



Kaspersky Symphony XDR

kaspersky активируй будущее

Факты о XDR

EDR важен

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

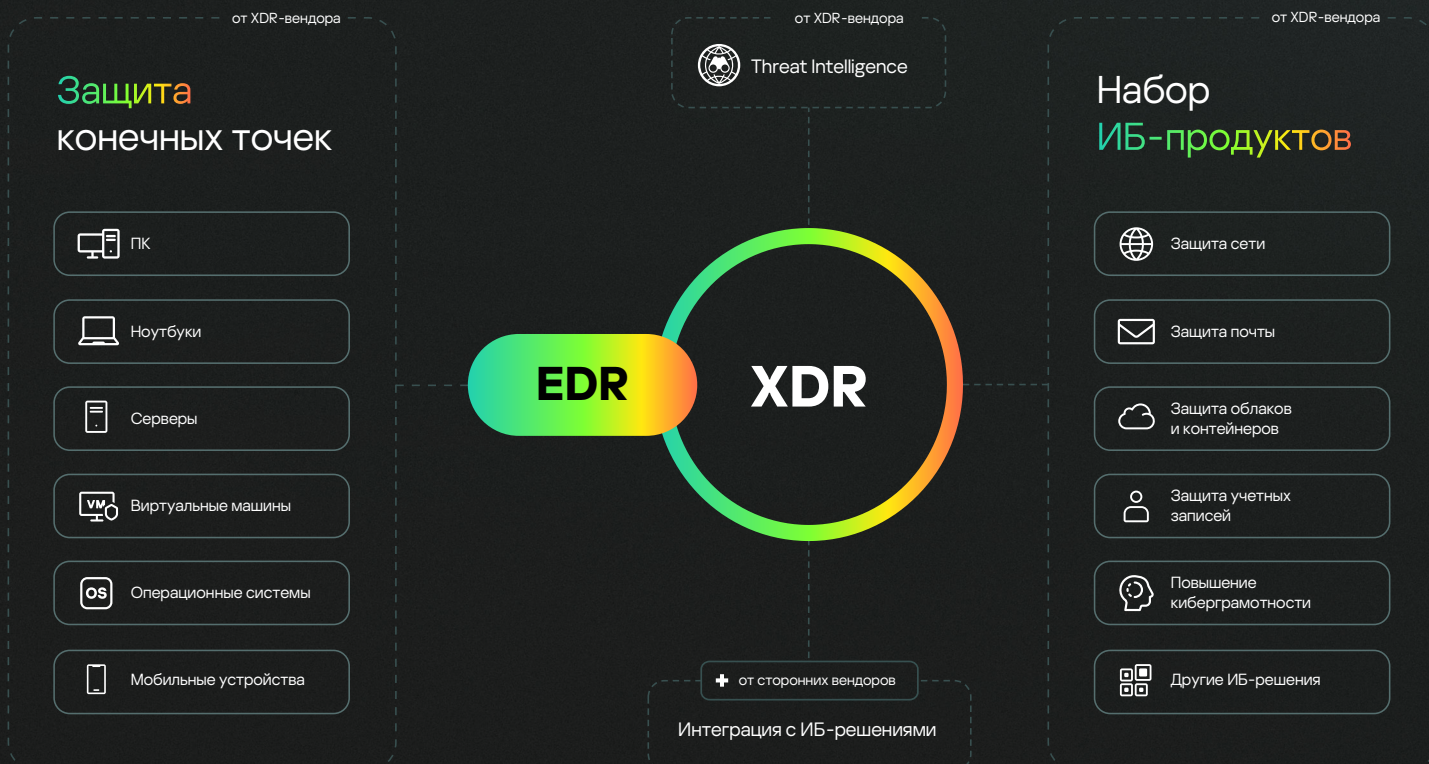
Эти классы решения не являются взаимоисключающими. В зависимости от выбранного пути разработки конкретного вендора SIEM может стать важной частью гибридной концепции XDR, чтобы, в том числе, обеспечивать расширенную интеграцию с ИБ-решениями сторонних поставщиков.

О концепции XDR — Extended Detection and Response

XDR — это концепция в ИБ, которая направлена на проактивное выявление угроз на разных уровнях инфраструктуры, реагирования на них и противодействия сложным кибератакам. XDR объединяет EDR с другими ИБ-инструментами максимально от одного производителя и иные комплементарные источники данных и защитные ИБ-средства с целью предоставить аналитикам единую точку принятия решения с удобным интерфейсом и расширенные возможности в работе со сложными киберинцидентами.



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.





О Kaspersky Symphony XDR

Kaspersky Symphony XDR — самое продвинутое решение линейки Kaspersky Symphony по выстраиванию собственной защиты в рамках всей инфраструктуры организации.

Всесторонняя защита

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

Kaspersky Symphony Security

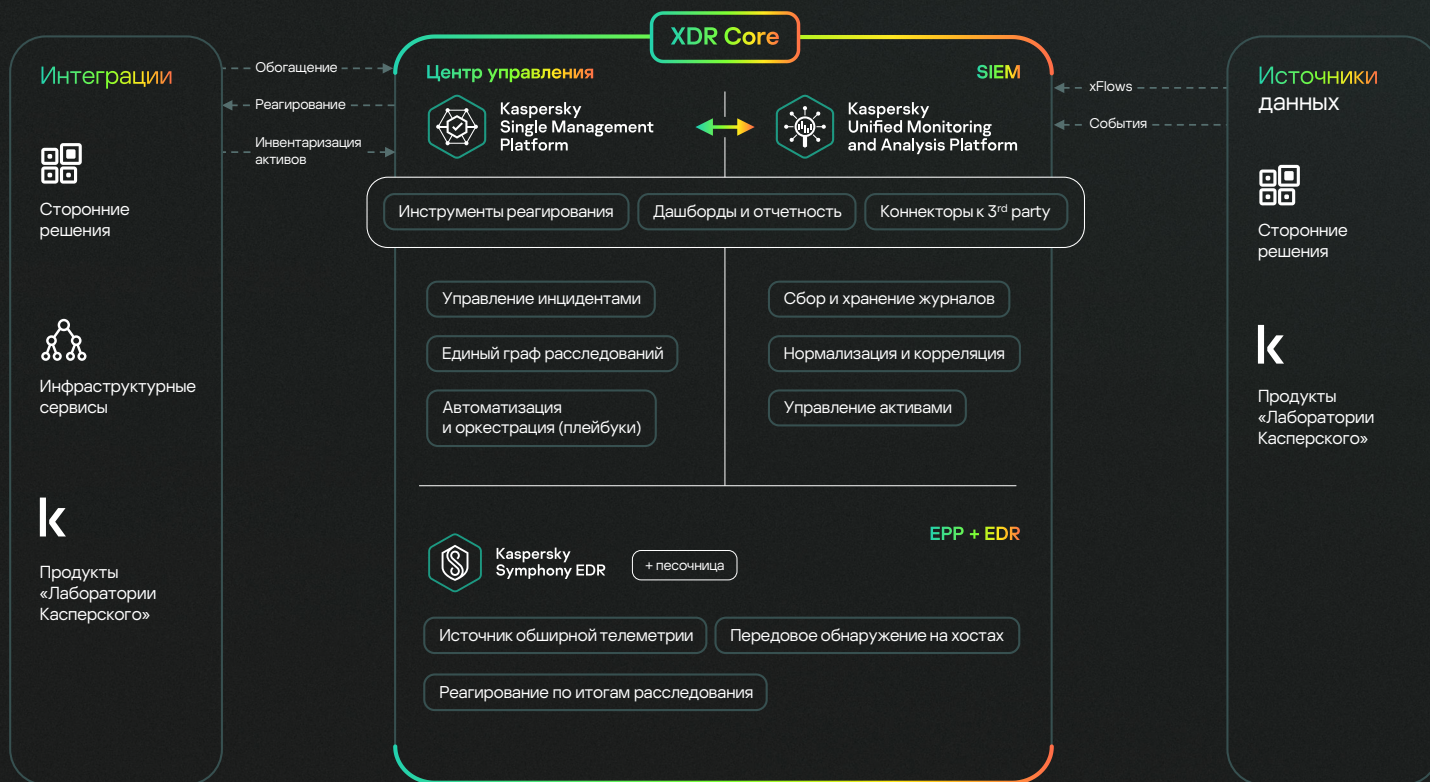
Kaspersky Symphony EDR



Kaspersky Symphony XDR

Kaspersky Symphony XDR, в том числе отдельно лицензируемое ядро решения Kaspersky Symphony XDR Core, позволяет централизованно управлять всей ИБ-системой и защищать многочисленные точки входа потенциальной угрозы. Kaspersky Symphony XDR Core включает в себя ключевой набор продуктов и идеально подходит организациям, для которых важна гибкость в построении мощной XDR-защиты: как на базе всех продуктов от Kaspersky, так и сторонних решений. Благодаря платформе управления Kaspersky Single Management Platform решение обеспечивает унифицированный интерфейс представления информации, единый граф расследования, оркестрацию и управление инцидентами.

Архитектура решения





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 помогает значительно сократить количество времени и сил, которые сотрудники службы ИБ обычно тратят на защиту от угроз повышенной сложности.

Kaspersky Symphony XDR

Kaspersky Symphony XDR Core

Kaspersky
Single Management
Platform

Kaspersky
Unified Monitoring
and Analysis Platform

Kaspersky
Symphony EDR + песочница

Интеграции
с ИБ-решениями



Сторонние
решения



Решения
Kaspersky

Включенная **защита**
на уровне **сети**



Kaspersky
Anti Targeted
Attack



Kaspersky
Security для
почтовых серверов



Kaspersky
Security для
интернет-шлюзов

Включенная
платформа
киберграмотности



Kaspersky
Automated Security
Awareness Platform

Включенное потоковое
обогащение



Kaspersky
