



Kaspersky Symphony XDR

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

Факты о XDR

Что такое XDR

Это современная моновендорная концепция, которая представляет собой кросс-продуктовое взаимодействие с дополнительными функциональными возможностями.

EDR важен

Решение класса EDR – это ключевой элемент XDR. Без сильного EDR в синергии с EPP не может быть сильного XDR.

XDR не равно EDR

XDR основан на расширении технологии EDR и контроля потенциальных точек входа злоумышленника за пределами рабочих мест и серверов.

XDR и SIEM

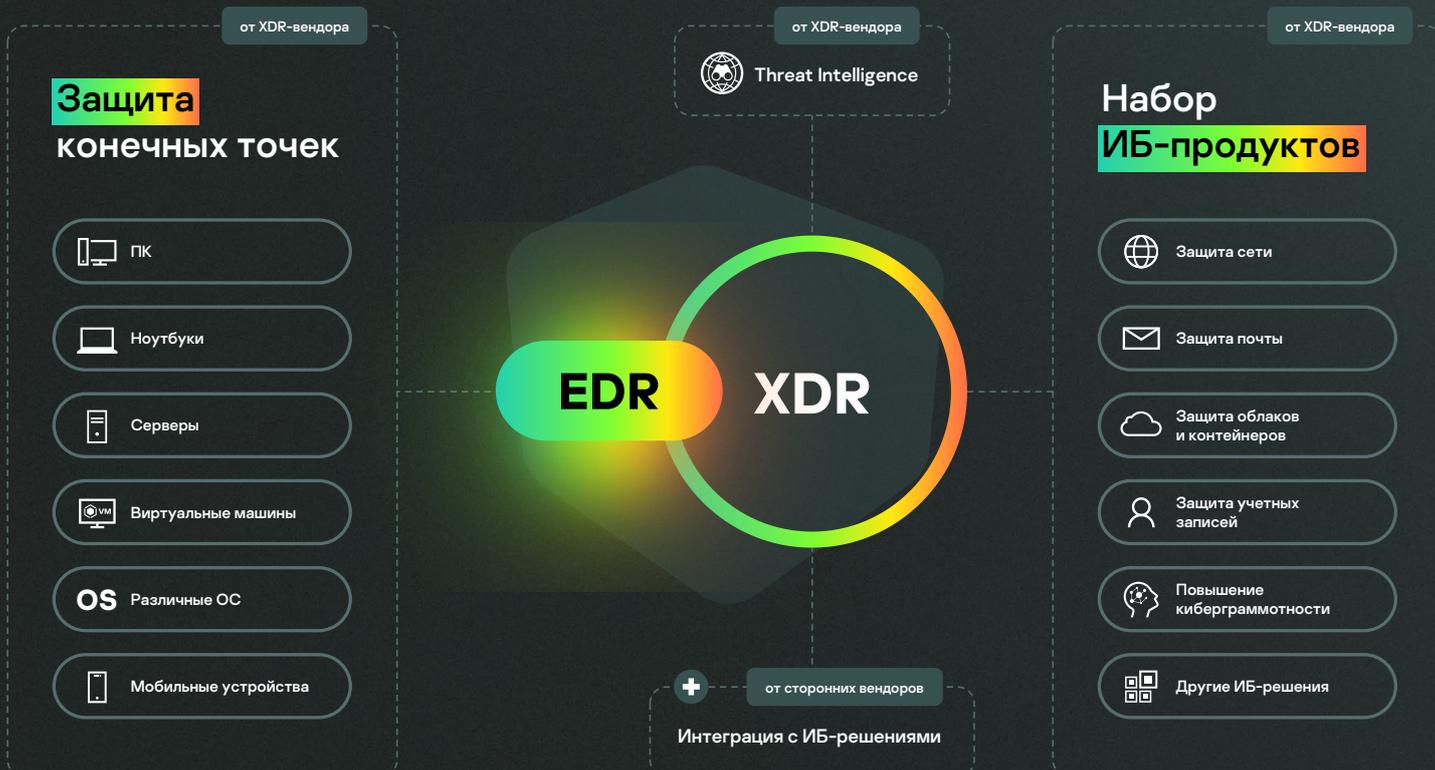
Эти классы решения не являются взаимоисключающими. Напротив – они могут объединяться в гибридную концепцию XDR, чтобы обеспечивать интеграцию с ИБ-решениями сторонних поставщиков.

О концепции XDR – Extended Detection and Response

XDR – это концепция в ИБ, которая обеспечивает расширенное обнаружение кибератак и реагирование на них. XDR – это следующий шаг в развитии технологии EDR. XDR объединяет EDR с другими ИБ-инструментами и источниками данных с целью предоставить аналитиками расширенные возможности по обнаружению, расследованию и реагированию на сложные киберинциденты.



Ценность XDR определяется удобством эксплуатации, повышением уровня автоматизации и эффективностью процесса работы с инцидентами. XDR предоставляет экспертам полный обзор происходящего в инфраструктуре и лучшее понимание угроз, возможности глубокого анализа первопричин и централизованного реагирования на инциденты.





Всесторонняя защита

Kaspersky Symphony — это целая линейка решений, которая воплощает собой системный подход к защите бизнеса: от безопасности рабочих мест всех платформ — к всеобъемлющей защите всей инфраструктуры с соблюдением регуляторных требований.

О Kaspersky Symphony XDR

Kaspersky Symphony XDR – самое продвинутое решение линейки Kaspersky Symphony.

Kaspersky
Symphony Security

Kaspersky
Symphony EDR

Kaspersky
Symphony XDR

Решение объединяет в рамках одной лицензии технологии EPP и EDR, почтовый и интернет-шлюзы, песочницу, инструменты анализа сетевого трафика, платформу повышения осведомлённости сотрудников, аналитические данные о киберугрозах, систему мониторинга и корреляции событий безопасности и модуль взаимодействия с ГосСОПКА.

Kaspersky Symphony XDR — это всё что сегодня нужно ИБ-экспертам, чтобы успешно отражать сложные кибератаки.

Продуктовый состав Kaspersky Symphony XDR

Защита конечных точек

Kaspersky Symphony EDR



Kaspersky
Endpoint Detection
and Response



Kaspersky Symphony Security



Kaspersky
Endpoint Security
для бизнеса
Расширенный



Kaspersky
Security для виртуальных
и облачных сред

Kaspersky Symphony XDR

Threat Intelligence



Kaspersky
Threat Lookup



Kaspersky
Threat Data
Feeds



Kaspersky
CyberTrace

Набор ИБ-продуктов



Kaspersky
Anti Targeted
Attack



Kaspersky
Security для
почтовых серверов



Kaspersky
Security для
интернет-шлюзов



Kaspersky
Automated Security
Awareness Platform



Kaspersky
Unified Monitoring
and Analysis Platform



Интеграция с ИБ-решениями
сторонних поставщиков



Оркестр
ИБ-технологий.
Под вашим
управлением.

Все экспертные инструменты — в едином решении

С Kaspersky Symphony XDR специалисты по IT-безопасности получают **в едином решении все инструменты**, которые позволят выявлять кибератаки на всех этапах их развития, проводить анализ первопричин и проактивный поиск угроз, а также оперативно и централизованно реагировать на сложные инциденты. Это поможет значительно сократить количество времени и сил, которые сотрудники службы ИБ обычно тратят на защиту от угроз повышенной сложности.



XDR позволяет

Упростить управление
инфраструктурой
информационной безопасности

Повысить операционную
эффективность ИБ-системы

Максимально автоматизировать
и упростить процесс реагирования
на инциденты

Оптимизировать ИБ-ресурсы

Сценарии взаимодействия элементов



Автоматические

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении их песочницей в сетевом и почтовом трафике

Потоковое обогащение событий, предварительно обработанных в Kaspersky CyberTrace, в Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Передача в KUMA событий, релевантных сложным атакам, с хостов, шлюзов и KATA для корреляции с данными от сторонних источников

Автоматическая блокировка на уровне почтового шлюза, до доставки получателю, неизвестных вредоносных объектов, обнаруженных детектирующими механизмами платформы Kaspersky Anti Targeted Attack (KATA)

Автоматическая блокировка на уровне веб-шлюза по результатам детектирования в KATA

Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя*

Передача сырой телеметрии с EDR в KUMA

Реагирование через EPP и EDR на найденные угрозы в KUMA

Автоматическое реагирование на найденные угрозы в KUMA средствами сторонних решений через запуск различных сценариев (поддержка API)



Полуавтоматические

Построение модели активов в KUMA на основании данных из Kaspersky Security Center (KSC)

Доступ в поисковую систему Kaspersky Threat Lookup для получения дополнительного контекста при проведении расследований

Передача информации о произошедших инцидентах в НКЦКИ с помощью встроенного в решение модуля ГосСОПКА

