Непрерывный поиск, обнаружение и устранение угроз, направленных на ваше предприятие

Kaspersky Managed Detection and Response

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Преимущества сервиса Kaspersky MDR

Уверенность в том, что вы находитесь под постоянной защитой даже от самых сложных и изощренных угроз

Сокращение расходов на безопасность из-за отсутствия необходимости нанимать новых ИБ-специалистов

Возможность направить внутренние ИБ-ресурсы компании на решение других ИБ-задач

Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри компании

Быстрое подключение и простота использования консоли управления

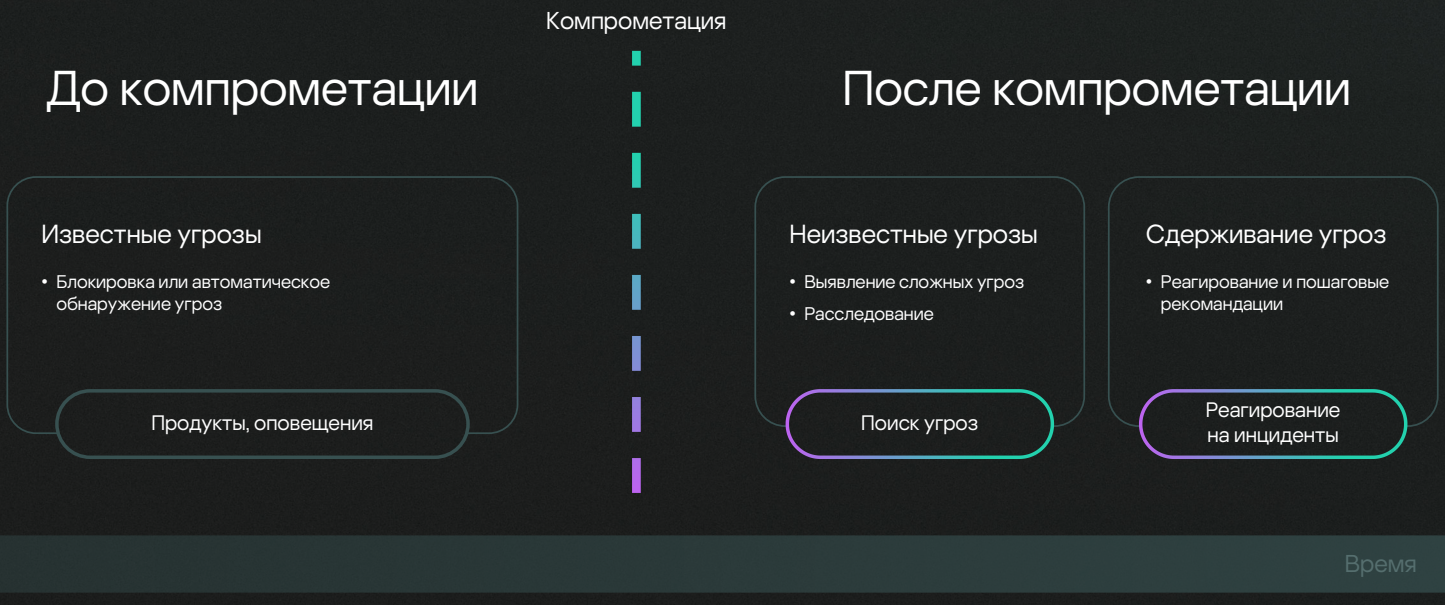
Управляемая защита вашего бизнеса

В связи с широкомасштабной автоматизацией бизнес-процессов деятельность предприятий все сильнее зависит от информационных технологий. Это делает компании более уязвимыми для хакерских атак на корпоративные ИТ-системы. При этом организации могут иметь ограниченные ИБ-ресурсы или же службы ИБ могут быть перегружены рутинными задачами, что оставляет им мало времени для тщательной обработки киберинцидентов. Кроме того, найти опытных специалистов по обнаружению и реагированию на инциденты — совсем не простая задача.

Kaspersky Managed Detection and Response (MDR) предоставляет круглосуточную управляемую защиту от растущего числа киберугроз и сложных атак, обходящих автоматические средства безопасности. Сервис подходит как небольшим организациям, у которых нет выделенных ИБ-специалистов или которые испытывают нехватку знаний в вопросе реагирования на киберинциденты, так и более крупным компаниям, ИБ-эксперты которых нуждаются в дополнительной точке зрения.

Эффективные функции обнаружения и реагирования дополнены знаниями одной из самых успешных и опытных в отрасли команд по активному поиску угроз. Kaspersky MDR использует модели машинного обучения, постоянный доступ к аналитическим данным об угрозах и результатам успешных расследований APT-атак. Сервис автоматически повышает устойчивость организации к киберугрозам, помогает эффективно использовать имеющиеся ресурсы, а также оптимизировать будущие инвестиции в информационную безопасность.

Kaspersky MDR обеспечит защиту бизнеса в режиме 24/7, даже если до подключения сервиса компрометация уже случилась, действия злоумышленников не останутся не обнаруженными.



Источники телеметрии для MDR:

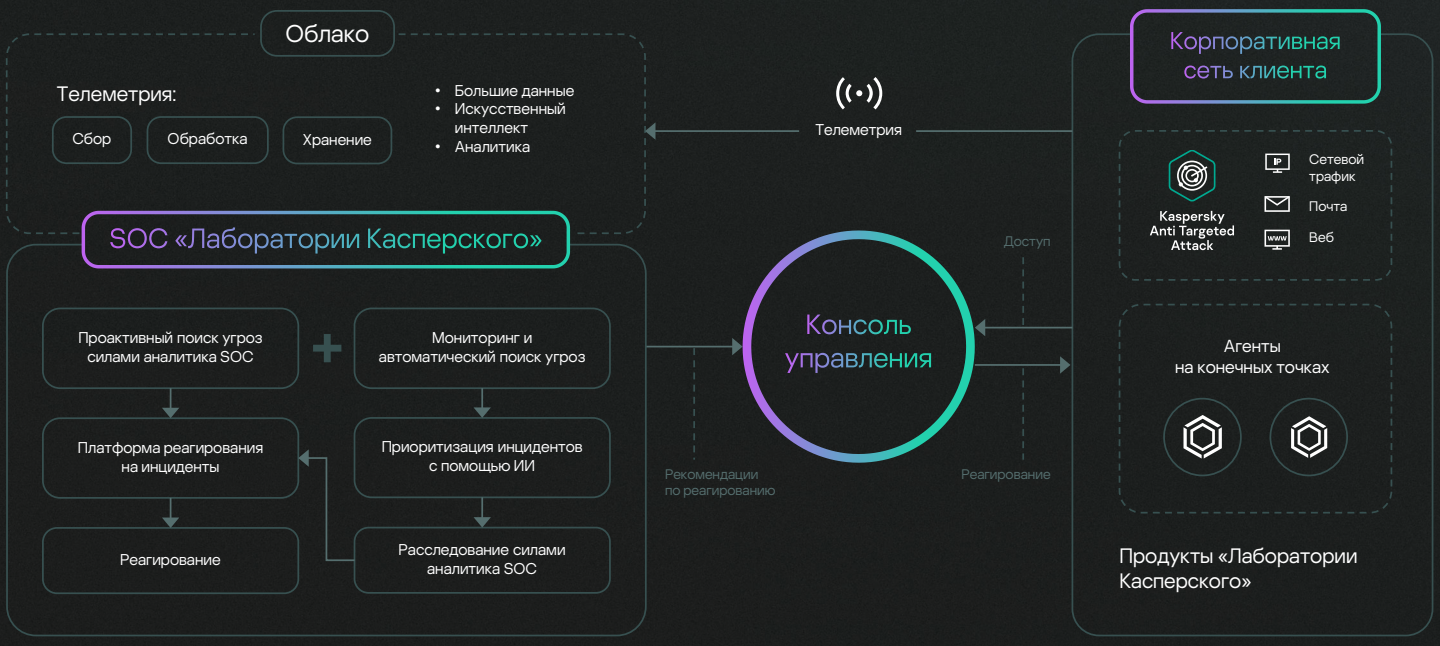
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent Windows
- Kaspersky Anti Targeted Attack

Как работает сервис

Команда Kaspersky MDR расследует события безопасности и проактивно анализирует телеметрию, получаемую от установленных в сети клиента продуктов «Лаборатории Касперского», на предмет инцидентов. Эта телеметрия сопоставляется с аналитическими данными «Лаборатории Касперского» об угрозах для выявления тактик, техник и процедур, применяемых злоумышленниками против конкретной организации. При этом уникальные индикаторы атак позволяют обнаружить скрытые угрозы, не использующие вредоносное ПО и имитирующие легитимную активность.

В рамках сервиса у клиента есть возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию для дальнейшей проверки экспертами SOC «Лаборатории Касперского». Встроенные механизмы искусственного интеллекта (ИИ) в Kaspersky MDR помогают минимизировать число ложноположительных срабатываний и ускорить процесс обработки событий безопасности. При возникновении вопросов всегда можно обратиться напрямую к экспертам SOC.

