

Обзор возможностей

Kaspersky Managed Detection and Response

kaspersky активируй
будущее

Содержание

Обзор Kaspersky MDR	3
Принцип работы Kaspersky MDR	4
Возможности решения	5
Поддерживаемые продукты	7
Чем Kaspersky MDR отличается от других решений	8

Обзор Kaspersky MDR



Kaspersky Managed Detection and Response

Решение **Kaspersky Managed Detection and Response (MDR)** предоставляет круглосуточную управляемую защиту, включающую мониторинг, обнаружение, расследование и реагирование на инциденты информационной безопасности. Вы получаете все основные преимущества собственного центра SOC без необходимости его создания.

Решение MDR позволяет выявлять угрозы на всех этапах кибератаки, как до компрометации, так и после проникновения злоумышленников в инфраструктуру организации. Это достигается благодаря двум неотъемлемым компонентам Kaspersky MDR – превентивной защите и проактивному поиску угроз.

Использование MDR совместно с Kaspersky Incident Response повышает эффективность всего цикла управления инцидентами – от обнаружения угрозы до устранения последствий атаки.

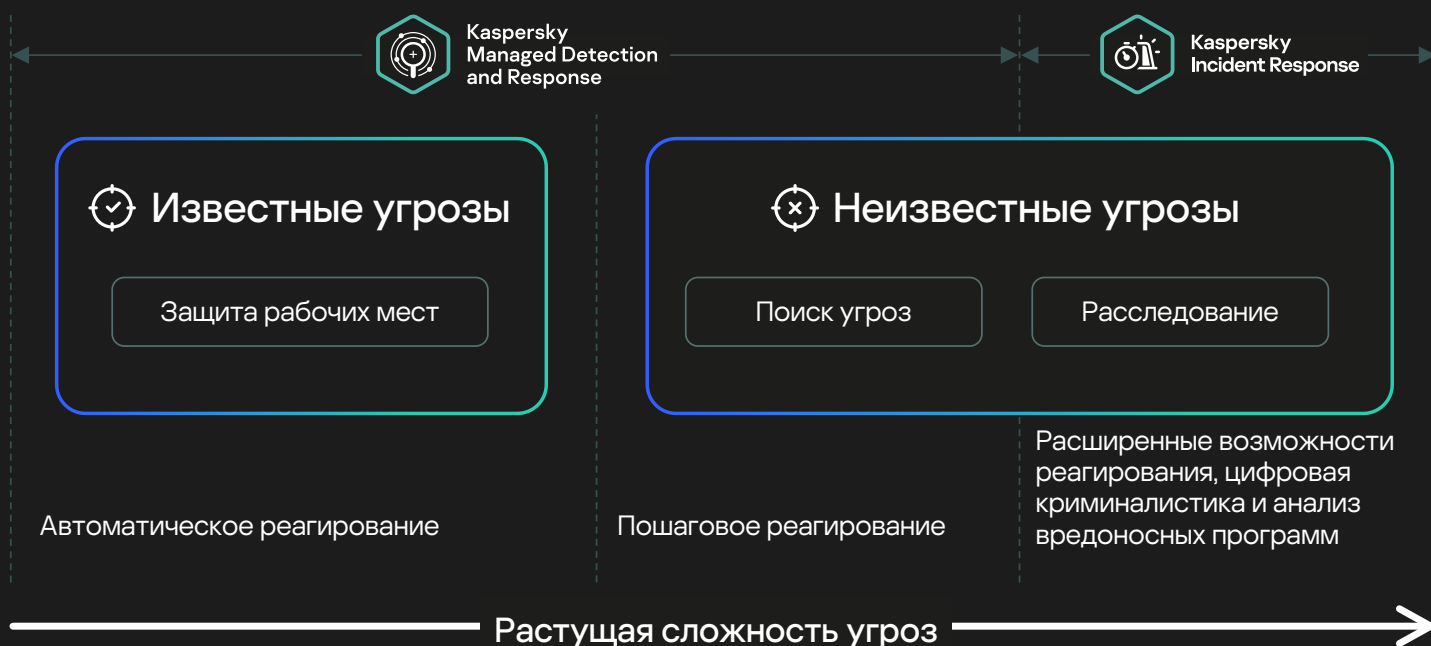


Kaspersky Incident Response

Kaspersky Incident Response позволяет получить полное представление об инциденте. Сервис включает полный цикл расследования инцидентов и реагирования на них – от раннего реагирования и сбора доказательств до идентификации дополнительных следов компрометации и подготовки плана по устранению последствий.

Kaspersky MDR и Kaspersky Incident Response **работают как единое целое**, благодаря нашим экспертам, которые круглосуточно следят за вашей IT-инфраструктурой и готовы незамедлительно отреагировать на атаку любой сложности.

Безупречное взаимодействие сервисов



Ключевые компоненты Kaspersky MDR



SOC «Лаборатории Касперского»

Международная команда экспертов с десятилетним опытом работы с организациями разного масштаба из всех секторов экономики.



