

Kaspersky Managed Detection and Response

Преимущества сервиса по круглосуточной управляемой защите 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 по-настоящему важных задач.
- Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри компании.

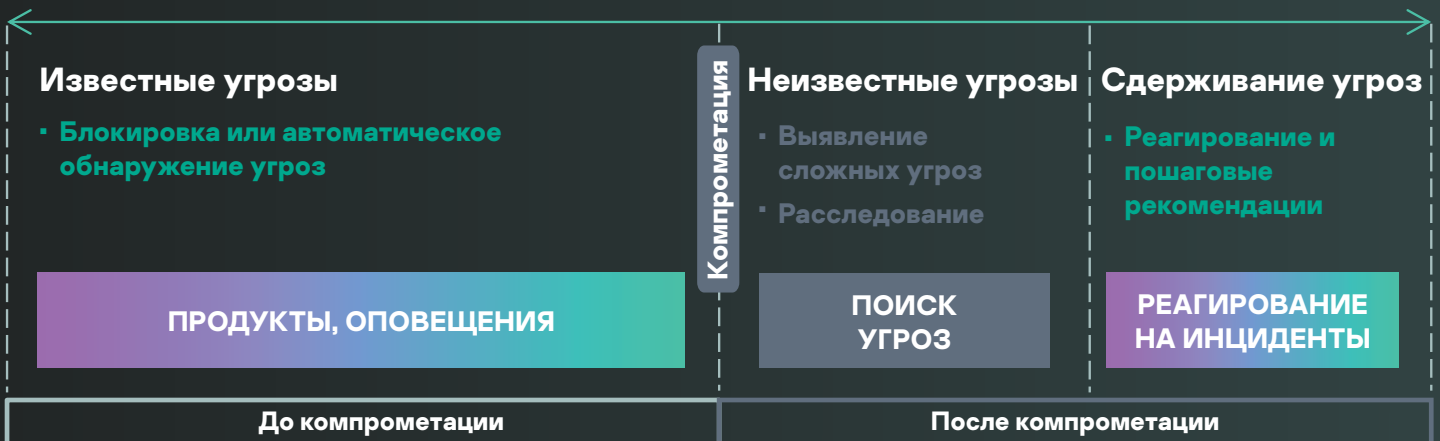
Управляемая защита вашего бизнеса

В связи с повсеместной широкомасштабной автоматизацией бизнес-процессов деятельность предприятий все сильнее зависит от информационных технологий. Это делает компании более уязвимыми для хакерских атак на корпоративные ИТ-системы. Организации могут вообще не иметь ИБ-специалистов или 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 ИБ-специалистов или которые испытывают нехватку знаний в вопросе реагирования на киберинциденты, так и более крупным компаниям, ИБ-эксперты которых перегружены.

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

KASPERSKY MANAGED DETECTION AND RESPONSE



Время

Как работает сервис

Поддерживаемые продукты и приложения:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- Kaspersky Security для Windows Server
- Kaspersky Security для виртуальных сред Легкий агент
- Kaspersky EDR для бизнеса Оптимальный
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

Kaspersky MDR проверяет оповещения и проактивно анализирует метаданные, получаемые от установленных в сети клиента продуктов «Лаборатории Касперского», на предмет наличия признаков компрометации. Эти метаданные сопоставляются с аналитическими данными «Лаборатории Касперского» об угрозах для выявления тактик, техник и процедур, применяемых преступниками против конкретной организации. При этом уникальные индикаторы атак позволяют обнаружить скрытые угрозы, не используя вредоносное ПО и имитирующие легитимную активность. Встроенные механизмы искусственного интеллекта (ИИ) в Kaspersky MDR помогают минимизировать число ложноположительных срабатываний и ускорить процесс приоритизации оповещений.



Знания и опыт экспертов международного уровня



Передовые технологии защиты



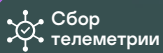
Проактивный мониторинг и поиск угроз



Автоматизированное и управляемое реагирование

ОБЛАКО

- Большие данные
- Искусственный интеллект
- Аналитика



Сбор телеметрии



Обработка телеметрии



Хранение телеметрии

Телеметрия

SOC «Лаборатории Касперского»



Мониторинг и автоматический поиск угроз

Приоритизация уведомлений с помощью ИИ

Расследование силами аналитика SOC

Реагирование на инциденты и рекомендации



Единая консоль

Доступ

Проактивный поиск угроз силами аналитика SOC

Платформа реагирования на инциденты

Осуществление ответных мер



Агенты на конечных точках



Корпоративная сеть клиента

Под защитой «Лаборатории Касперского»

Уровни Kaspersky MDR

Дополнительно к Kaspersky MDR «Лаборатория Касперского» предлагает:

- **ГИБКИЕ ВОЗМОЖНОСТИ** хранения данных для соответствия нормативным требованиям и поддержки цифровой криминалистики
- **СЕРВИС ПО РЕАГИРОВАНИЮ** на инциденты разной степени сложности
- **ОЦЕНКА КОМПРОМЕТАЦИИ** и проверка эффективности текущей защиты
- **ПРАКТИЧЕСКИЕ ТРЕНИНГИ** для ИБ-экспертов по реагированию на инциденты

Kaspersky MDR предусматривает два уровня защиты и подходит организациям с разными ИБ-потребностями. Kaspersky MDR Optimum мгновенно 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 точно на них реагировать. Kaspersky MDR Expert включает в себя все возможности Kaspersky MDR Optimum, а также предоставляет дополнительную гибкость для опытных ИБ-команд. Более крупные организации с развитой ИБ-экспертизой могут передать процессы классификации и расследования инцидентов в «Лабораторию Касперского» и направить свои ресурсы на решение более важных задач.

Автоматизированный активный поиск угроз в Kaspersky MDR Optimum использует автоматические срабатывания индикаторов атак для последующей проверки, расследования и обнаружения компрометации, в то время как Kaspersky MDR Expert дополнительно включает в себя проактивный поиск угроз силами экспертов «Лаборатории Касперского». Аналитики SOC «Лаборатории Касперского» используют все свои знания и опыт, чтобы обнаружить те инциденты, по которым не было автоматических срабатываний. Организации получают доступ к преимуществам SOC без расходов на его создание и развитие.



Optimum

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанных данных в течение 1 месяца

Expert

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года

ТОЛЬКО В EXPERT

- Хранение необработанных данных в течение 3 месяцев
- Проактивный поиск угроз (threat hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Доступ к порталу Kaspersky Threat Lookup
- API для загрузки данных



Доказанная
эффективность

GREAT GLOBAL RESEARCH
& ANALYSIS TEAM

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

MITRE | ATT&CK

Качество обнаружения угроз в Kaspersky MDR подтверждено оценкой MITRE ATT&CK в 2020 году (детекты MSSP).

Международное признание

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

FORRESTER

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



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 2021 году.



**Kaspersky
Managed
Detection and
Response**

Узнать больше

www.kaspersky.ru

© 2021 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.