- Знания и опыт экспертов международного уровня
- Передовые технологии защиты
- Проактивный мониторинг и поиск угроз
- Автоматизированное и управляемое реагирование



Дополнение к Kaspersky MDR:

Kaspersky Incident Response

Глубокое расследование и расширенное реагирование на инциденты разной степени сложности

Kaspersky Digital Footprint Intelligence

Выявление внешних признаков атаки через поиск угроз в открытых источниках, базе знаний «Лаборатории Касперского» и на ресурсах даркнет

Kaspersky Cybersecurity Training

Практические тренинги для ИБ-экспертов по реагированию на инциденты

Kaspersky Threat Intelligence

Дополнительный контекст по индикаторам, тактикам, техникам и процедурам, используемым злоумышленниками

Уровни Kaspersky MDR

Kaspersky MDR предусматривает два уровня защиты (Optimum и Expert) и подходит организациям с разными ИБ-потребностями.

Kaspersky MDR Optimum повышает уровень информационной безопасности небольших организаций с невысоким уровнем ИБ-экспертизы за счет быстрого развертывания услуги «под ключ». Решение обеспечивает круглосуточный мониторинг, обнаружение и приоритизацию инцидентов, а также помогает оперативно и эффективно на них реагировать.

Kaspersky MDR Expert включает в себя все возможности Kaspersky MDR Optimum, а также предоставляет дополнительную гибкость для опытных ИБ-команд. Крупные организации с развитой ИБ-экспертизой могут передать вопросы классификации и обнаружения инцидентов в «Лабораторию Касперского» или же получить дополнительное мнение по обнаруженным самостоятельно инцидентам.

Качество и эффективность ретроспективного анализа в рамках уровня Kaspersky MDR Expert увеличиваются благодаря хранению телеметрии в течение 3 месяцев, что способствует расширению возможностей по выявлению инцидентов. Организациям также предоставляется доступ к порталу Kaspersky Threat Lookup и Kaspersky Cloud Sandbox, что позволяет обогащать имеющиеся знания подробными актуальными данными по веб-адресам, доменам, IP-адресам, хешам файлов, статистическим и поведенческим данным, данным WHOIS/DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и прочему. Облачная песочница (Kaspersky Cloud Sandbox) позволяет связать эти данные с индикаторами компрометации, сгенерированными анализируемым образцом.

Kaspersky Managed Detection and Response

	Optimum	Expert
Круглосуточный мониторинг	●	●
Автоматизированный поиск угроз	●	●
Проактивный поиск угроз (Threat Hunting) силами экспертов «Лаборатории Касперского»	●	●
Сценарии реагирования и автоматическое реагирование на инциденты	●	●
Консультации аналитиков SOC «Лаборатории Касперского»	●	●
Обзор всех защищаемых ресурсов с их текущим статусом	●	●
Консоль управления с панелями мониторинга и отчетами	●	●
Хранение истории инцидентов безопасности в течение 1 года	●	●
Доступ к порталу Kaspersky Threat Intelligence		●
API для интеграции с IRP/SOAR		●
Возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию и получить подробный анализ от экспертов SOC		●
Хранение необработанной телеметрии	1 месяц	3 месяца

Подтвержденная эффективность

Сервис Kaspersky MDR разработан на основе аналитических данных об APT-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского».

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Наши технологии признаны во всем мире и удостоены многочисленных международных наград.

The Radicati Group, Inc.
A Technology Market Research Firm

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете Advanced Persistent Threat (APT) Protection в 2022 году

AV comparatives

Ежегодно защитные решения класса EPP «Лаборатории Касперского» получают высокие оценки в тестированиях AV-Comparatives

Gartner Peer Insights Customers' Choice 2022

Сервис Kaspersky Managed Detection and Response получил наивысшие оценки в рейтинге Gartner Peer Insights™ (в категории «Сервисы MDR»). 100% пользователей готовы рекомендовать сервис Kaspersky MDR

Quadrant Knowledge Solutions

Консалтинговая компания «Quadrant Knowledge Solutions» назвала «Лабораторию Касперского» технологическим лидером 2022 года на глобальном рынке решений MDR, а также лидером на рынке управляемых сервисов MSS

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave: External Threat Intelligence Services, 2021)

MITRE | ATT&CK®

Качество обнаружения угроз в Kaspersky MDR подтверждено оценкой MITRE ATT&CK в 2020 году

Kaspersky Managed Detection and Response

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее