Kaspersky Symphony

kaspersky

Краткий план

- Наша экспертиза
- Экосистемный подход к защите
- О Kaspersky Symphony
- Почему Kaspersky?

Наша экспертиза

Наша экспертиза

380 000

уникальных вредоносных объектов
мы обнаруживаем ежедневно

Наша экспертиза

1 млрд

Общее число образцов в нашей вирусной коллекции превысило

200+ APT-групп

Отслеживали деятельность

121 отчёт

выпустили об APT атаках

300+ инцидентов

Приняли участие в расследовании

Экосистемный подход к защите

Как развивается и расширяется наша экосистема

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

GREAT

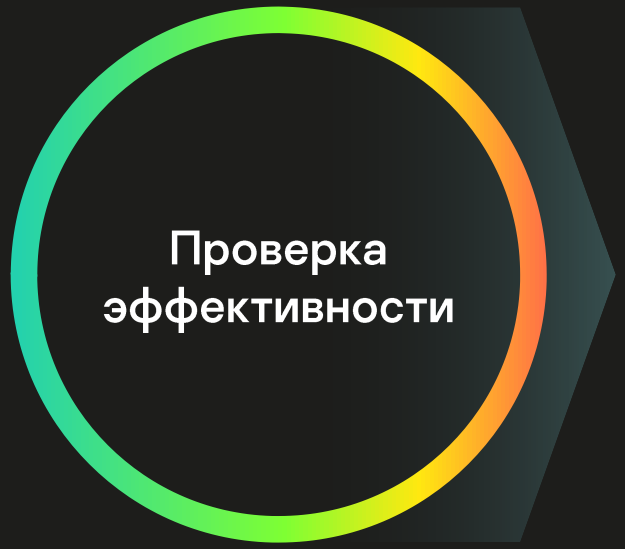
Kaspersky APT Research team

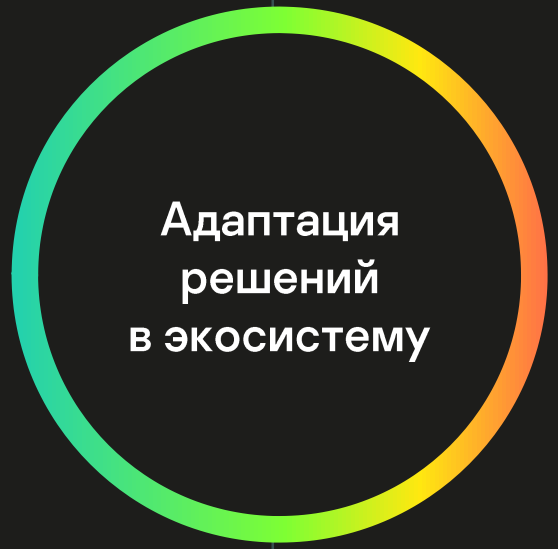
Kaspersky SOC

Kaspersky Red Team

Kaspersky ICS CERT

Как развивается и расширяется наша экосистема





Добавление в портфолио новых сценариев борьбы с угрозами

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 вендора 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

