



Непрерывный поиск,
обнаружение и помощь
в устранении киберугроз,
направленных на вашу
организацию

Kaspersky MDR

kaspersky активируй
будущее

Преимущества



Уверенность в том, что вы находитесь под постоянной защитой



Сокращение расходов 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

Сегодня компании сталкиваются с целенаправленной киберагрессией и хактивизмом. Как следствие — необходимость в эффективной киберзащите возрастает с каждым днем. Организации могут иметь ограниченные ИБ-ресурсы, или же службы ИБ могут быть перегружены, что оставляет им мало времени для тщательной обработки киберинцидентов. К тому же найти опытных специалистов по обнаружению и реагированию на инциденты — совсем непростая задача.

Kaspersky Managed Detection and Response (MDR) — это решение по круглосуточной управляемой защите от растущего числа киберугроз и сложных атак, обходящих автоматические средства безопасности. Решение повышает уровень информационной безопасности небольших организаций с невысоким уровнем ИБ-экспертизы за счет быстрого развертывания услуги «под ключ». А для опытных команд с развитой ИБ-экспертизой предоставляет дополнительную гибкость, поскольку они могут передать вопросы обнаружения и классификации инцидентов в «Лабораторию Касперского» или же получить дополнительное мнение по обнаруженным самостоятельно инцидентам.

Решение Kaspersky MDR повышает устойчивость организации к киберугрозам, помогает эффективно использовать имеющиеся ресурсы, а также оптимизировать будущие инвестиции в информационную безопасность.

Ключевые возможности

1

Мониторинг и проактивный поиск угроз (Threat Hunting)

2

Обзор всех защищаемых ресурсов с их текущим статусом

3

Автоматическое реагирование и другие сценарии реагирования на инциденты

4

Консультации аналитиков SOC

5

REST API для интеграции с IRP / SOAR

6

Консоль управления с панелями мониторинга и отчетами

7

Хранение необработанной телеметрии в течение 3 месяцев

8

Возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию

9

Хранение истории инцидентов безопасности в течение 1 года

Возможные источники телеметрии для Kaspersky MDR:



Kaspersky Endpoint Security for Windows



Kaspersky Endpoint Security for Mac



Kaspersky Endpoint Security for Linux



Kaspersky Security for Virtualization Light Agent



Kaspersky Anti Targeted Attack

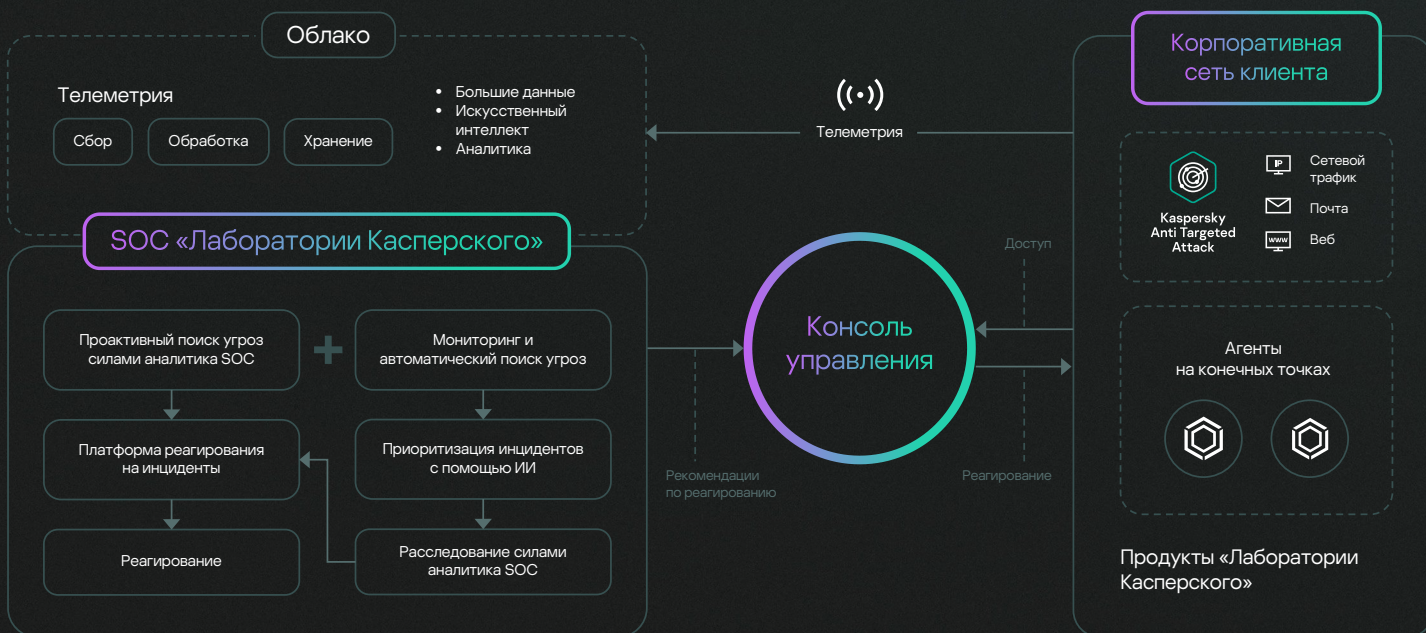
Как работает решение

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» о киберугрозах и результатами успешных расследований APT-атак 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 процесса обработки событий безопасности в Kaspersky MDR внедрены механизмы искусственного интеллекта (ИИ). Они способствуют снижению количества ложноположительных срабатываний и ускоряют процесс обработки событий безопасности. При обнаружении потенциальной угрозы решение классифицирует ее по уровню критичности и отправляет уведомление об инциденте на электронную почту и/или в Telegram. А анализ первопричин позволяет выявлять источники и принимать меры для их нейтрализации.

В рамках решения клиент может частично или полностью передать возможности по реагированию команде SOC «Лаборатории Касперского». Имеющиеся вопросы в рамках инцидента можно обсудить в интерактивном чате в веб-консоли Kaspersky MDR.

Архитектура решения



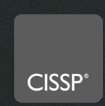
Kaspersky MDR совместим со сторонними антивирусными решениями.

Подтвержденная эффективность

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Решение Kaspersky MDR признано во всем мире и удостоено многочисленных международных наград. А эффективные функции обнаружения и реагирования в Kaspersky MDR дополнены знаниями одной из самых успешных и опытных в отрасли команд по активному поиску угроз — команды SOC «Лаборатории Касперского», эксперты которой обладают многочисленными сертификатами, подтверждающими их высокий уровень экспертизы и знаний.



MITRE | ATT&CK®



Kaspersky Managed Detection and Response

[Подробнее](#)

www.kaspersky.ru

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее