kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Managed Detection and Response

Большинство служб IT-безопасности прежде всего заняты отслеживанием оповещений об инцидентах и реагируют, только когда инцидент уже произошел. При этом новые угрозы выпадают из поля зрения, и возникает ложное ощущение безопасности. Компании все больше осознают потребность в проактивном поиске угроз, пока никак не проявивших себя, но уже проникших в корпоративную инфраструктуру.

Преимущества сервиса:

- 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 ресурсы компании на решение по-настоящему важных задач.
- Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри компании.

Kaspersky Managed Detection and Response – это круглосуточная расширенная защита от растущего числа угроз, способных обойти автоматические системы безопасности. Она отлично подходит организациям, которым не хватает ресурсов и квалифицированных специалистов.

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

Основные возможности

- Быстрое масштабируемое развертывание, позволяет мгновенно активировать передовые функции защиты без необходимости нанимать и обучать сотрудников.
- Эффективная защита даже против самых сложных и изощренных угроз, не использующих вредоносное ПО, предотвращает простои и минимизирует ущерб от инцидентов.
- Управляемое или автоматизированное реагирование на инциденты дает возможность обеспечить своевременные ответные меры, позволяя при этом контролировать процесс от и до.
- Обзор всех защищаемых активов с их текущим статусом в реальном времени и получение актуальной информации по наиболее удобным каналам связи.

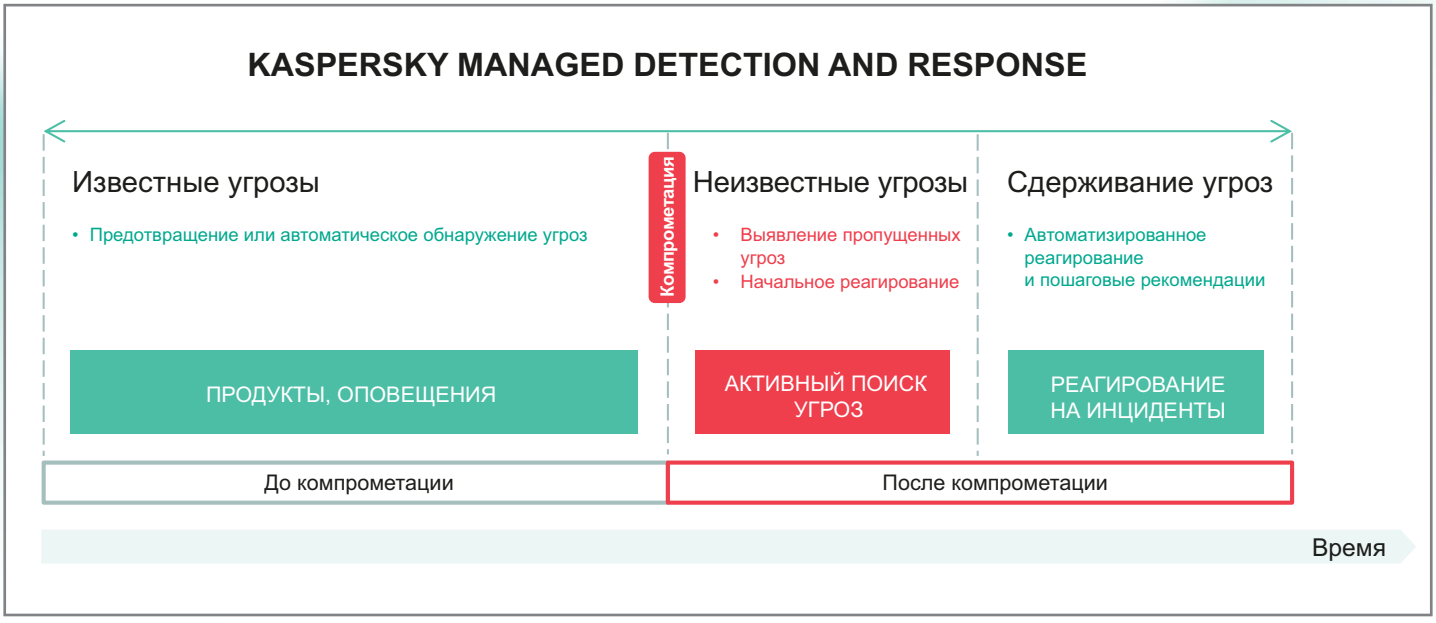

Рис. 1. Kaspersky Managed Detection and Response

Поддерживаемые продукты:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Security для Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Security для Mac[1]

Как работает сервис

Kaspersky Managed Detection and Response проверяет оповещения от установленных в сети клиента продуктов «Лаборатории Касперского», чтобы убедиться, что автоматическое предотвращение угроз работает эффективно, и проактивно анализирует получаемые от этих продуктов метаданные на предмет наличия признаков компрометации. Сбор этих метаданных осуществляет Kaspersky Security Network. Они автоматически в режиме реального времени сопоставляются с аналитическими данными «Лаборатории Касперского» об угрозах для выявления тактик, методов и процедур, используемых преступниками против конкретной организации. Собственные индикаторы атак позволяют обнаружить скрытые угрозы, не использующие вредоносное ПО и имитирующие легитимную активность. В первые 2–4 недели продукт адаптируется к вашей инфраструктуре. Это нужно для минимизации числа ложноположительных срабатываний при определении, какая активность легитимна, а какая – нет.

Kaspersky Managed Detection and Response предусматривает два уровня защиты и поэтому подходит организациям любых масштабов с разными уровнями ИБ-зрелости (рис. 2). Благодаря быстрому развертыванию Kaspersky Managed Detection and Response Optimum мгновенно повышает уровень информационной безопасности, позволяет не нанимать дополнительных сотрудников и не переобучать существующих. Kaspersky Managed Detection and Response Expert включает в себя все возможности уровня Optimum, а также предоставляет дополнительную гибкость для опытных ИБ-команд. Вы можете передать процессы классификации и расследования инцидентов в «Лабораторию Касперского» и направить ваши ресурсы на решение более важных задач.

Рис. 2. Уровни решения Kaspersky Managed Detection and Response

Автоматизированный активный поиск угроз в MDR Optimum использует автоматические срабатывания индикаторов атак для последующей проверки, расследования и обнаружения компрометации, в то время как MDR Expert включает в себя активный поиск угроз силами экспертов «Лаборатории Касперского». Эксперты компании используют все свои знания и опыт, чтобы обнаружить те инциденты, по которым не было автоматических срабатываний.

Для адаптации продукта к требованиям организации доступны дополнительные возможности:

- Гибкие функции хранения данных для соответствия нормативным требованиям и поддержки цифровой криминалистики
- Соглашение о реагировании на инциденты, обеспечивающее максимум поддержки со стороны «Лаборатории Касперского» в разрешении ваших инцидентов безопасности
- Проведение комплексной оценки на предмет наличия существующих признаков компрометации для уверенности в том, что существующая защита эффективна
- Практические тренинги для аналитиков SOC для повышения общей готовности к инцидентам

Противодействие целевым атакам требует большого опыта и постоянного обучения. Около десяти лет назад «Лаборатория Касперского» стала одной из первых в отрасли компаний, организовавшей специализированный центр для расследования сложных угроз, и обнаружила множество кибератак глобального масштаба. За счет этого уникального опыта Kaspersky Managed Detection and Response позволяет извлечь максимум из используемых вами защитных решений «Лаборатории Касперского», предоставляя индивидуально настраиваемый сервис обнаружения, приоритизации, расследования и реагирования на инциденты информационной безопасности. Вы получаете доступ к преимуществам SOC без необходимости строить его внутри компании.

[1] Планируется во 2 кв. 2021 г.
[2] Планируется в 1 кв. 2021 г.
[3] Планируется в 2021 г.
[4] Планируется в 1 кв. 2021 г.

www.kaspersky.ru