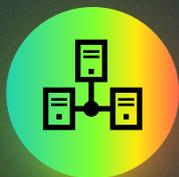
Принудительный запуск обновления баз и антивирусной проверки через KSC из карточки инцидента в KUMA

Запуск действий по реагированию через EDR из карточки инцидента в KUMA*

Возможность назначить обучение основам киберграмотности из карточки инцидента в KUMA*

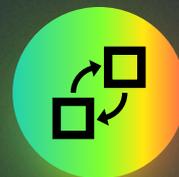
* В ближайшей дорожной карте

Сильные стороны Kaspersky Symphony XDR



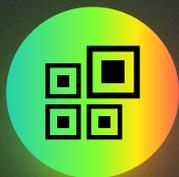
Общепризнанная защита конечных точек

Протестированное MITRE решение класса EDR в синергии с EPP, которое защищает более 60 млн корпоративных рабочих мест по всему миру



Взаимодействие элементов системы ИБ

Тесная интеграция включенных элементов с поддержкой различных кросс-продуктовых сценариев. Возможность взаимодействия с решениями сторонних поставщиков



Гибкость сетевой защиты

Защита электронной почты и доступа в интернет, анализ сетевого трафика и Netflow, песочница, а также возможность загрузки фидов с данными об угрозах в сторонние сетевые инструменты



Повышение уровня киберграмотности

Онлайн-тренинги, повышающие уровень киберграмотности сотрудников, что снижает число успешных атак, связанных с человеческим фактором (например, использующих социальную инженерию)



Обогащение аналитическими данными

Признанная лучшей в мире аналитика об угрозах (по результатам исследования Forrester Wave: External Threat Intelligence Services в 2021 г.)



Соответствие требованиям регуляторов

Соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА



Факторы успеха при выборе XDR

Почему Kaspersky Symphony XDR?

Преимущества для бизнеса:

Уменьшение ущерба от целевых атак и других сложных угроз

Поддержка непрерывности бизнеса благодаря продвинутым инструментам реагирования

Соответствие требованиям законодательства, в том числе ФЗ-187 и приказу ФСТЭК России №239

Сокращение рутинных операций для высвобождения ресурсов ИБ-специалистов

Повышение продуктивности службы ИБ благодаря использованию аналитических данных и тесной интеграции компонентов

Единый системный подход, который снижает издержки и уменьшает вероятность обхода системы защиты



Опыт и знания экспертов

Решение включает ряд запатентованных технологий и разработано на основе аналитических данных об APT-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского» (GReAT)



Технологии, получившие признание

Входящие в решение продукты и сервисы являются обладателями различных наград, их эффективность доказана независимыми тестовыми лабораториями, они получили признание со стороны ведущих аналитических агентств и клиентов



Эффективное обнаружение

Решение отличается высоким уровнем обнаружения угроз и отсутствием ложноположительных срабатываний, что подтверждается независимыми тестовыми лабораториями ICSA labs, AV test и SE labs



Гибкие варианты установки

Возможность полностью локальной установки – без взаимодействия с облачными сервисами и с полным соблюдением нормативных требований, в том числе в области конфиденциальности



Комплексное решение

Единое предложение для защиты всей инфраструктуры с технологиями EPP, EDR, Sandbox, Threat Intelligence Platform и другими, объединенное с собственной SIEM-системой, которая позволяет решению быстро встраиваться в существующую ИБ-систему



Понятные перспективы развития

Четкие планы развития решения: поддержка облачной поставки, усиление возможностей большим количеством кросс-продуктовых сценариев, а также планируемое включение в экосистему прорывной технологии SASE, благодаря приобретению компании Brain4net

Международное признание

Независимые тесты:

MITRE | ATT&CK®



Качество обнаружения киберугроз решениями «Лаборатории Касперского» подтверждено оценками MITRE ATT&CK, SE Labs, AV test и другими независимыми тестовыми лабораториями



FORRESTER® | IDC

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Эффективность технологий и экспертных знаний «Лаборатории Касперского» подтверждена ведущими аналитическими агентствами (Gartner, Forrester, IDC, Radicati Group и другими)

Решение обеспечит передовую защиту бизнеса от самых сложных кибератак, повысит эффективность работы вашей команды ИБ и поможет соответствовать требованиям регуляторов.



Kaspersky
Symphony XDR

Подробнее

www.kaspersky.ru

© 2023 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.