Решение класса XDR: современная защита от сложных кибератак

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Платформа XDR от «Лаборатории Касперского» позволяет

- **ВНЕДРИТЬ** единую надежную систему защиты корпоративной инфраструктуры от сложных угроз и целевых атак
- **СНИЗИТЬ** нагрузку на службу информационной безопасности
- **ОПТИМИЗИРОВАТЬ** затраты на процесс расследования и реагирования на комплексные инциденты
- **ОБЕСПЕЧИТЬ** соответствие требованиям регуляторов

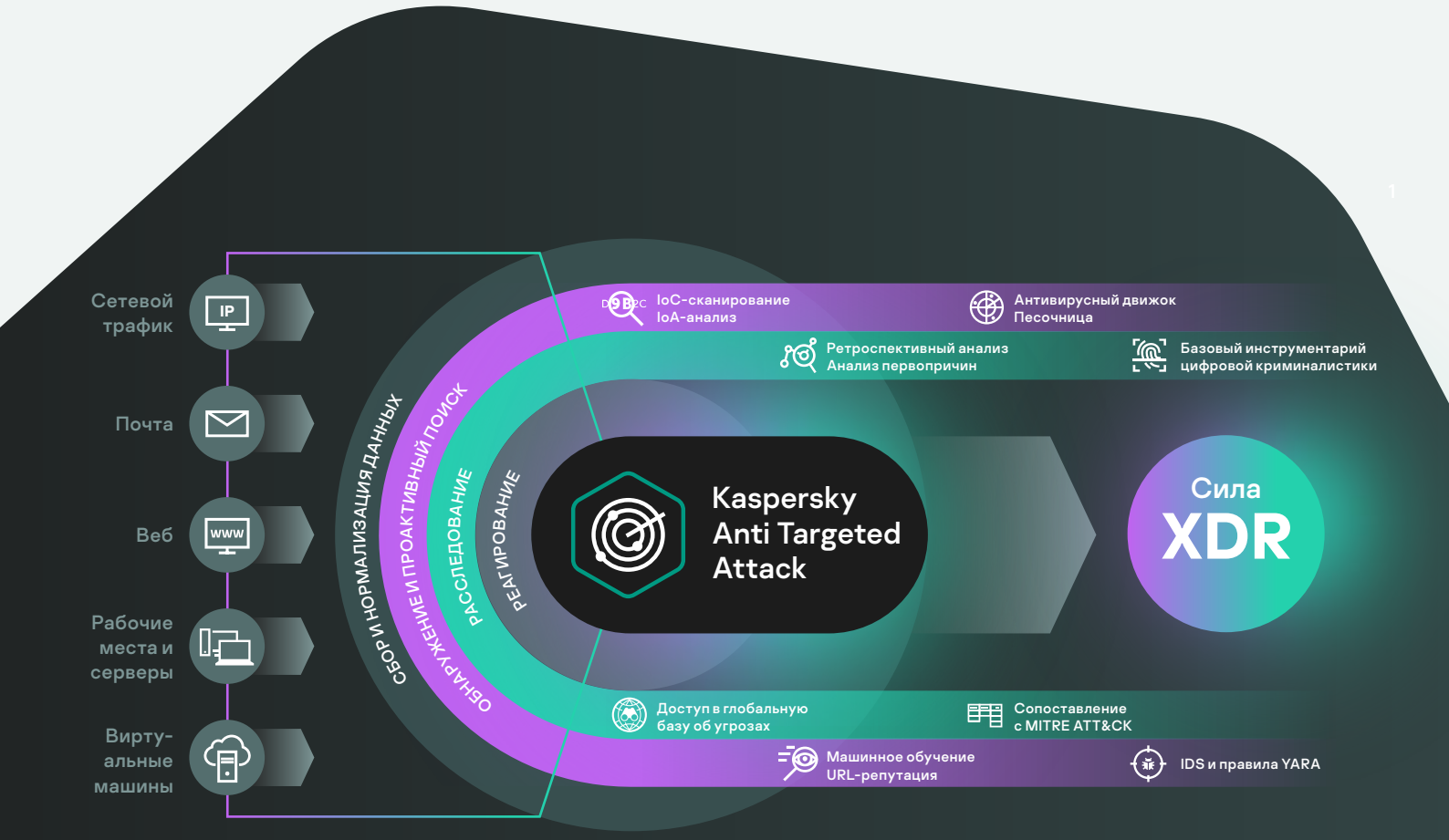
Максимальная защита в едином решении

Сегодня надежная защита данных, безопасность IT-инфраструктуры, устойчивость бизнес-процессов и соответствие требованиям законодательства – необходимое условие для устойчивого развития бизнеса.

«Лаборатория Касперского» обеспечивает надежную защиту организаций от сложных угроз, APT- и целевых атак в полном соответствии с требованиями законодательства, предоставляя решение класса XDR (Extended Detection and Response).

Платформа Kaspersky Anti Targeted Attack, объединенная с Kaspersky EDR, сочетает расширенный функционал для обнаружения угроз на уровне сети и возможности EDR. Это комплексное решение класса XDR для обнаружения, расследования и реагирования на кибератаки на основе унифицированной серверной архитектуры и централизованного управления из единой веб-консоли. Теперь вы можете контролировать и надежно защищать все популярные точки входа потенциальных угроз: сеть, веб-трафик, электронную почту, рабочие места, серверы и виртуальные машины.

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.



Соответствие региональному и международному законодательству

Платформа Kaspersky Anti Targeted Attack помогает организациям соответствовать стандартам банковской отрасли, PCI DSS, а также нормативным требованиям GDPR и приказам ФСБ в части установления причин и условий возникновения компьютерных инцидентов с учетом требований российского законодательства.

Преимущества платформы XDR:

- **Сокращение рисков** информационной безопасности
- **Повышение продуктивности** и качества работы сотрудников ИТ- и ИБ-департаментов
- **Оптимизация трудозатрат** высококвалифицированных кадров
- **Сокращение количества** рутинных ручных операций
- **Увеличение количества обрабатываемых инцидентов** без дополнительных трудозатрат
- **Сбор, хранение и предоставление информации** об инцидентах ИБ в рамках требований внутреннего и внешнего регулирования и отраслевого законодательства

Основные возможности

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.

Высокопроизводительная песочница позволяет запускать подозрительные объекты в изолированной среде и осуществлять их многоуровневый анализ. Возможности детально исследовать поведение анализируемых объектов, а также сопоставлять обнаруженную подозрительную активность с базой знаний MITRE ATT&CK позволяют оперативно реагировать на сложные инциденты.

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.

Аналитика угроз, работающая в двух режимах, – автоматическая сверка с глобальными репутационными данными Kaspersky Security Network и доступ к порталу Kaspersky Threat Intelligence.

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.

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.

Ваш выбор защиты для устойчивого развития бизнеса

Решение XDR «Лаборатории Касперского» обеспечивает надежную защиту корпоративной инфраструктуры организаций от сложных угроз и целевых атак в полном соответствии с требованиями законодательства. Это комплексное 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. При интеграции в текущую стратегию организации платформа обеспечивает службу IT-безопасности и команды SOC всем необходимым для надежного и эффективного отражения сложных атак, дополняя существующие сторонние технологии защиты и поддерживая интеграцию с SIEM-системами.

Международное признание

SE Labs протестировала эффективность платформы Kaspersky Anti Targeted Attack против широкого спектра кибератак и **присвоила решению рейтинг AAA.**

Победитель Gartner Peer Insights Customers' Choice в категории EDR-решения, 2020 год.

«Лаборатория Касперского» получила высокую награду Gartner Peer Insights Customers' Choice в категории EDR-решений. Всего 6 производителей в мире стали обладателями этой награды. Покупатели высоко оценили платформу Kaspersky Anti Targeted Attack и Kaspersky EDR.

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

Качество обнаружения подтверждено оценкой MITRE ATT&CK

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

Подробнее: kaspersky.com/MITRE

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» **ведущим игроком (Top Player) в отчете «Advanced Persistent Threat (APT) Protection – Market Quadrant, 2021».**

Kaspersky Anti Targeted Attack

Узнать больше

www.kaspersky.ru