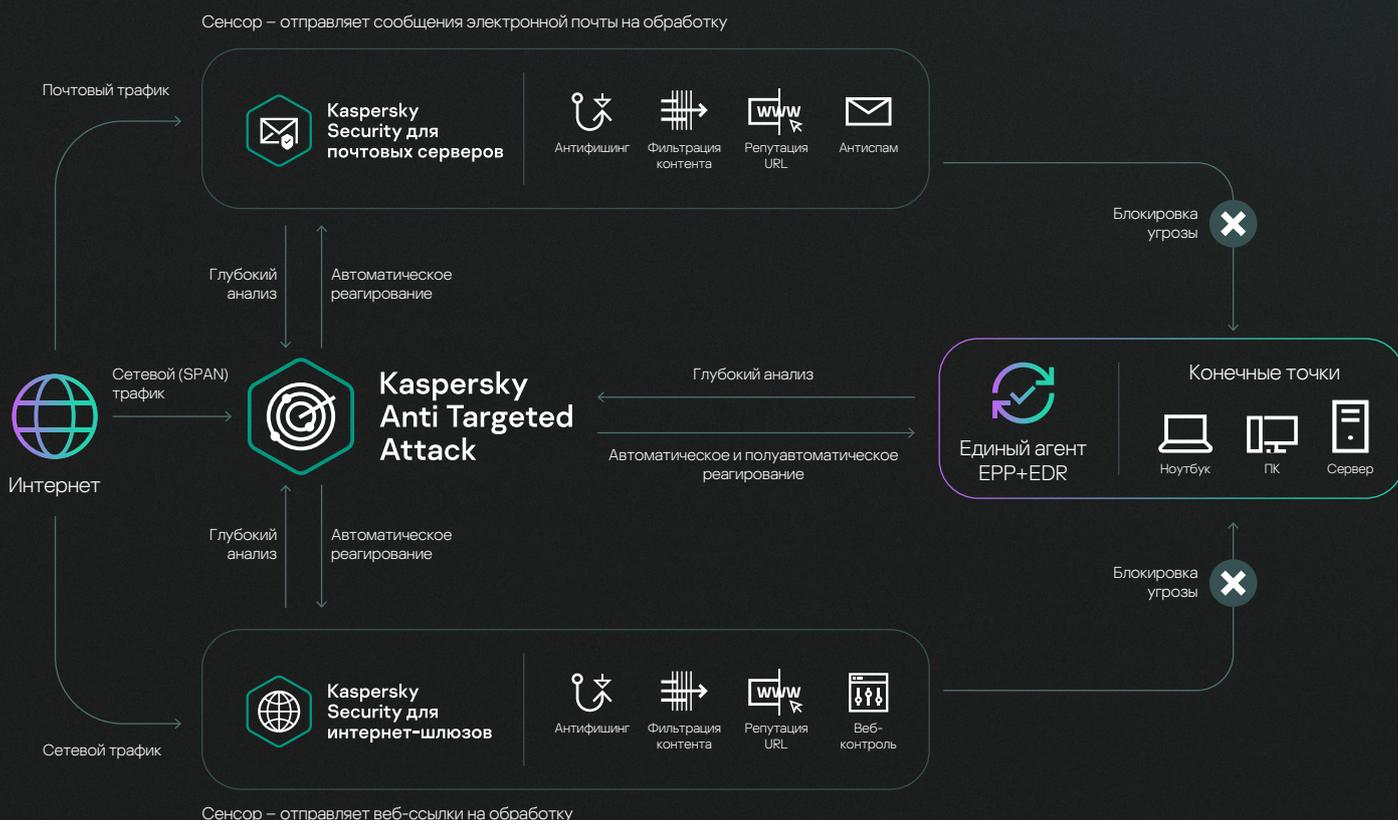
Обеспечить соответствие требованиям регуляторов.

# Максимальная защита в едином решении

Несмотря на киберагрессию, усиливающийся хактивизм и массовое импортозамещение, поддержка непрерывности бизнес-процессов, безопасность данных и IT-инфраструктуры, а также соответствие требованиям законодательства остаются необходимыми условиями для устойчивого развития бизнеса.

Платформа Kaspersky Anti Targeted Attack, усиленная возможностями Kaspersky EDR Expert, обеспечивает передовую защиту от комплексных угроз и целевых атак в едином решении и представляет собой решение класса XDR нативного типа. Kaspersky Security для почтовых серверов и Kaspersky Security для интернет-шлюзов выступают сенсорами для автоматического ответа на сложные угрозы на уровне сети. Организации теперь могут **контролировать и надежно защищать** все популярные точки входа потенциальных угроз: сеть, веб-трафик, электронную почту, рабочие места, серверы и виртуальные машины.

Полная визуализация данных, возможность проведения глубокого анализа сетевого трафика, эмуляция угроз при помощи продвинутой песочницы и мощные технологии EDR – все это делает расследование и реагирование на инциденты более быстрыми, точными и эффективными. В дополнение к встроенным передовым технологиям обнаружения и анализа платформа обогащается аналитическими данными об угрозах (Threat Intelligence) и сопоставлением обнаружений с базой знаний тактик и техник злоумышленников MITRE ATT&CK.



## Преимущества

Обнаружение сетевой активности по 80 протоколам, в частности по 53 протоколам прикладного уровня

Корреляция сетевых событий с событиями на рабочих станциях в одном продукте

Поддержка российских операционных систем

Доступ к сильнейшей в мире аналитике об угрозах

Более 300 успешных проектов по России и миру

Отзывы

## Соответствие требованиям

Решение помогает организациям соответствовать стандартам банковской отрасли, PCI DSS, а также нормативным требованиям GDPR и № 187-ФЗ.

Решение сертифицировано ФСТЭК России и ФСБ России, полностью соответствует требованиям закона о защите персональных данных, включено в реестр российского ПО (рег. номер ПО № 8350 от 30.12.2020 и рег. номер ПО № 8352 от 30.12.2020), а также соответствует требованиям ГОСТ Р 56939-2016.

Подробнее

## Основные возможности

Kaspersky Anti Targeted Attack с входящим Kaspersky EDR Expert обеспечивает надежную защиту корпоративной инфраструктуры организаций от сложных угроз и целевых атак в полном соответствии с требованиями законодательства. Это решение помогает службам IT-безопасности отражать продвинутые атаки значительно быстрее и с меньшими усилиями благодаря оптимально настроенной автоматизации защитных действий на уровне сети и рабочих мест, доступу к актуальной информации об угрозах и управлению через единую консоль.



### Многоуровневая архитектура

обеспечивает абсолютную прозрачность за счет совместной работы сетевых, почтовых и интернет-сенсоров, а также агентов на рабочих местах.



### Мощные аналитические модули

работают с данными сетевых сенсоров (анализ сетевого трафика) и агентов рабочих мест (функциональность EDR), обеспечивая быстрое вынесение вердиктов.



### Производительная песочница

позволяет запускать подозрительные объекты в изолированной среде и осуществлять их многоуровневый анализ. Поддерживается кастомизация образов.



### Аналитика угроз в двух режимах

автоматическая сверка с глобальными репутационными данными Kaspersky Security Network и доступ к portalу Kaspersky Threat Intelligence.



### Ретроспективный анализ

в том числе в ситуациях, когда конечные устройства недоступны, а данные зашифрованы. Это возможно благодаря автоматизированному сбору данных, объектов и вердиктов в централизованное хранилище.



### Проактивный поиск сложных атак

аналитики могут составлять сложные запросы для поиска аномального поведения, техник MITRE ATT&CK, а также подозрительной активности и угроз, характерных для вашей инфраструктуры.



### Автоматический поиск сложных угроз

обеспечивается благодаря большому набору встроенных передовых механизмов обнаружения угроз. События сопоставляются с уникальным набором индикаторов атак и базой знаний тактик и техник злоумышленников MITRE ATT&CK, содержащей четкие описания, примеры и рекомендации по реагированию.

# Международное признание



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



«Лаборатория Касперского» получила высокую награду Gartner Peer Insights Customers' Choice в категории EDR-решений. Покупатели высоко оценили платформу Kaspersky Anti Targeted Attack и Kaspersky EDR Expert.



В независимом тесте ICSA Labs: Advanced Threat Defense платформа Kaspersky Anti Targeted Attack показала 100-процентный результат обнаружения угроз, не допустив ни одного ложного срабатывания.



Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете «Advanced Persistent Threat (APT) Protection – Market Quadrant, 2022».



Качество обнаружения подтверждено оценкой MITRE ATT&CK.



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



## Kaspersky Anti Targeted Attack

[Подробнее](#)



## Kaspersky EDR Expert

[Подробнее](#)

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2023 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky  
#активнуйбудущее