Консоль управления

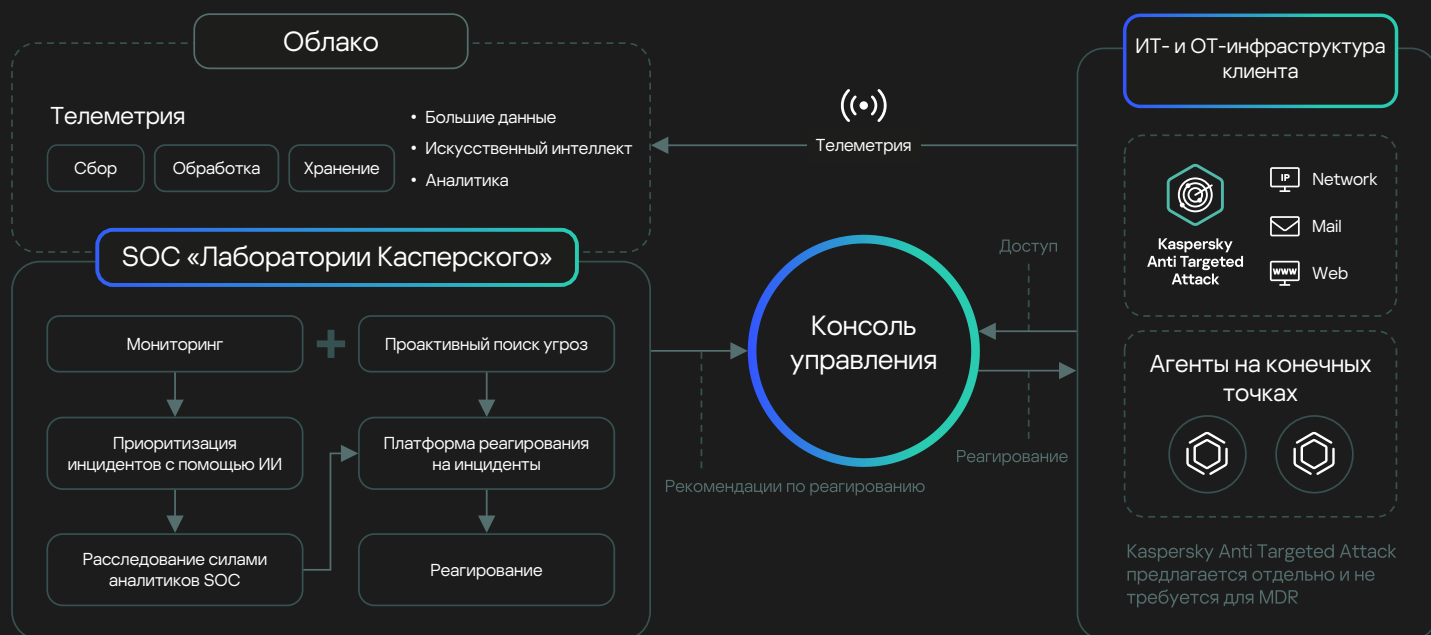
Интерфейс для работы с системой защиты сети организации, находящейся под управлением Kaspersky MDR.



Защита рабочих мест

Продукты «Лаборатории Касперского» для защиты рабочих мест и хранящихся на них данных от вредоносного ПО и других угроз.

Архитектура Kaspersky MDR



Принцип работы

1

Решения «Лаборатории Касперского», установленные на устройствах заказчика, собирают данные телеметрии и отправляют их экспертам SOC «Лаборатории Касперского».

2

Телеметрия анализируется с помощью инструментов машинного обучения при непосредственном участии наших экспертов.

3

Эксперты SOC анализируют события безопасности, уведомляют клиента о вредоносной активности, дают рекомендации по устранению угроз и инструкцию по пошаговому реагированию.

¹ Автоматическое реагирование начинается после того, как клиент одобрит его в консоли Kaspersky MDR (если клиент этого не сделает, консоль MDR запросит разрешение до начала автоматического реагирования)

Возможности Kaspersky MDR

Полная безопасность

Возможность

Описание



Круглосуточный мониторинг

Kaspersky MDR обеспечивает круглосуточный мониторинг ваших ИТ- и ОТ-сред, гарантируя своевременное выявление и устранение любых подозрительных действий, независимо от того, когда они происходят.



Проактивный поиск угроз

Команда SOC использует передовую аналитику об угрозах (Threat Intelligence), машинное обучение для проактивного поиска признаков компрометации и скрытых угроз в вашей инфраструктуре, которые могут быть пропущены автоматическими инструментами безопасности.



Автоматическое реагирование и другие сценарии реагирования на инциденты

После подтверждения угрозы Kaspersky MDR предоставляет инструкции для реагирования, а также может в удаленном режиме выполнять действия для устранения угрозы. Если требуется более глубокое расследование, по запросу клиента подключается команда Kaspersky Incident Response, которая проводит цифровую криминалистическую экспертизу и анализ вредоносного ПО (сервис приобретается отдельно).



Прямой доступ к аналитикам SOC «Лаборатории Касперского»

Клиенты MDR имеют возможность обращаться к аналитикам SOC «Лаборатории Касперского» за оперативной экспертной помощью по конкретным инцидентам безопасности. Аналитики могут предоставить дополнительную информацию, рекомендации и поддержку для эффективного реагирования на сложные угрозы. Если у заказчика есть подписка на Kaspersky Incident Response, то также включено углубленное расследование инцидентов и реагирование на них силами экспертов нашего международного отдела оперативного решения компьютерных инцидентов.



Возможность самостоятельно зарегистрировать инцидент

При подозрении на компрометацию среды, клиент может вручную сообщить об инциденте через консоль Kaspersky MDR. Эта функция особенно полезна в ситуациях, когда клиент замечает необычную активность, не приводящую к срабатыванию автоматических оповещений, или если он обладает инсайдерской информацией об угрозе.



Совместимость со сторонними приложениями для защиты рабочих мест

Конфигурация решения позволяет использовать Kaspersky Managed Detection and Response совместно со сторонними приложениями для защиты рабочих мест, уже установленными в компании.

Прозрачность происходящих событий и осведомленность

Возможность

Описание



Удобные панели мониторинга

Дашборды содержат сведения об активных инцидентах безопасности и их статусах, количестве защищаемых устройств, ответных мерах на инциденты и многое другое. Благодаря этому клиент может следить за ситуацией в режиме реального времени.



Обзор всех защищаемых активов

Решение наглядно отображает состояние всех активов в вашей сети, обеспечивая уверенность в том, что все рабочие места учтены и защищены.



Проверка работоспособности системы безопасности

Функция позволит выяснить, какие ресурсы защищены с помощью Kaspersky Managed Detection and Response, а какие не отправляли телеметрию в течение определенного периода времени.



Управление решением через REST API

Возможность скачивать данные из Kaspersky Managed Detection and Response, выполнять их дальнейший анализ и формировать на их основе отчеты для последующей интеграции с другими системами и специализированными приложениями. REST API использует протокол HTTP и набор методов запроса/ответа. Он позволяет управлять решением Kaspersky MDR не только через его собственную консоль, но и через стороннее решение.



Вариативность каналов для получения уведомлений из консоли MDR

Пользователи могут получать уведомления от Kaspersky Managed Detection and Response о зарегистрированных инцидентах и обновлении данных о них по электронной почте и/или в Telegram.

Регионы локации аналитиков SOC «Лаборатории Касперского»

- 1 Россия
- 2 Ближний Восток
- 3 Европа
- 4 Латинская Америка



Мы защищаем более 220 000 компаний почти в 200 странах и регионах



Поддерживаемые продукты «Лаборатории Касперского»

Сценарий активации Kaspersky MDR

Продукты «Лаборатории Касперского»

Преимущества

Существующие или новые пользователи решений «Лаборатории Касперского» для защиты рабочих мест

- Kaspersky Endpoint Security для Windows / Mac / Linux

Полнофункциональное обнаружение угроз и защита рабочих мест клиента.

Существующие или новые клиенты, использующие виртуальные инфраструктуры

- Kaspersky Security для виртуальных сред - Легкий агент для Windows / Linux

Полнофункциональный мониторинг угроз и защита виртуальных машин.

Существующие или новые пользователи Kaspersky Anti Targeted Attack (KATA)

- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Security для Windows / Mac / Linux

Kaspersky MDR получает данные о критических инцидентах, которые обнаружены системами IPS/IDS¹ или песочницей.

Kaspersky MDR позволяет пользователям KATA работать с продвинутыми APT-обнаружениями непосредственно через Kaspersky Anti Targeted Attack.

Существующие или новые пользователи Kaspersky Industrial Cybersecurity for Nodes

- Kaspersky Industrial Cybersecurity for Nodes

Круглосуточный мониторинг, поиск и обнаружение угроз в OT-среде

Новые клиенты, использующие сторонние продукты для защиты рабочих мест

- Kaspersky Endpoint Security для Windows в конфигурации агента EDR

Мониторинг и обнаружение инцидентов, но без полноценной антивирусной защиты.

В каждом сценарии могут использоваться дополнительные комбинации продуктов.

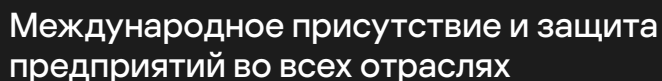
Kaspersky Endpoint Security для Windows в конфигурации агента EDR

Теперь Kaspersky Endpoint Security для Windows можно установить наряду со сторонними приложениями для защиты рабочих мест в режиме агента EDR – то есть для интеграции Kaspersky MDR в инфраструктуру клиента не требуется лицензия Kaspersky Security для бизнеса. В этом случае Kaspersky Endpoint Security выполняет функцию агента мониторинга и не обеспечивает защиту рабочих мест.

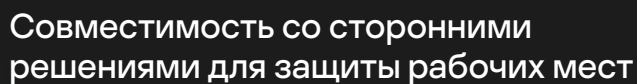
[Подробнее](#)



Подробнее



Подробнее



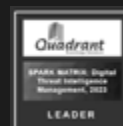
Подробнее



Международная команда экспертов

Прозрачность и практическая аналитика

Подробнее





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