Threat Data
Feeds

- Malicious URL
- Malicious Hashes
- Phishing URL
- Botnet C&C URL
- IP Reputation
- Ransomware URL



Kaspersky
CyberTrace

Включенный
поисковый портал
о киберугрозах
и взаимосвязях



Kaspersky
Threat Lookup

Упростить управление
инфраструктурой
информационной безопасности

Оптимизировать ИБ-ресурсы

Kaspersky
Symphony XDR
позволяет

Максимально автоматизировать
и упростить процесс
реагирования на инциденты

Повысить операционную
эффективность ИБ-системы

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

Тесная интеграция включенных элементов с поддержкой различных кросс-продуктовых сценариев. Взаимодействие с решениями сторонних поставщиков и единая платформа управления



Гибкость сетевой защиты

Защита электронной почты и доступа в интернет, анализ сетевого трафика и Netflow, а также эмуляция угроз с помощью передовой песочницы



Осведомленность об угрозах

Онлайн-тренинги, повышающие уровень киберграмотности сотрудников, что снижает число успешных атак, связанных с человеческим фактором



Обогащение данных аналитикой

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



Соответствие требованиям

Помощь в соответствии требованиям регуляторов, в том числе благодаря встроенному модулю ГосСОПКА

Факторы
успеха при
выборе XDR

Преимущества для бизнеса:

Уменьшение ущерба от целевых атак и других сложных угроз

Поддержка непрерывности бизнеса благодаря продвинутым инструментам реагирования

Соответствие требованиям законодательства в области информационной безопасности

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

Почему Kaspersky Symphony XDR?

1

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)

2

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

3

Эффективное обнаружение

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

4

Гибкие варианты установки

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

5

Комплексное решение

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

6

Понятные перспективы развития

Четкие планы развития решения: усиление возможностей большим количеством кросс-продуктовых сценариев, а также планируемое включение в экосистему прорывной технологии SASE

Международное признание

Независимые тесты:

MITRE | ATT&CK®



AVTEST

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

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее