kaspersky

Блокируем угрозы
до того, как они причинят
ущерб вашему бизнесу

Kaspersky Managed Detection and Response

Повысьте надежность своей системы кибербезопасности с помощью круглосуточной управляемой защиты

Kaspersky Managed Detection and Response – это экспертный сервис для круглосуточного мониторинга, обнаружения и расследования сложных кибератак и быстрого реагирования на них. Позволяет усилить существующие средства защиты благодаря функциям обнаружения угроз с участием экспертов и использованию глобальной аналитики угроз. Этот сервис позволяет повысить уровень безопасности OT- и IT-инфраструктуры – вне зависимости от размера вашей организации и сферы ее деятельности.

На организации любого масштаба постоянно оказывают давление такие факторы, как удаленная работа, быстро растущий объем обмена цифровыми данными, усиливающаяся нехватка квалифицированных кадров в мире, а также увеличение числа киберугроз, способных обходить традиционные автоматизированные средства контроля. В этих условиях крайне важно быстро и эффективно реагировать на все инциденты.

Обзор современных киберугроз[1]

1 Начальные векторы атак

31% действительные учетные записи

13% доверительные отношения

39% эксплуатация общедос-тупного приложения

2 Двигайтесь вперед и достигайте целей

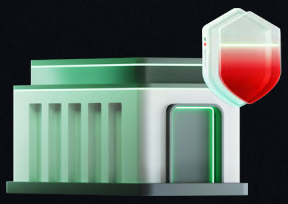
Злоумышленники часто используют легитимные инструменты (такие как Mimikatz, PsExec, SoftPerfect Network Scanner) в инфраструктурах, где отсутствует надлежащий контроль за конфигурацией системы.

3 Влияние

42% файлов шифруются

17% утечка данных

11% закрепление в системе для будущих атак



Факты свидетельствуют о том, что злоумышленники часто возвращаются после проведения успешной атаки.

Длительность атаки

Быстрая	В среднем	Длительные
45%	20%	35%
в пределах одного дня	13 дней	253 дня

Ключевые преимущества

Постоянная расширенная защита по всей поверхности атаки – на рабочих местах, в сети, облачных средах и других компонентах инфраструктуры – с первого дня использования.

Готовый круглосуточно работающий центр мониторинга и реагирования без затрат на создание и поддержку собственного SOC.

Снижение нагрузки на ваших ИБ-специалистов: функции мониторинга, первичной оценки и расследования угроз передаются нам.

Эффективность средств защиты: экспертиза наших специалистов, аналитика угроз и использование ИИ-технологий позволяют предотвращать инциденты до того, как они нанесут ущерб вашему бизнесу.

> Это сотрудничество вывело нас на совершенно новый уровень выстраивания внутренних ИБ-процессов
>
> **Максим Иванов,**
> начальник отдела ИТ, телефонной связи и телевидения службы связи ИТиТСБ «Государственного академического Большого театра России»

Большой театр

Подробнее

1 Отчет по Kaspersky MDR и реагированию на инциденты

Возможности Kaspersky MDR

Непрерывная защита от комплексных угроз сразу после внедрения

Kaspersky MDR активируется за несколько минут и не требует дополнительной инфраструктуры. Благодаря нашим специалистам из центра мониторинга и реагирования, а также аналитике угроз обеспечивается многоуровневое обнаружение угроз по всей инфраструктуре. Благодаря анализу множества сигналов телеметрии, сервис проактивно обнаруживает угрозы, выявляет первопричины инцидентов и обеспечивает оперативное реагирование на них, защищая организацию от известных угроз и угроз нулевого дня с первого дня работы.

Управление безопасностью под руководством экспертов с использованием данных аналитики

При использовании сервиса Kaspersky MDR безопасность вашей организации поддерживают международные эксперты с большим практическим опытом работы, имеющие престижные отраслевые сертификаты. Работа экспертов дополняется лучшими на рынке технологиями аналитики угроз и искусственного интеллекта – они встроены в сервис и позволяют повысить точность и контекстность оповещений, ускорить обнаружение угроз и сократить среднее время реагирования на инциденты (MTTR).

Эффективность работы и предсказуемость затрат

- Kaspersky MDR позволяет избежать сложностей и затрат, связанных с созданием собственного центра мониторинга и реагирования с нуля. Это помогает быстрее внедрять необходимые улучшения в области безопасности без значительного увеличения нагрузки на бюджет.
- Если у вас уже есть собственный центр мониторинга и реагирования, наш сервис возьмет на себя задачи по круглосуточному мониторингу, приоритизации оповещений и классификации инцидентов, чтобы ваши аналитики могли сосредоточиться на более важной стратегической работе.

Сценарии использования

- Круглосуточная защита «под ключ» для организаций, не имеющих службы ИБ
- Совместная модель управления ИБ, позволяющая расширить возможности собственных специалистов по кибербезопасности
- Расширенная защита промышленной инфраструктуры
- Непрерывная специализированная защита встраиваемых систем

30 минут
– среднее время реагирования на инцидент [2]

30%
всех полученных оповещений обрабатываются Автоматическим аналитиком на базе ИИ [1]

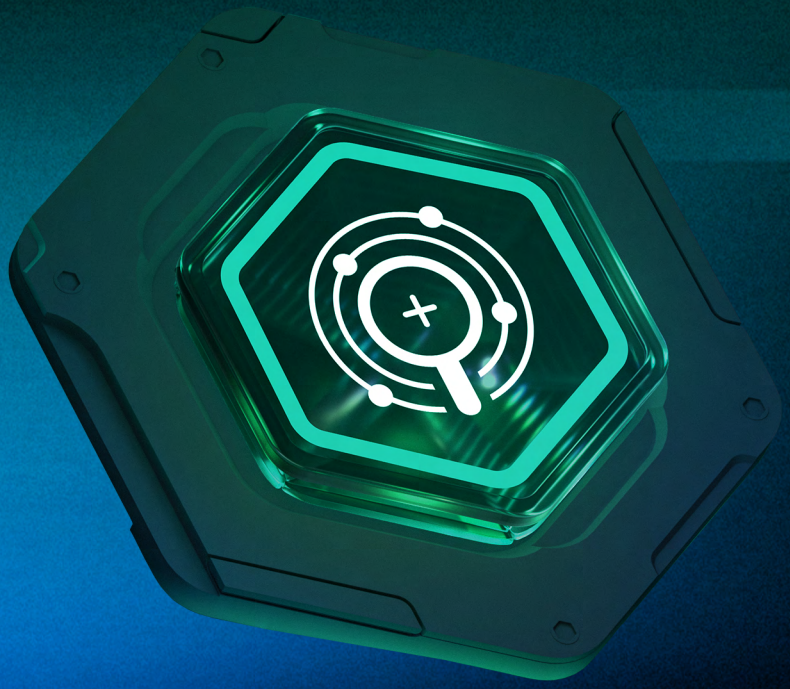
Не более 15 минут
– столько времени требуется на активацию сервиса Kaspersky MDR

До 2 лет
– столько времени требуется на создание собственной службы ИБ с нуля

70%
специалистов по ИБ с трудом справляются с тем количеством оповещений, которое генерируется их средствами защиты [3]

2 Согласно нашим ежегодным аналитическим отчетам MDR

3 Портрет современного специалиста по информационной безопасности на 2024 год



Kaspersky Managed Detection and Response

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее