Платформа Kaspersky Anti Targeted Attack

kaspersky АКТИВИРУЙ БУДУЩЕЕ

В эпоху цифровой трансформации корпоративная служба информационной безопасности должна стать ключевым звеном цифровой бизнес-стратегии организаций. Построение надежной системы защиты корпоративной инфраструктуры от сложных угроз и целевых атак, а также оперативное выявление инцидентов, уменьшение объема ручных операций, оптимизация трудозатрат и повышение эффективности работы службы ИБ и команд SOC позволяют обеспечить устойчивое развитие крупного бизнеса.

Крайне важно, чтобы предприятия продолжали усиливать и адаптировать свои средства защиты ИТ,

чтобы оставаться на шаг впереди растущих темпов киберугроз и предупреждать возможные финансовые потери.

Платформа Kaspersky Anti Targeted Attack 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

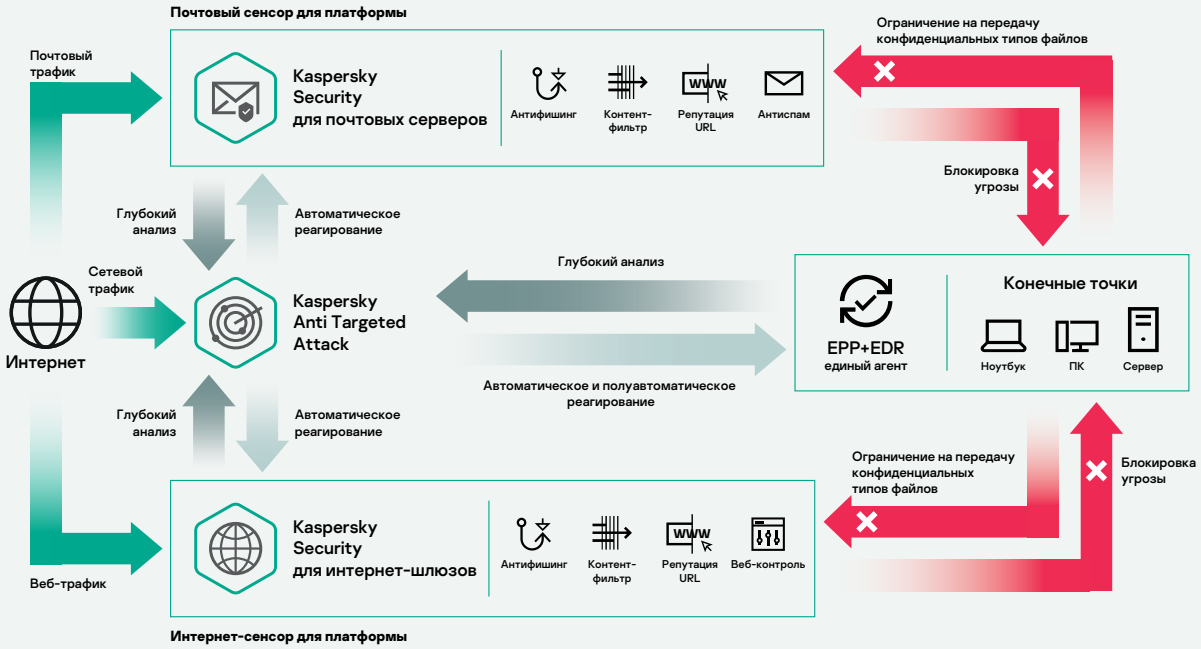
Максимальная защита в едином решении

Современные киберпреступники используют многовекторный подход. Платформа Kaspersky Anti Targeted Attack объединяет возможности обнаружения продвинутых угроз на уровне сети и технологии EDR. Специалисты по IT-безопасности получают в едином решении все инструменты, которые позволят выявлять угрозы на всех уровнях развития целевой атаки, проводить эффективные расследования и проактивный поиск угроз, а также оперативно и централизованно реагировать на инциденты.

Специализированная платформа для противодействия комплексным угрозам

Платформа Kaspersky Anti Targeted Attack – это решение класса Extended Detection and Response, которое обеспечивает комплексную защиту от сложных угроз и целевых атак, позволяя контролировать все точки входа потенциальных угроз – сеть, веб-трафик, электронную почту, ПК, ноутбуки, 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.

Платформа Kaspersky Anti Targeted Attack полностью интегрируется с **Kaspersky Security для бизнеса** через единый агент с Kaspersky EDR. Платформа также интегрируется с **Kaspersky Security для почтовых серверов** и **Kaspersky Security для интернет-шлюзов,** которые выполняют роль сенсоров и позволяют автоматически реагировать на более сложные угрозы на сетевом уровне, найденные платформой.



Соответствие региональному и международному законодательству

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

Преимущества платформы Kaspersky Anti Targeted Attack:

- **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. 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.

Комплексная защита бизнеса от 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.

Устойчивое развитие бизнеса

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

Платформа Kaspersky Anti Targeted Attack 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.**

В независимом тесте ICSA Labs: Advanced Threat Defense (3 квартал 2019 года.) платформа Kaspersky Anti-Targeted Attack показала **100% 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, 2020».**

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.

Наши результаты:

- Высший рейтинг (4.9 / 5.0) среди всех EDR-поставщиков.
- 98% клиентов рекомендуют платформу Kaspersky Anti Targeted Attack и Kaspersky EDR.

Качество обнаружения подтверждено оценкой MITRE ATT&CK

Ключевой элемент платформы Kaspersky Anti Targeted Attack – 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

Узнать больше:

kaspersky.ru/enterprise-security/anti-targeted-attack-platform

www.kaspersky.ru