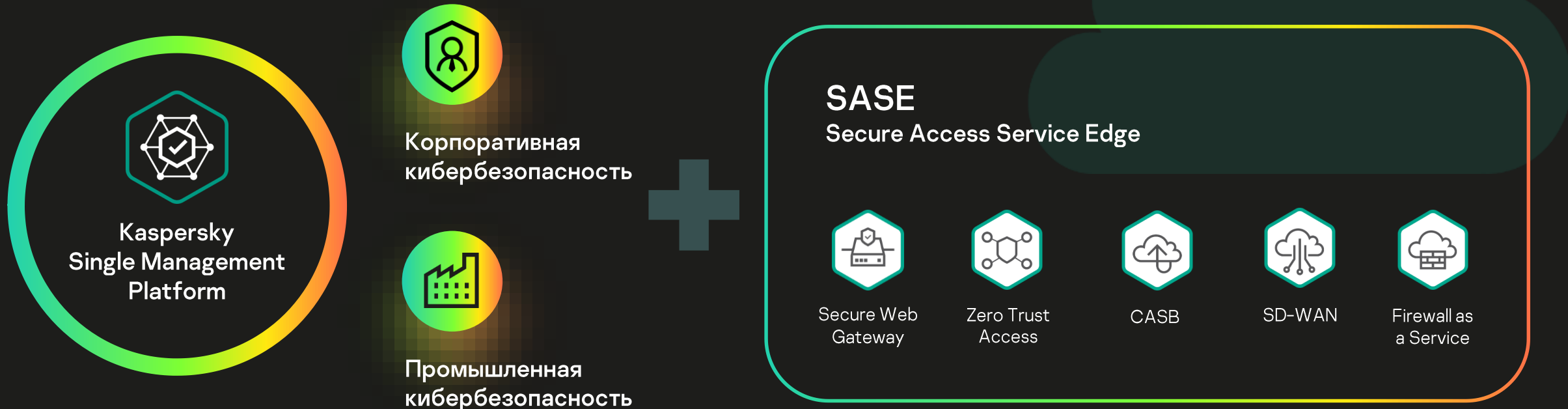
Покупка Brain4Net

Анонс Kaspersky Symphony

new

Kaspersky Symphony

«Лаборатория Касперского» завершила сделку по приобретению компании Brain4Net



О концепции XDR - Extended Detection and Response

Интересные факты об XDR

XDR

Это современная концепция, которая представляет собой кросс-продуктовую историю, обогащенную поверх дополнительными функциональными возможностями, в том числе Threat Intelligence

EDR

это ключевой элемент XDR. Без EDR не может быть XDR. XDR должен строиться на сильном EDR в синергии с EPP

XDR не равно EDR

XDR основан на расширении технологии EDR и контроля потенциальных точек входа злоумышленника за пределами конечных точек

Буква “X”

в начале сокращенного варианта названия “XDR” означает разнообразие подключаемых источников / продуктов

Минимальный комплект XDR

это охват конечных точек, сети, почтового и веб трафика, то есть, наиболее популярных точек проникновения злоумышленников в инфраструктуру, с обязательным обогащением данными Threat Intelligence

XDR и SIEM

это не про выживание одного из классов решений с рынка, а про их объединение или отличное дополнение друг друга

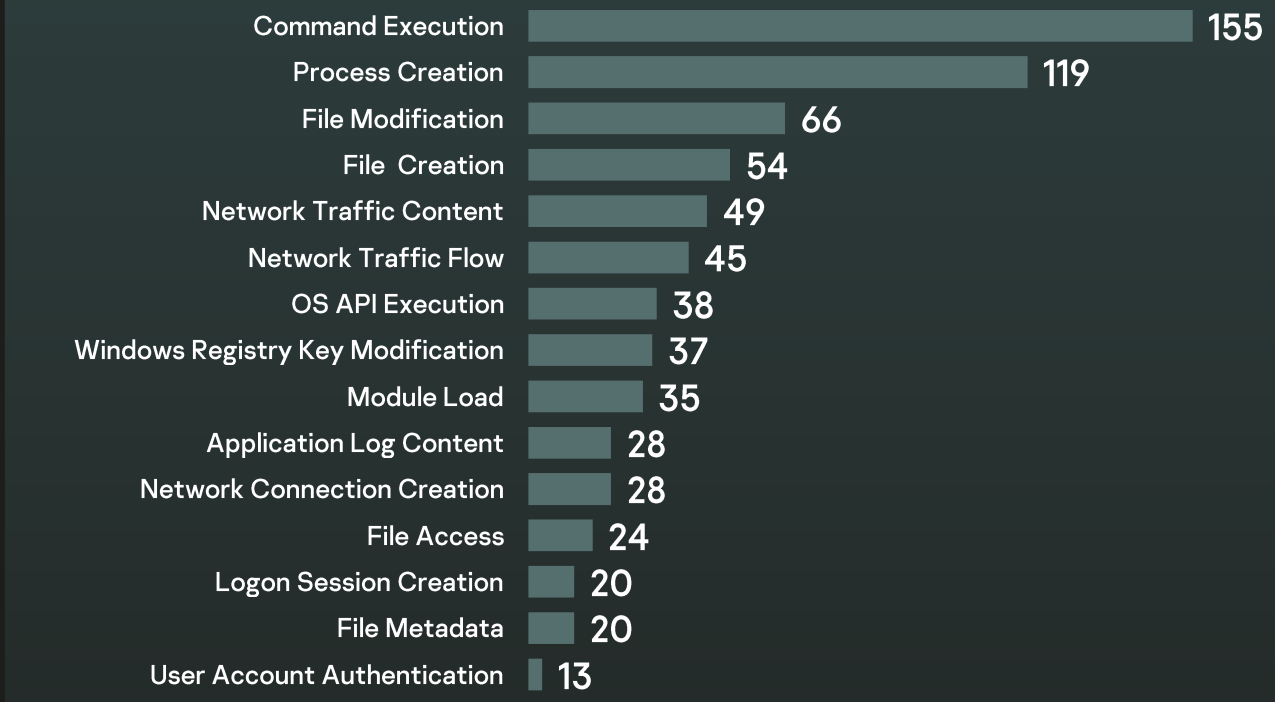
EDR – важнейший элемент XDR

Конечные точки

Основной источник данных для качественного расследования и понимания первопричин

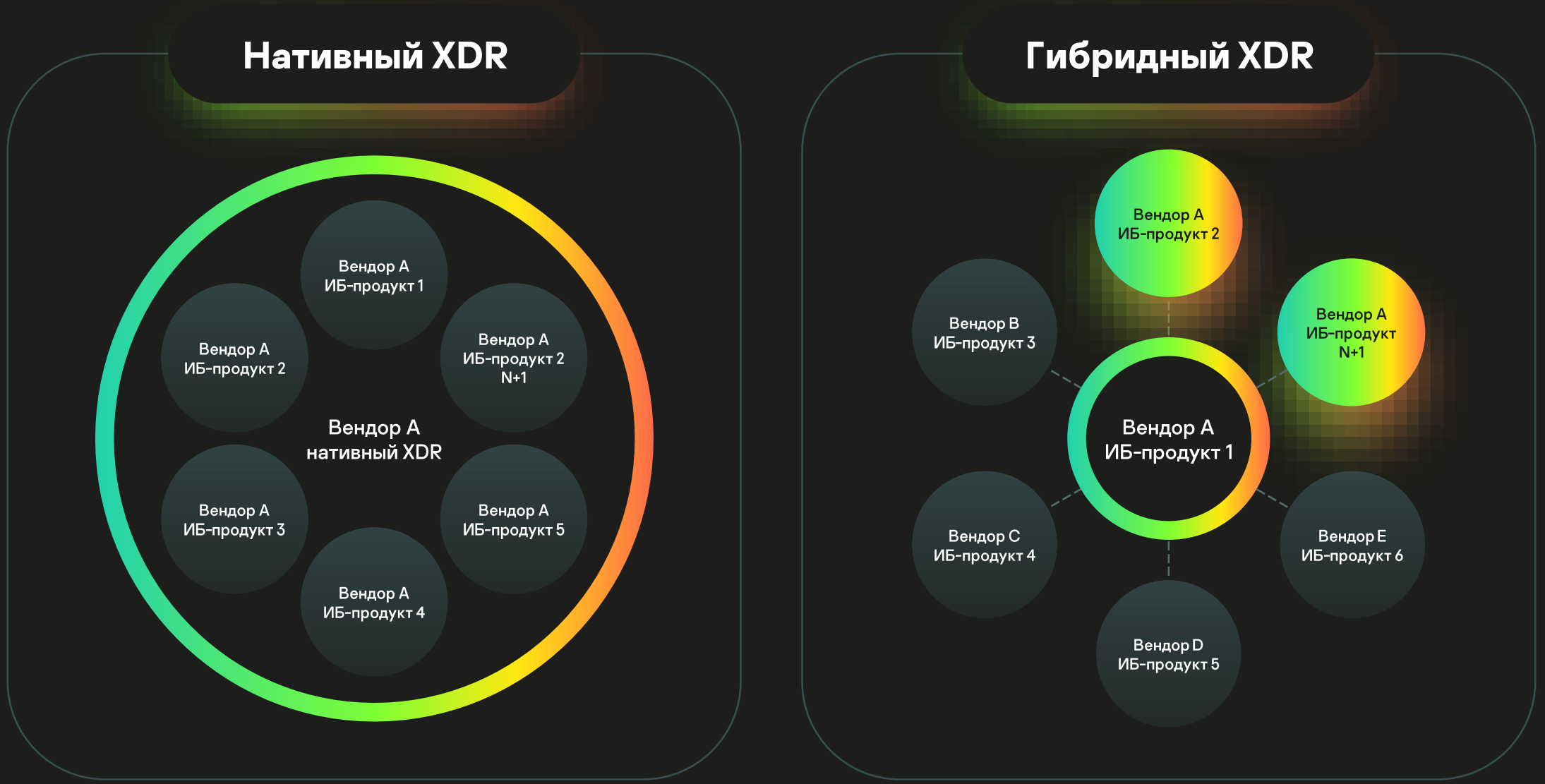
Топ 15 техник

Наиболее важные компоненты данных



Источник: https://github.com/mitre-attack/attack-datasources

Типы XDR



Источник: Forrester

Типы XDR

Нативный XDR

Kaspersky
Anti Targeted
Attack

Гибридный XDR

NEW

Kaspersky
Symphony
XDR

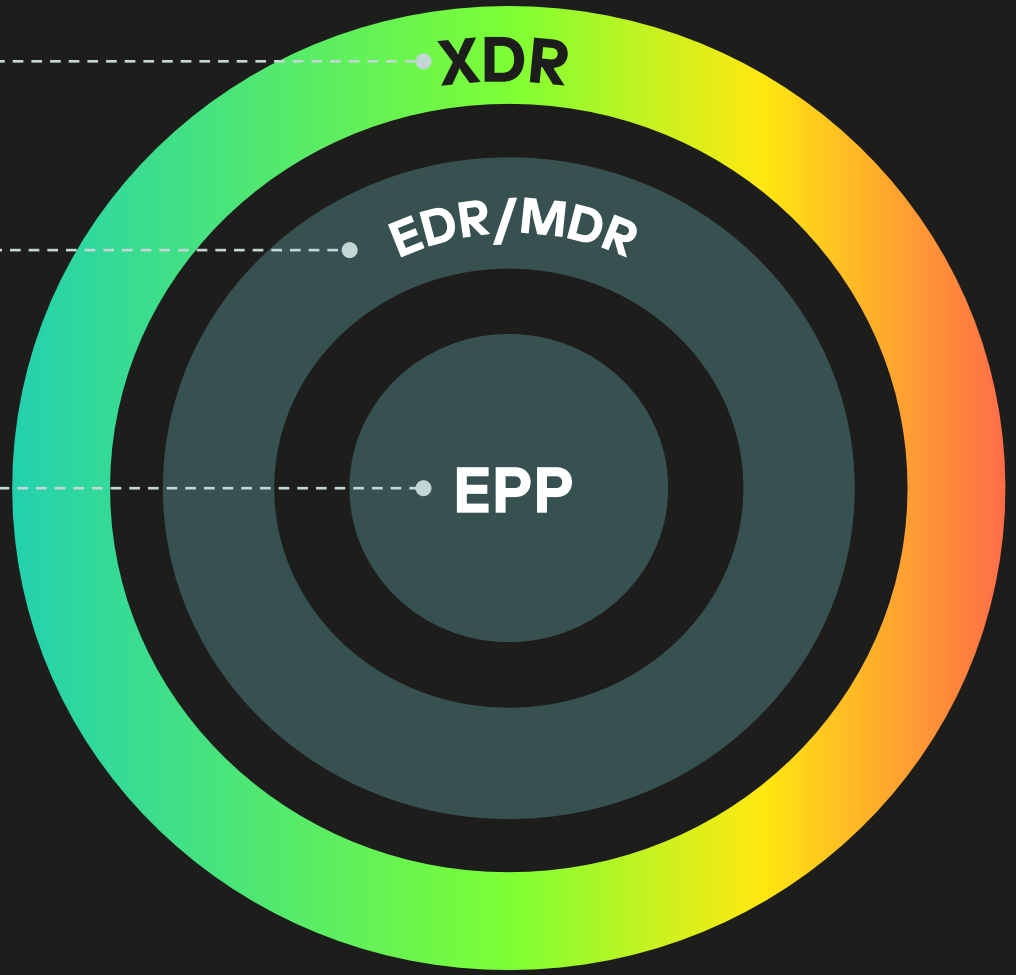
О новой линейке Kaspersky Symphony

Kaspersky Symphony. Уровни защиты

Kaspersky Symphony
XDR

Kaspersky Symphony
EDR / MDR

Kaspersky Symphony
Security



Состав уровней Kaspersky Symphony

Kaspersky Symphony	Security	EDR / MDR	XDR
Комплексная защита рабочих мест и серверов (физических, мобильных и виртуальных)	●	●	●
Выявление причин инцидентов и реагирование на них		●	●
Детектирование продвинутых угроз & Ретроспективный анализ		●	●
Защита электронной почты & Песочница & Анализ сетевого трафика			●
Встроенный контроль за повышением киберграмотности			●
Сбор и корреляция событий безопасности & Взаимодействие с ГосСОПКА & Кросс-продуктовые сценарии взаимодействия			●
Управление данными о киберугрозах & Потоки данных & доступ в Threat Lookup			●

Лицензирование по устройствам

Сильные стороны Kaspersky Symphony XDR

Kaspersky Symphony XDR

Фокус на конечные точки

В основе EDR в синергии с EPP, находящийся на страже у более чем 60 млн. корпоративных рабочих мест по всему миру

Фокус на обогащение Threat Intelligence

Признанная в мире лучшей глобальная аналитика об угрозах*

* «Лаборатория Касперского» признана лидером по результатам Forrester Wave: External Threat Intelligence Services 2021

