Kaspersky Symphony

Обзор новой линейки решений

kaspersky 25 лет

Краткий план презентации

1. Проблематика
2. Экосистемный подход к защите
3. Концепция новой линейки решений
4. XDR и Kaspersky Symphony XDR

Проблематика

Современные реалии ИБ

Беспрецедентный рост ландшафта киберугроз, включая целевую киберагрессию

Кардинальное изменение IT-инфраструктуры, которая требует защиты

Интенсивное усиление требований регуляторов, особенно в отношении обеспечения защиты КИИ

Усиливается глобальный дефицит ИБ-экспертов на рынке труда

Процесс обеспечения защиты и работы с инцидентами становится более сложным и ресурсозатратным

Увеличиваются вероятность и стоимость реализации киберинцидента

~$1 млн*

*Источник: IT security economics in 2021, Kaspersky

Тренд на экосистемность

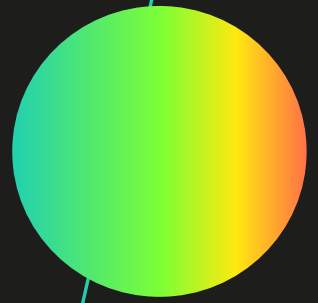
Единый партнер по кибербезопасности

Видит полную картину происходящего, снижает издержки и дает уверенность в завтрашнем дне.

kaspersky

Экосистемный подход к защите

Стратегические цели



Обеспечить защиту клиентов от максимального количества возможных векторов атак

Создать целостную экосистему безопасности для всех заказчиков

Как достичь цель?

Создать целостную экосистему для блокировки, выявления и реагирования всех видов атак

Полнота экосистемы

Покрыть все сценарии защиты для всех типов защищаемых объектов в сети предприятия

Открытость платформы

Обеспечить открытость и расширяемость платформы, поддержку автоматизации и дополнить технологиями

Интеграция с Zero trust

Выйти за рамки конечных точек для реализации подхода Zero trust в рамках XDR платформы

Как развивается и расширяется наша экосистема

- Kaspersky Security Network
- Поисковые роботы
- Мониторинг ботнет-угроз
- Ловушки для спама
- Сенсоры
- Партнеры
- Открытые источники (OSINT)

GREAT

Kaspersky APT Research team

Kaspersky SOC

Kaspersky Red Team

Kaspersky ICS CERT

Наша экспертиза

380 000

уникальных вредоносных объектов
мы обнаруживаем ежедневно*

*Kaspersky, 2021

1 млрд+

Общее число образцов в нашей вирусной коллекции

200+ APT-групп

Выявила и исследовала «Лаборатория Касперского»

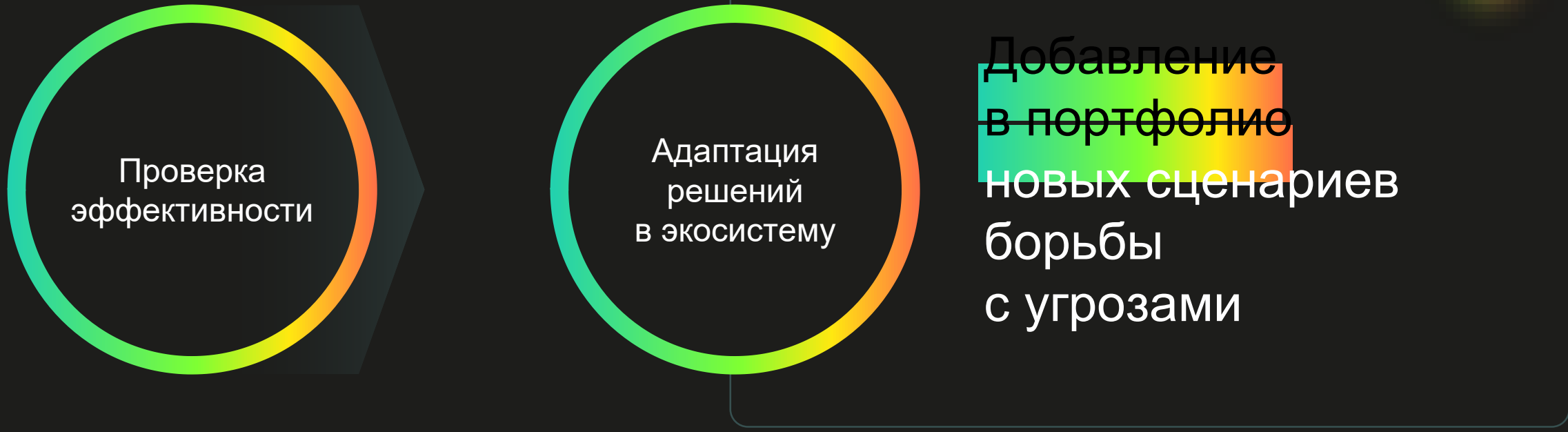
120+ отчётов

Об APT-атаках было выпущено за 2021 год

300+ инцидентов

Расследовали наши эксперты в 2021 году

Как развивается и расширяется наша экосистема



Наш путь к экосистеме ИБ и XDR в составе

Решение уже попало в несуществующий тогда класс решений XDR

2016

Выпуск платформы KATA с компонентом Endpoint sensor

Kaspersky Anti Targeted Attack

Первые вендоры заговорили о концепции XDR

2018

Трансформация Endpoint Sensor в платформе KATA в решение класса EDR

Kaspersky Endpoint Detection and Response

2019

EDR успешно протестирован MITRE

Старт разработки собственного SIEM

MITRE

Аналитики признали концепцию XDR

2020

Коммерческий релиз SIEM KUMA

Старт разработки SMP

Kaspersky Unified Monitoring and Analysis Platform

Q2 2021

Публичный анонс SMP

Лидеры TI по оценке Forrester

Kaspersky Single Management Platform

Q4 2021

Покупка Brain4Net

Анонс Kaspersky Symphony

new

Kaspersky Symphony

Аналитики признали концепцию XDR

2020

Коммерческий релиз SIEM KUMA

Старт разработки SMP

Kaspersky Unified Monitoring and Analysis Platform

Q2 2021

Публичный анонс SMP

Лидеры TI по оценке Forrester

Kaspersky Single Management Platform

Q4 2021

Покупка Brain4Net

Анонс Kaspersky Symphony

new

Kaspersky Symphony

Brain4net

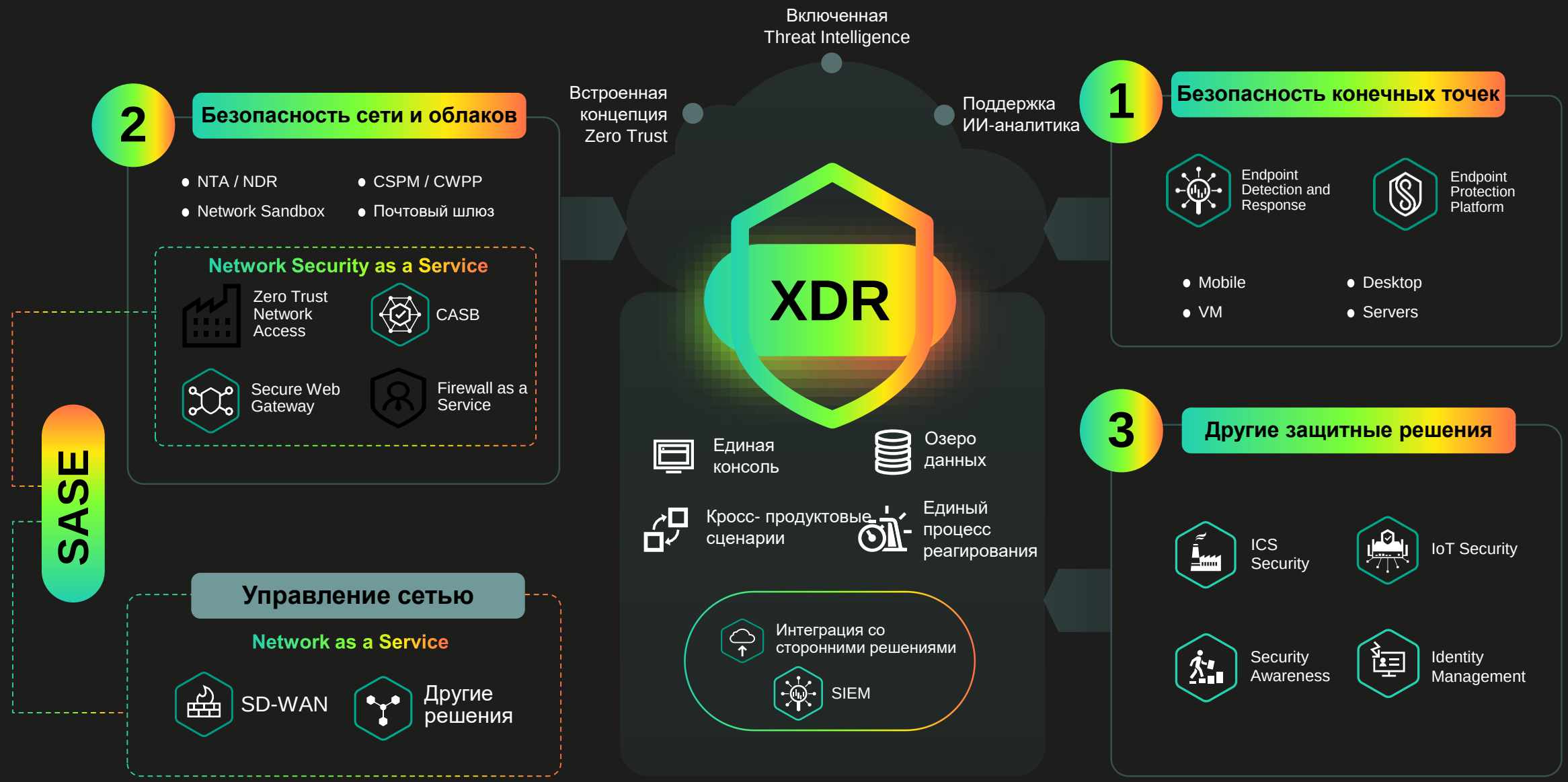
«Лаборатория Касперского» приобрела компанию Brain4Net

Brain4Net - это разработчик решений и сервисов, с помощью которых крупные предприятия и операторы связи адаптируют современные технологии, такие как SD-WAN (Software-Defined Wide-Area Network) и NFV (Network Functions Virtualization), под свою инфраструктуру.

Наши дальнейшие планы

Полнота экосистемы: собственные продукты, M&As или интеграции

Интегрированная концепций XDR + SASE + ZTNA



Концепция новой линейки Kaspersky Symphony

Почему Symphony?

Кибербезопасность в виртуозном исполнении:

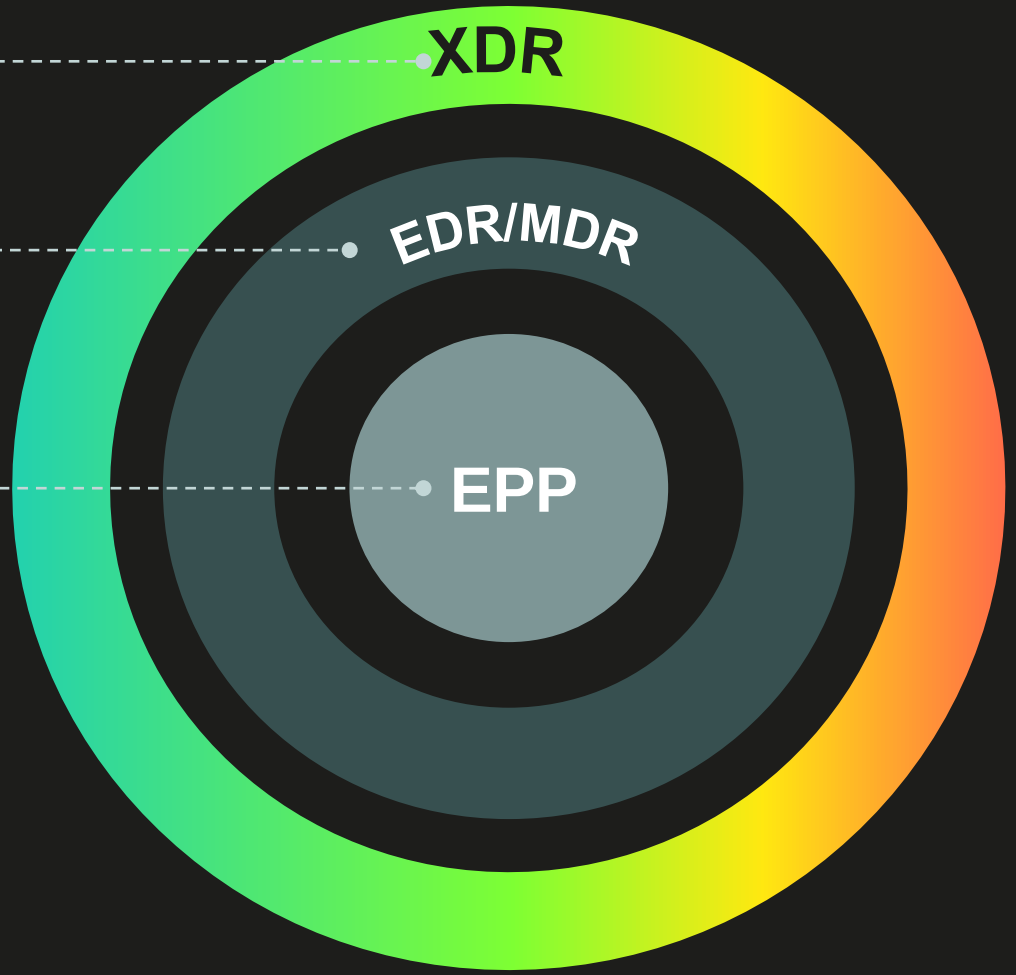
- Когда все инструменты идеально настроены.
- Когда все защитные решения действуют, как слаженный оркестр.
- Когда у вас есть всё, чтобы уверенно и просто дирижировать системой безопасности.

Kaspersky Symphony. Уровни защиты

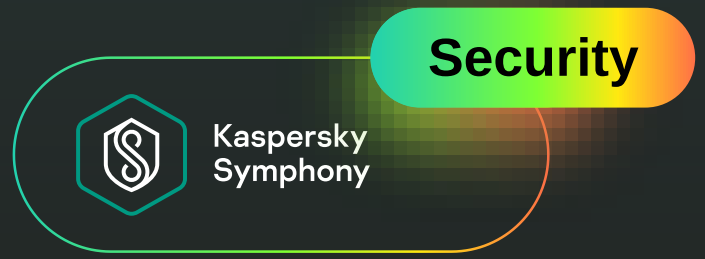
Kaspersky Symphony
XDR

Kaspersky Symphony
EDR / MDR

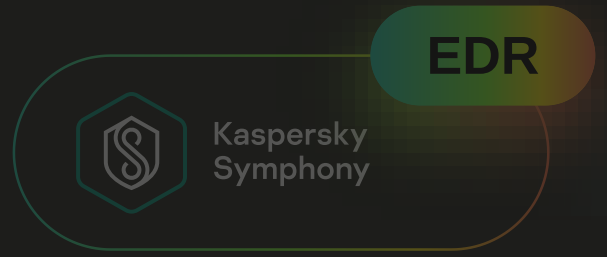
Kaspersky Symphony
Security

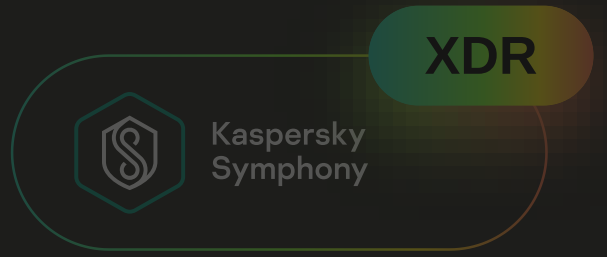


Основа безопасности

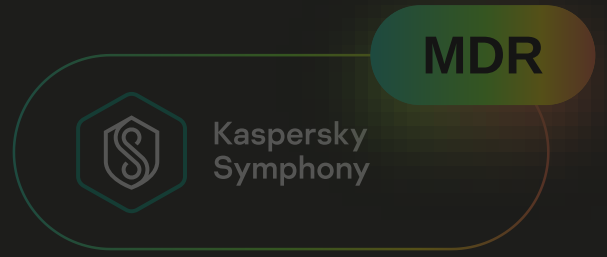


Расширение собственной защиты

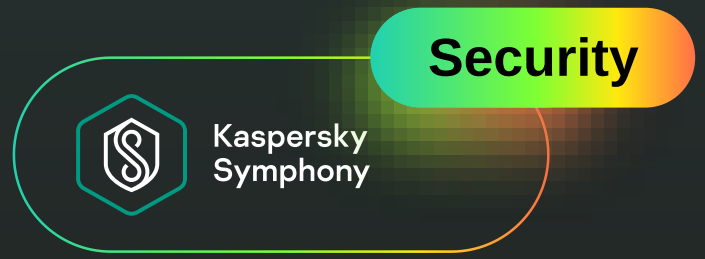




Выбор управляемой защиты

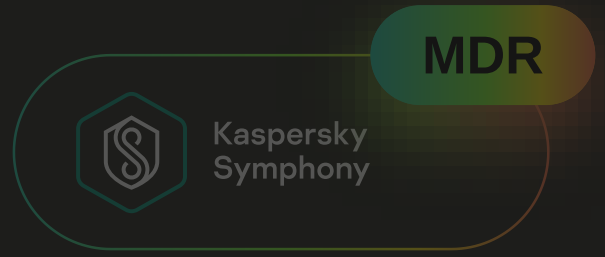


Основа безопасности

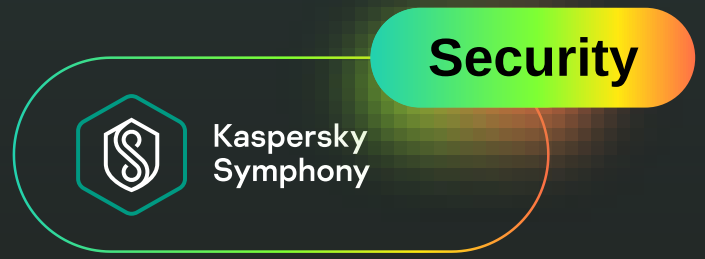


Расширение собственной защиты

Выбор управляемой защиты



Основа безопасности



Расширение собственной защиты

Выбор управляемой защиты

Функциональное сравнение уровней Kaspersky Symphony

Kaspersky Symphony	Security	EDR	MDR	XDR
Уровень защиты	Базовая собственная защита	Передовая собственная защита	Передовая управляемая защита	Расширенная собственная защита
Автоматическая защита конечных точек (физических, мобильных и виртуальных) от массовых угроз				
Передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них				
Защита электронной почты и анализ сетевого трафика				
Комплексный мониторинг и корреляция событий ИБ (+модуль ГосСОПКА)				
Управление аналитическими данными о киберугрозах				
Повышение киберграмотности рядовых сотрудников				

Лицензирование по устройствам

Что такое XDR?

Интересные факты об XDR

Буква “X”

“X” в начале сокращенного варианта названия “xDR” означает разнообразие подключаемых источников

Состав XDR

XDR охватывает наиболее популярные точки проникновения в инфраструктуру: рабочие станции, виртуальные машины , серверы, сеть, почтовый трафик. А также автоматически обогащает поступающую телеметрию данными Threat Intelligence

XDR и EDR

XDR основан на расширении технологии EDR контролем потенциальных точек входа злоумышленника за пределами рабочих мест и серверов. EDR - ключевой элемент XDR. XDR должен строиться на сильном EDR в синергии с EPP

XDR и SIEM

Это не про вытеснение одного из классов решений с рынка, а про их объединение или отличное дополнение и расширение функционала друг друга

Наиболее привлекательные функциональные возможности XDR

Источник: По данным опроса Enterprise Strategy Group «Влияние XDR на современный SOC»

Пример состава решения класса XDR

от XDR-вендора

Защита конечных точек

- ПК
- Ноутбуки
- Серверы
- Виртуальные машины
- OS Различные ОС
- Мобильные устройства

от сторонних вендоров

Интеграция с ИБ-решениями

от XDR-вендора

Набор ИБ-продуктов

- Защита сети
- Защита почты
- Защита облаков и контейнеров
- Защита учетных записей
- Повышение осведомленности сотрудников
- Другие ИБ-решения

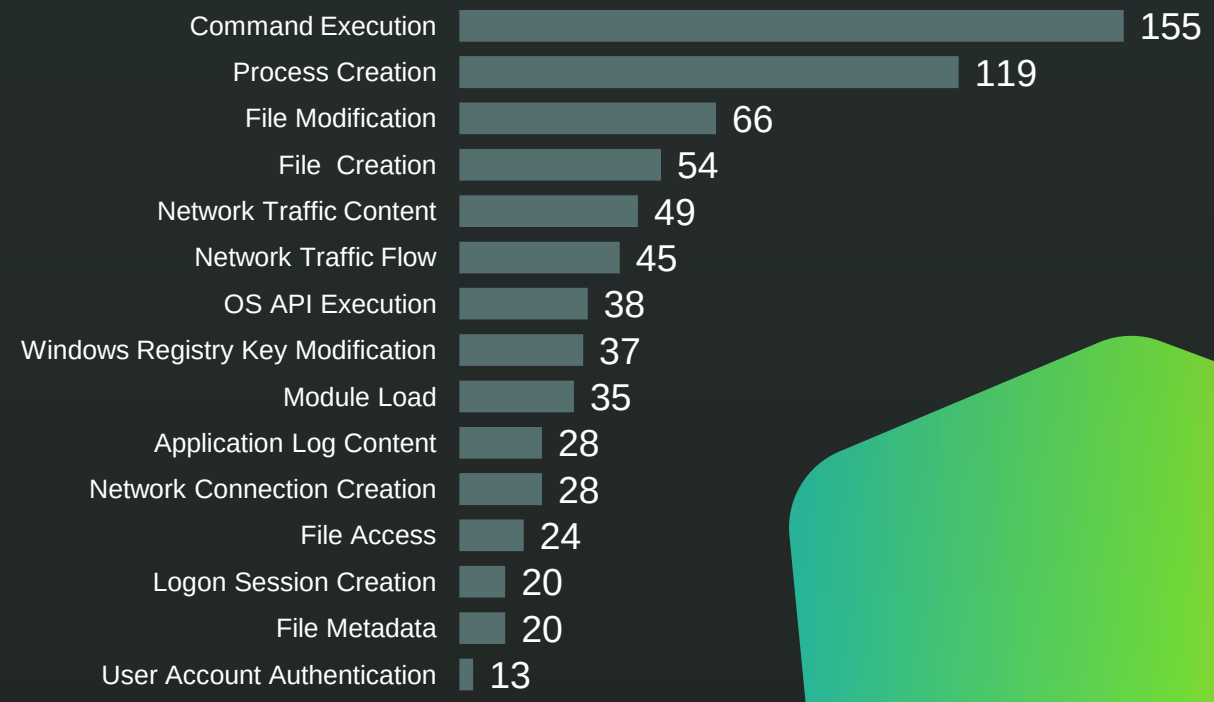
Конечные точки

Основной источник данных для качественного расследования и понимания первопричин

MITRE ATT&CK

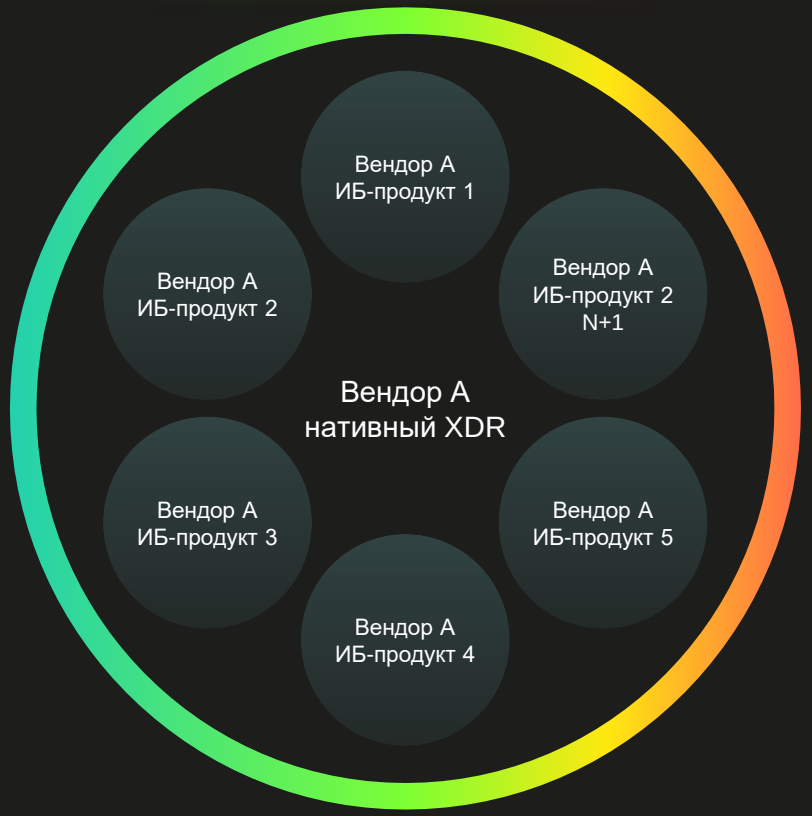
KASPERSKY

Наиболее важные компоненты данных в Топ 15 техник



Типы XDR

Нативный XDR



Гибридный XDR

Источник: Forrester

Типы XDR в портфеле «Лаборатории Касперского»

Нативный XDR

Kaspersky Anti Targeted Attack с EDR

Гибридный XDR

NEW

Kaspersky Symphony XDR

O Kaspersky Symphony XDR

Kaspersky Symphony XDR: Расширенные возможности защиты

- Включена функциональность платформы Threat Intelligence и потоки данных об угрозах
- Включено повышение осведомленности сотрудников
- Включен модуль ГосСОПКА для автоматического взаимодействия с НКЦКИ

Продуктовый состав Kaspersky Symphony XDR

Сильные стороны Kaspersky Symphony XDR

Kaspersky Symphony XDR

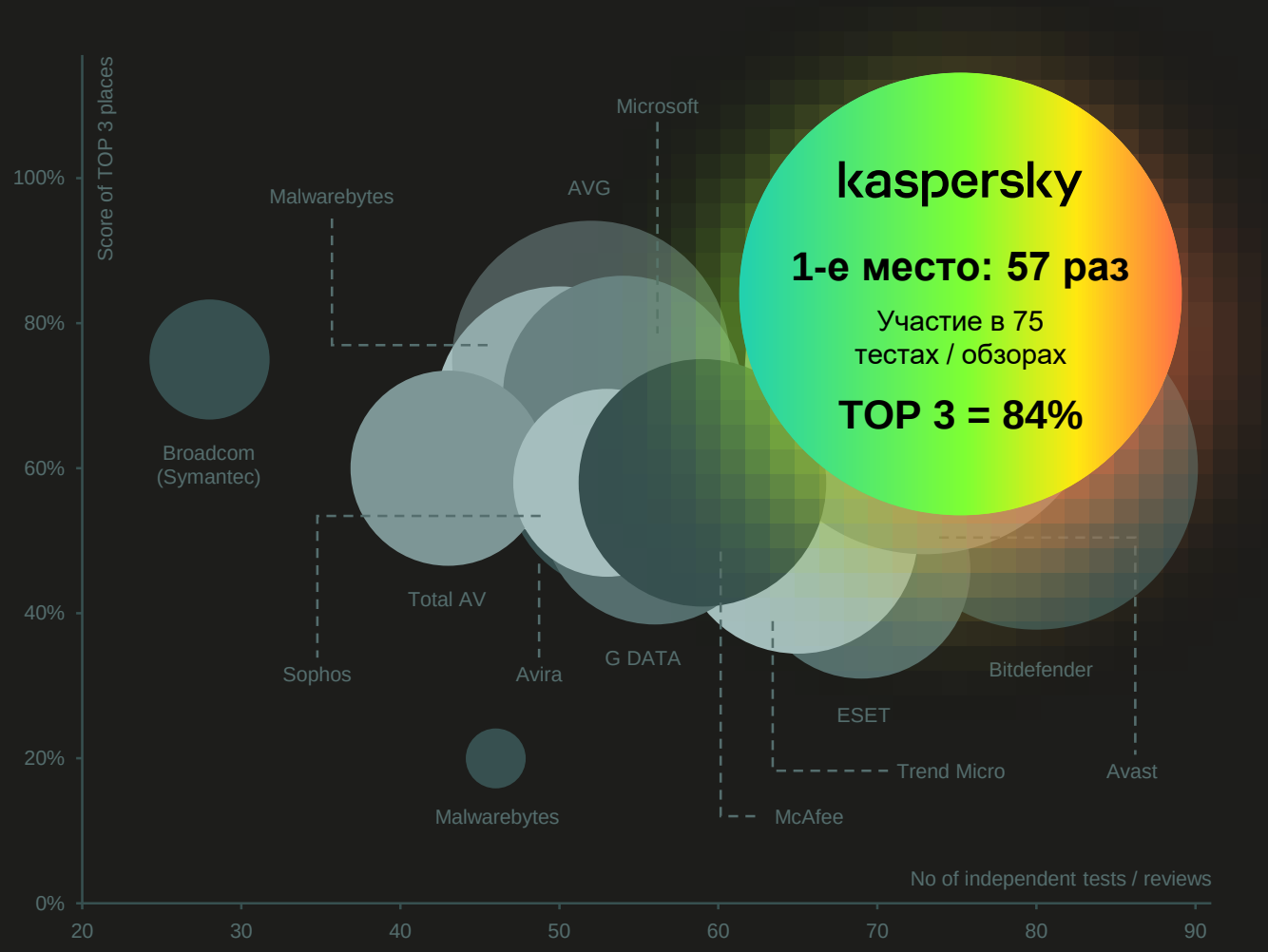
Фокус на конечные точки

Включен EDR в синергии с EPP – они уже защищают более чем 60 миллионов корпоративных рабочих мест по всему миру

Фокус на аналитику об угрозах

Включена признанная лучшей в мире аналитика об угрозах (по результатам Forrester Wave: External Threat Intelligence Services 2021)

Больше тестов. Больше наград. Защитные решения «Лаборатории Касперского»



MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

Узнать больше

В 2021 году продукты «Лаборатории Касперского» приняли участие в 75 независимых тестах и обзорах. Наши продукты получили 1 место 57 раз, а также вошли в топ-3 продуктов по результатам 63 тестов

* Примечания:

- ПО итогам суммарных результатов независимых тестов для корпоративных и домашних пользователей, а также мобильных продуктов в 2021 году
- Обзор описывает независимые тесты, проведенные AppEsteem, AV-Comparatives, AV-TEST, ICSA Labs, MRG Effitas, SE Labs, Testing Ground Labs, Virus Bulletin
- В рамках тестов, проведенных в этих программах оценивалась эффективность всех технологий защиты при противодействия известным, неизвестным и продвинутым угрозам
- Размер кругов соответствует количеству полученных первых мест
- Решения «Лаборатория Касперского» были протестированы больше всех за период с 2013 по 2021 год

Международное признание

В состав Kaspersky Symphony XDR входят продукты, заслужившие признание аналитиков, независимых лабораторий и клиентов по всему миру. Решение повышает эффективность команды ИБ и помогает бизнесу развиваться — устойчиво и гармонично

Gartner

Победитель Gartner Peer Insights Customers' Choice в категории:

- «EDR-решения» в 2020 г.
- «EPP-решения» в 2021 г.
- «Платформы повышения киберграмотности» в 2021 г.

Международная оценка

Radicati Group

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Ведущий игрок по защите
от APT-угроз по данным
исследовательской компании
Radicati Group в 2021 г.

Независимые тесты

MITRE | ATT&CK®

MITRE | ATT&CK®

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

Международная оценка

IDC

IDC

Ключевой игрок в области защиты конечных устройств для бизнеса по версии IDC MarketScape в 2021 г.

Forrester

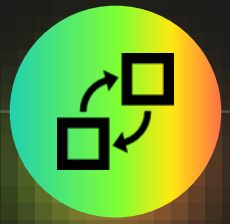
FORRESTER®

Лидер в области сервисов оперативного информирования о киберугрозах по данным Forrester Wave: External Threat Intelligence Services в 2021 г.

Сильные стороны Kaspersky Symphony XDR

Фокус на киберграмотность

Включен модуль контроля и повышение осведомленности рядовых сотрудников



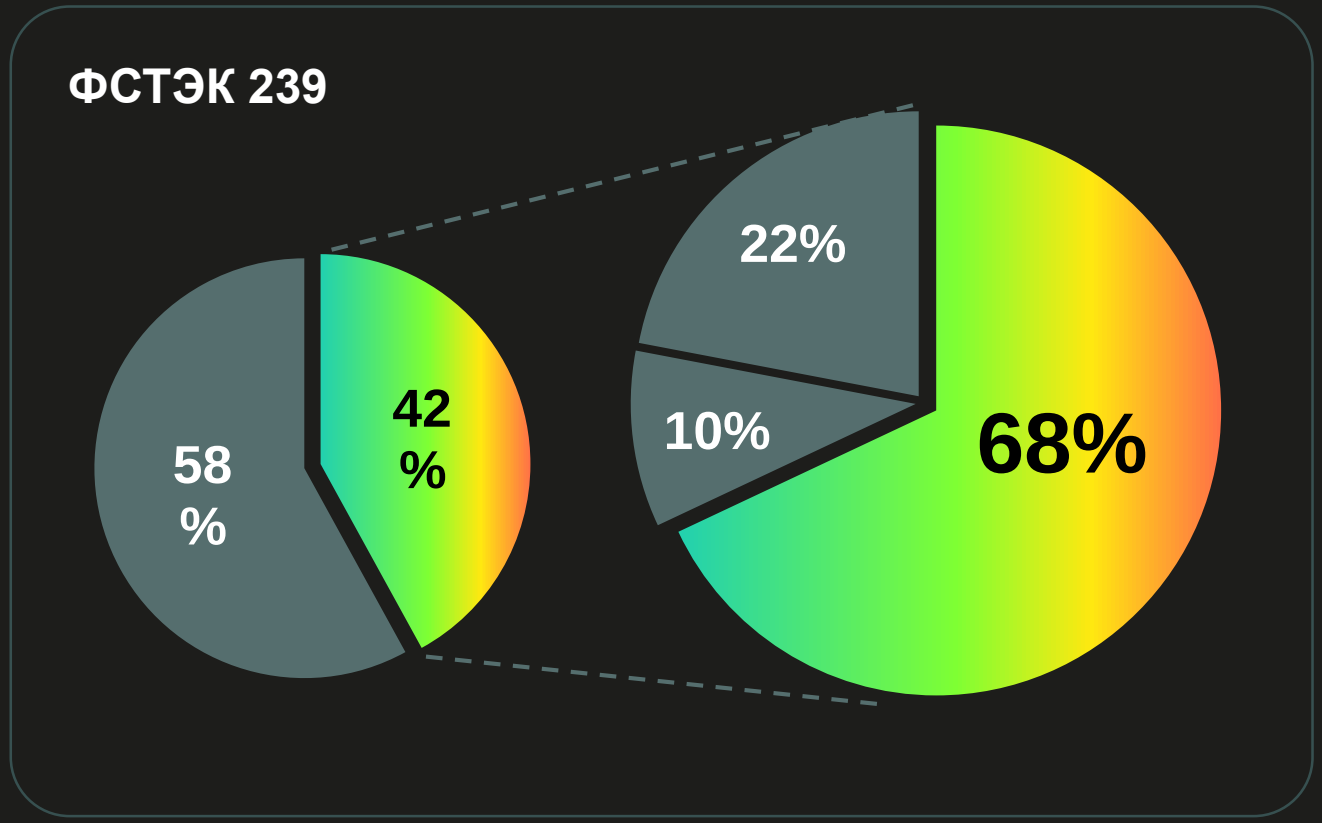
Фокус на взаимодействие

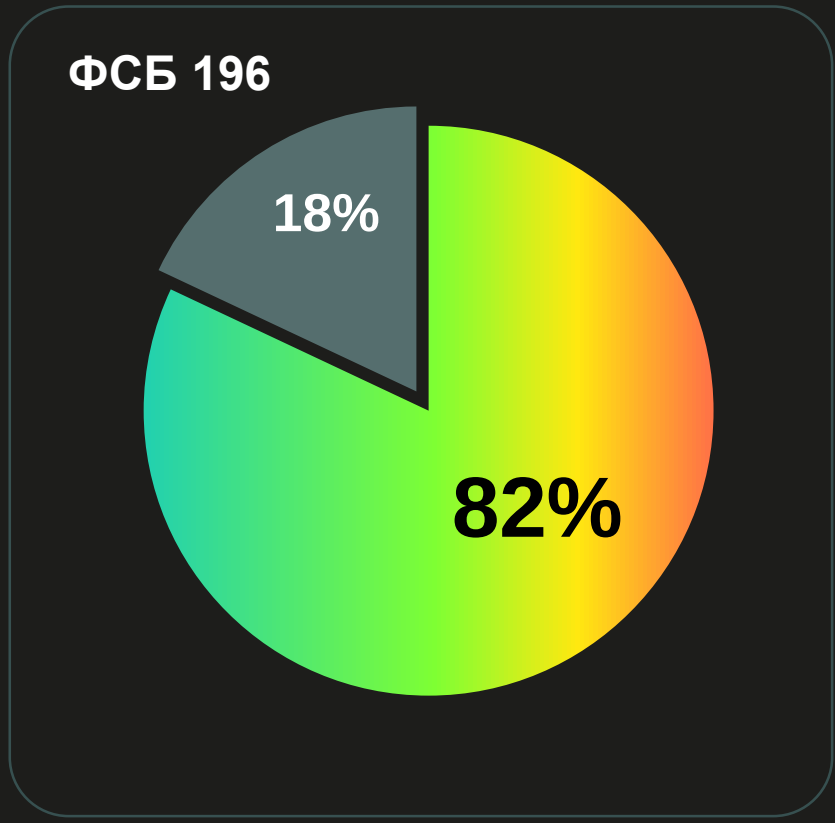
Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии, гибкость сетевой защиты (Netflow, движки KATA, загрузка TI в сторонние инструменты – IDS&APT фиды). Взаимодействие с решениями сторонних поставщиков.

Фокус на соответствие

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

Kaspersky Symphony XDR. Соответствие требованиям регуляторов





58% - Организационные меры, штатное ПО (OS, FW, BackUp)

42% - Наложенные СЗИ

68% - Kaspersky Symphony

10% - Другие решения Kaspersky

22% - Стороннее ПО или СЗИ

82% - Kaspersky Symphony

18% - Сторонние решения

Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Автоматические

- Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике
- Автоматическая блокировка на уровне почтового шлюза неизвестных вредоносных объектов, обнаруженных детектирующими механизмами KATA (до доставки получателю)
- Взаимодействие веб-шлюза и KATA через API для передачи объектов из веб-трафика на проверку в песочницу и последующей их автоматической блокировки в случае выявленной вредоносной нагрузки
- Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace
- Передача релевантных сложных атакам событий с KATA, KES, KEDR, KSMG, KWTS в KUMA для корреляции с данными от сторонних источников
- Передача сырой телеметрии с EDR в KUMA
- Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя*

Полуавтоматические

- Доступ в Threat Lookup для получения дополнительного контекста для эффективного расследования
- Построение и обогащение модели активов в KUMA на основании данных из KSC
- Принудительный запуск обновления баз, антивирусной проверки, установки патча и других задач через KSC с карточки инцидента в KUMA
- Запуск действий по реагированию через EDR с карточки инцидента в KUMA*
- Возможность назначить обучение по повышению киберграмотности из карточки инцидента в KUMA*
- Передача информации о произошедших инцидентах в НКЦКИ, благодаря встроенному в решение модулю ГосСОПКА

*В ближайшем Roadmap

Преимущества экосистемы

Всесторонняя осведомленность

- Централизованная отчетность
- Кросс-продуктовый Kill-chain*
- Единое управление инцидентами
- Обогащение данными Threat Intelligence и информацией о активах

Гибкая и ресурсоэффективная архитектура

- Производительный real-time коррелятор
- Гибкий и быстрый ретроспективный поиск
- Работа в распределённых инфраструктурах
- В 5 раз производительнее Elastic-based систем

Повышение эффективности аналитика

- AI-ассистент для улучшения точности детектирования*
- Коробочные интеграции между решениями (в том числе сторонними)
- Автоматизация типовых операций

*В ближайшем Roadmap

Фокус на снижение ложных срабатываний

Авто-аналитик

Более быстрое детектирование

Снижение FP на 35-40%

Эффективное использование ресурсов

Единый партнер
по кибербезопасности

Видит полную картину происходящего,
снижает издержки и дает уверенность
в завтрашнем дне.

kaspersky

Спасибо!