Фокус на особо уязвимых рядовых сотрудников

Встроенный контроль за повышением киберграмотности

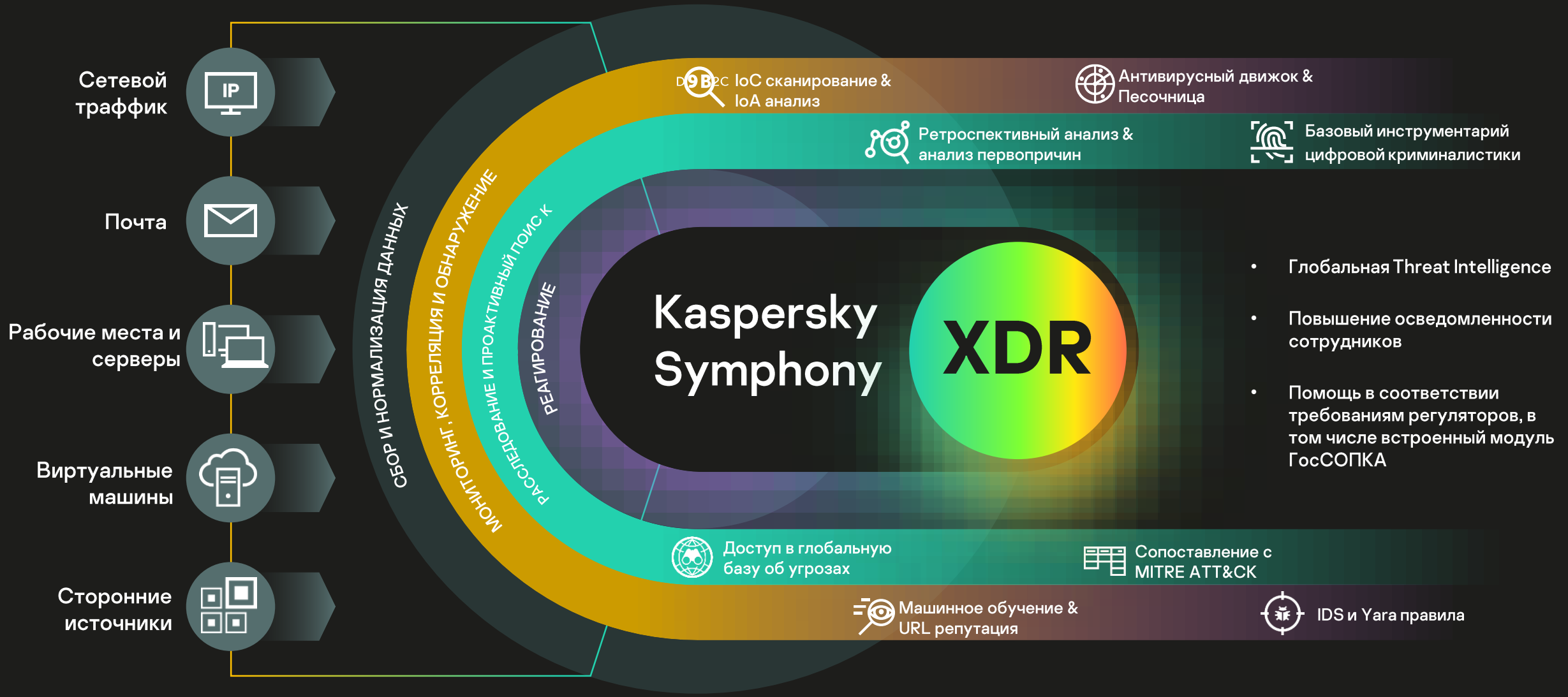
Фокус на взаимодействие

Тесное взаимодействие продуктов, кросс-продуктовые сценарии и соответствие требованиям

Фокус на гибкость сетевой защиты

- Netflow
- Движки KATA
- Загрузка нашего TI в сторонние инструменты (IDS&APT feeds)
- Движение в сторону SASE

XDR: Расширенные возможности защиты



- Глобальная Threat Intelligence
- Повышение осведомленности сотрудников
- Помощь в соответствии требованиям регуляторов, в том числе встроенный модуль ГосСОПКА

Почему Kaspersky ?

Единый партнер по кибербезопасности видит полную картину

Единый партнер по кибербезопасности снижает издержки

- Единый поставщик
- Единая служба поддержки
- Единая схема лицензирования

Единый партнер по кибербезопасности дает уверенность

Надежный

Проверенный

Стратегический

Спасибо!

https://go.kaspersky.com/symphony