KSD 2022
Kaspersky Security Day

Kaspersky Symphony XDR: сценарии кросс-продуктового взаимодействия

Евгений Бударин
Head of Presales

kaspersky 25 лет

Kaspersky Symphony XDR

Интеграция с решениями сторонних поставщиков

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 Unified Monitoring and Analysis Platform

Защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

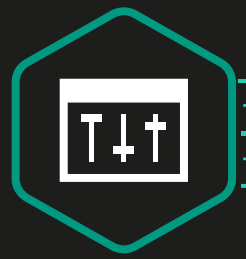
Обучение пользователей

- Kaspersky Automated Security Awareness Platform

Threat Intelligence

- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Kaspersky Endpoint Security для бизнеса



Kaspersky
Security Center

СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Обнаружение уязвимостей и управление установкой исправлений, а также расширенные возможности управления клиентскими системами

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Защита от известных, неизвестных и сложных угроз

ШИФРОВАНИЕ ДАННЫХ

Полностью интегрированная защита данных

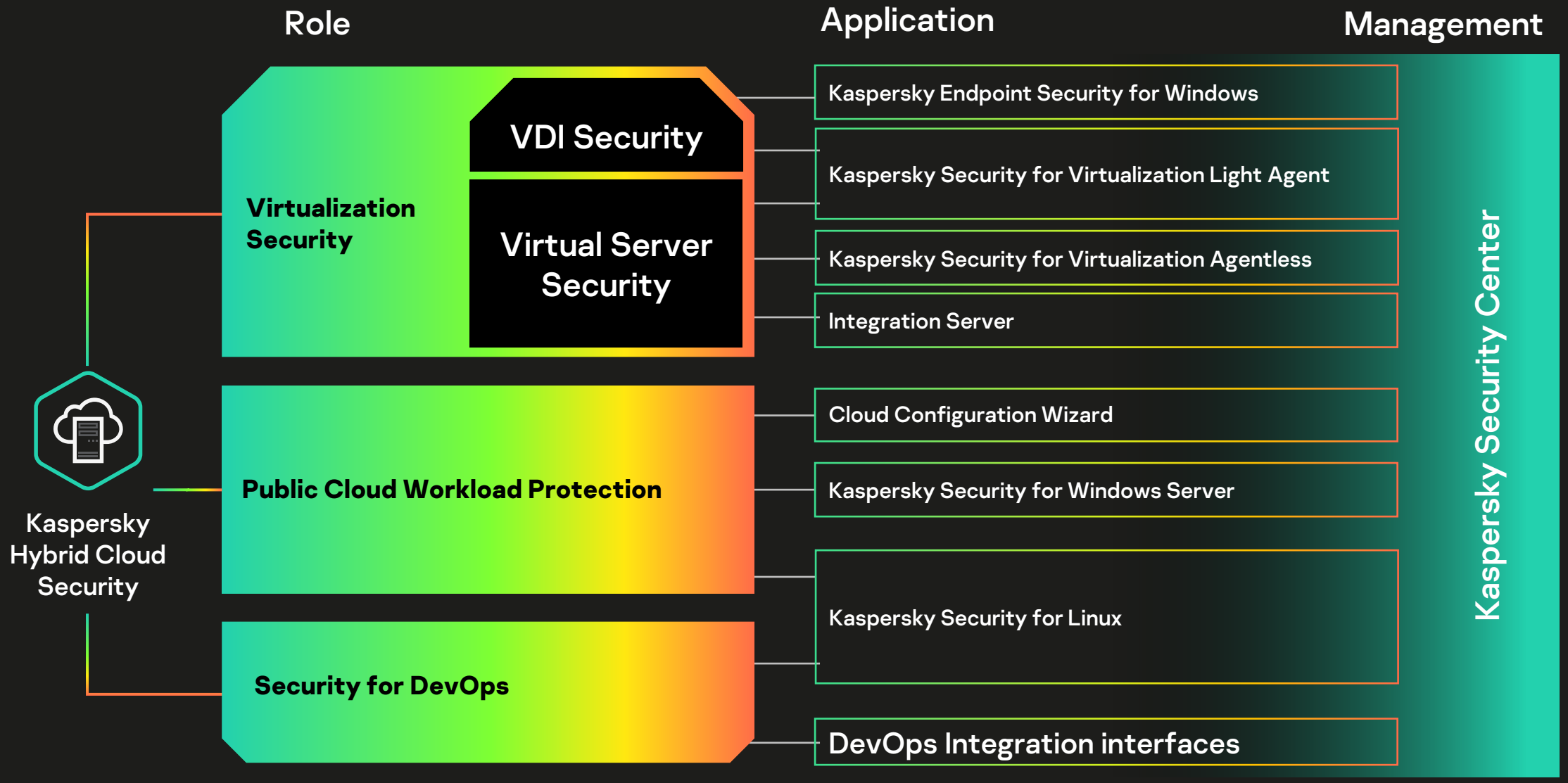
СРЕДСТВА КОНТРОЛЯ РАБОЧИХ МЕСТ

Контроль программ, Контроль устройств и Веб-Контроль

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Обеспечение безопасности смартфонов и планшетов и управление ими

Kaspersky Hybrid Cloud Security



Kaspersky Symphony XDR

Интеграция с решениями сторонних поставщиков

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 Unified Monitoring and Analysis Platform

Защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Обучение пользователей

- Kaspersky Automated Security Awareness Platform

Threat Intelligence

- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Автоматизированное обнаружение и реагирование

Kaspersky Symphony XDR

Интеграция с решениями сторонних поставщиков

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 Unified Monitoring and Analysis Platform

Защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

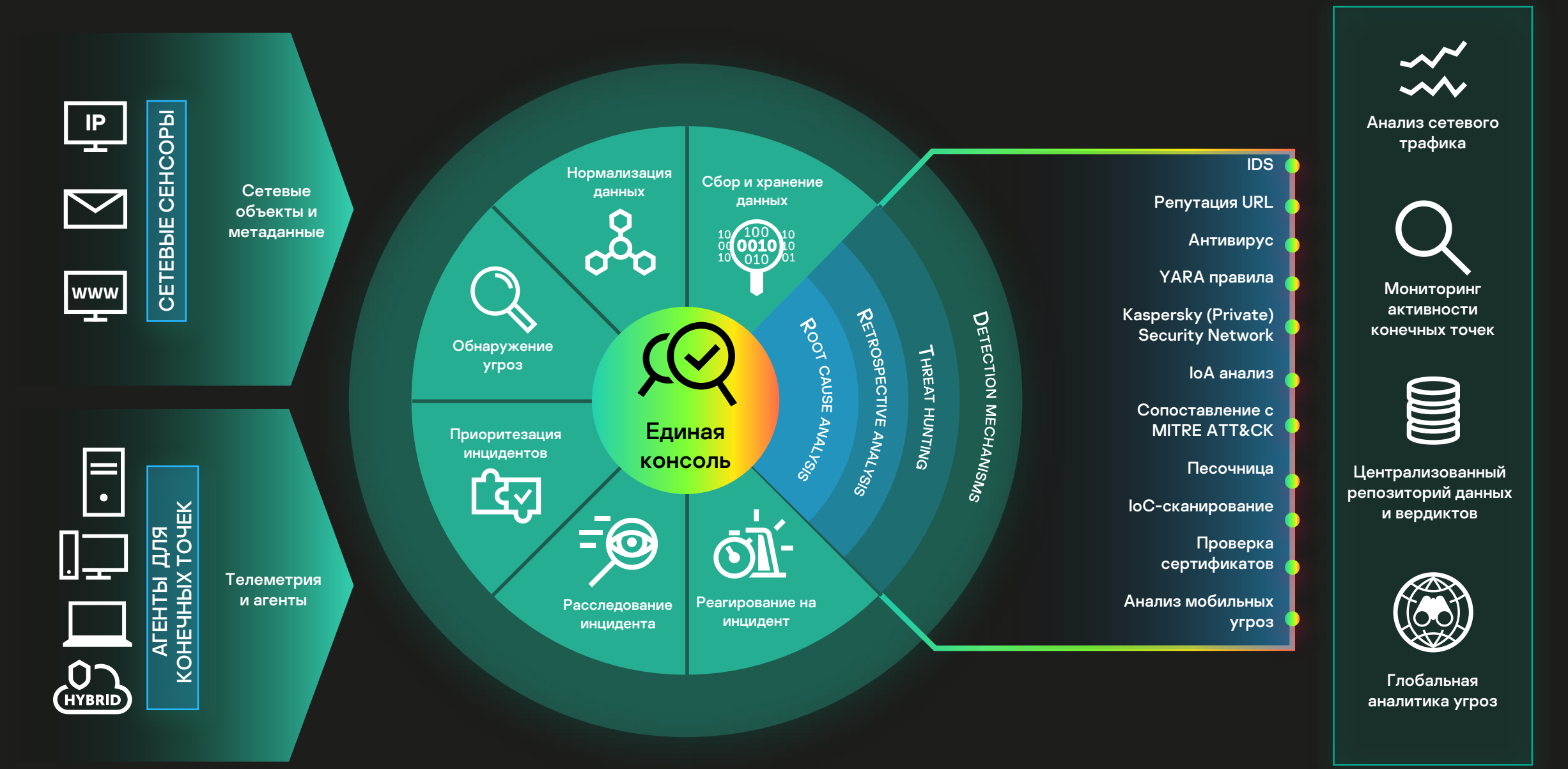
Обучение пользователей

- Kaspersky Automated Security Awareness Platform

Threat Intelligence

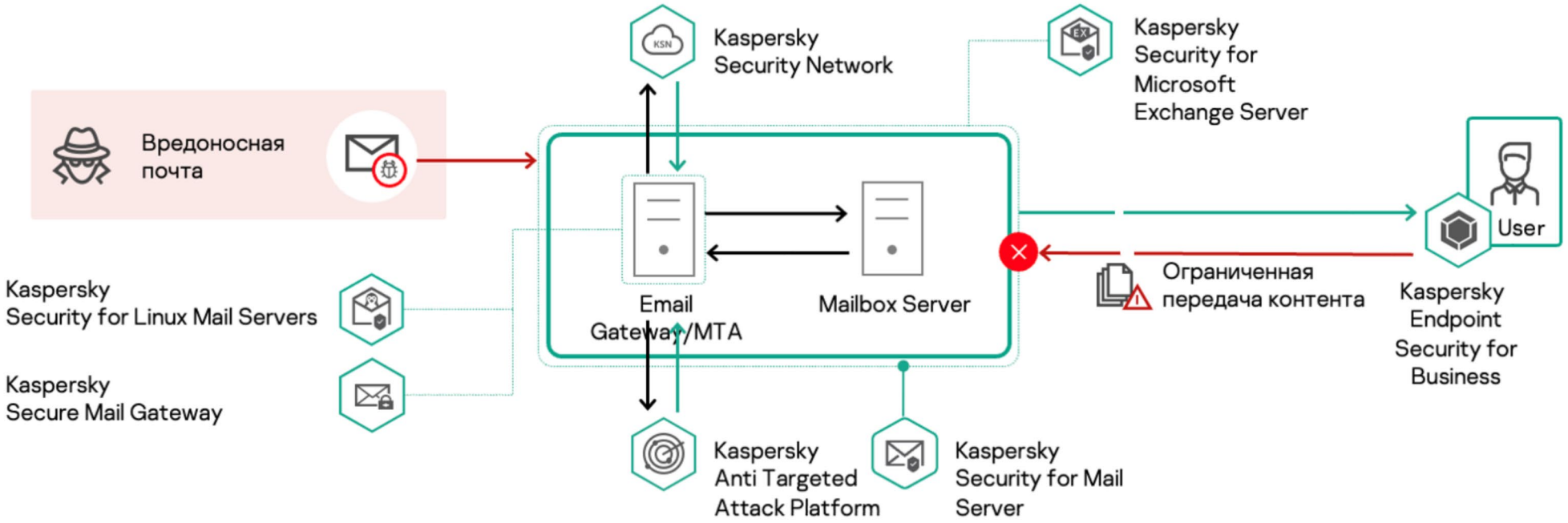
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Kaspersky Anti Targeted Attack (KATA) с EDR



Kaspersky Security для почтовых серверов

- Многоуровневая защита от ВПО и фишинга на основе ML
- Обнаружение вредоносных скриптов
- Контентная фильтрация для защиты снижения риска заражения
- Поддержка облачной инсталляции
- Автоматический анти-спам с репутацией
- Поддержка Linux and MS Exchange почтовых серверов
- Универсальное, готовое к использованию решение Secure Mail Gateway
- Углубленный анализ угроз с помощью Kaspersky Anti Targeted Attack



Kaspersky Security для интернет-шлюзов

Многоуровневая защита от угроз

- Защита от веб-угроз
- Антивирус
- Защита из облака (Kaspersky Security Network)
- Репутационная фильтрация
- Эмуляция песочницы
- Анти-фишинг
- Обнаружение скриптов
- Защита от шифровальщиков и криптомайнеров
- Блокирование файлов и веб-адресов

Расширенные функции контроля

- Веб-контроль
- Система категорий
- Контентная фильтрация

Обнаружение сложных угроз

- KATA*-сенсор
- Доступ к вердиктам KATA
- Интеграция с KPSN
- Sandbox (KATA)

Мониторинг и управление

- Мониторинг и отчеты
- Система ролевого доступа
- Рабочие области
- SIEM-интеграция
- Прокси-сервер
- Анализ событий обработки трафика
- Кластерная архитектура

*KATA – Kaspersky Anti Targeted Attack

Kaspersky Symphony XDR

Интеграция с решениями сторонних поставщиков

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 Unified Monitoring and Analysis Platform

Защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Обучение пользователей

- Kaspersky Automated Security Awareness Platform

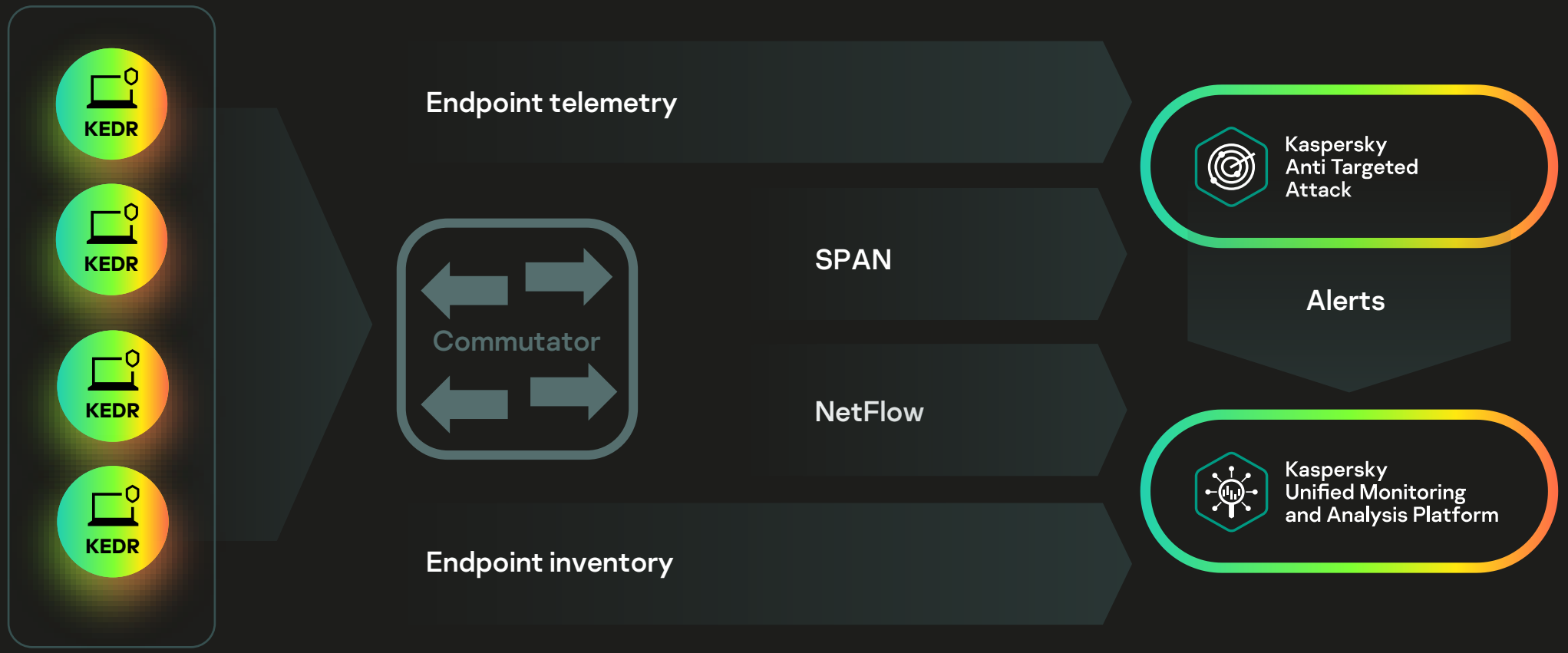
Threat Intelligence

- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

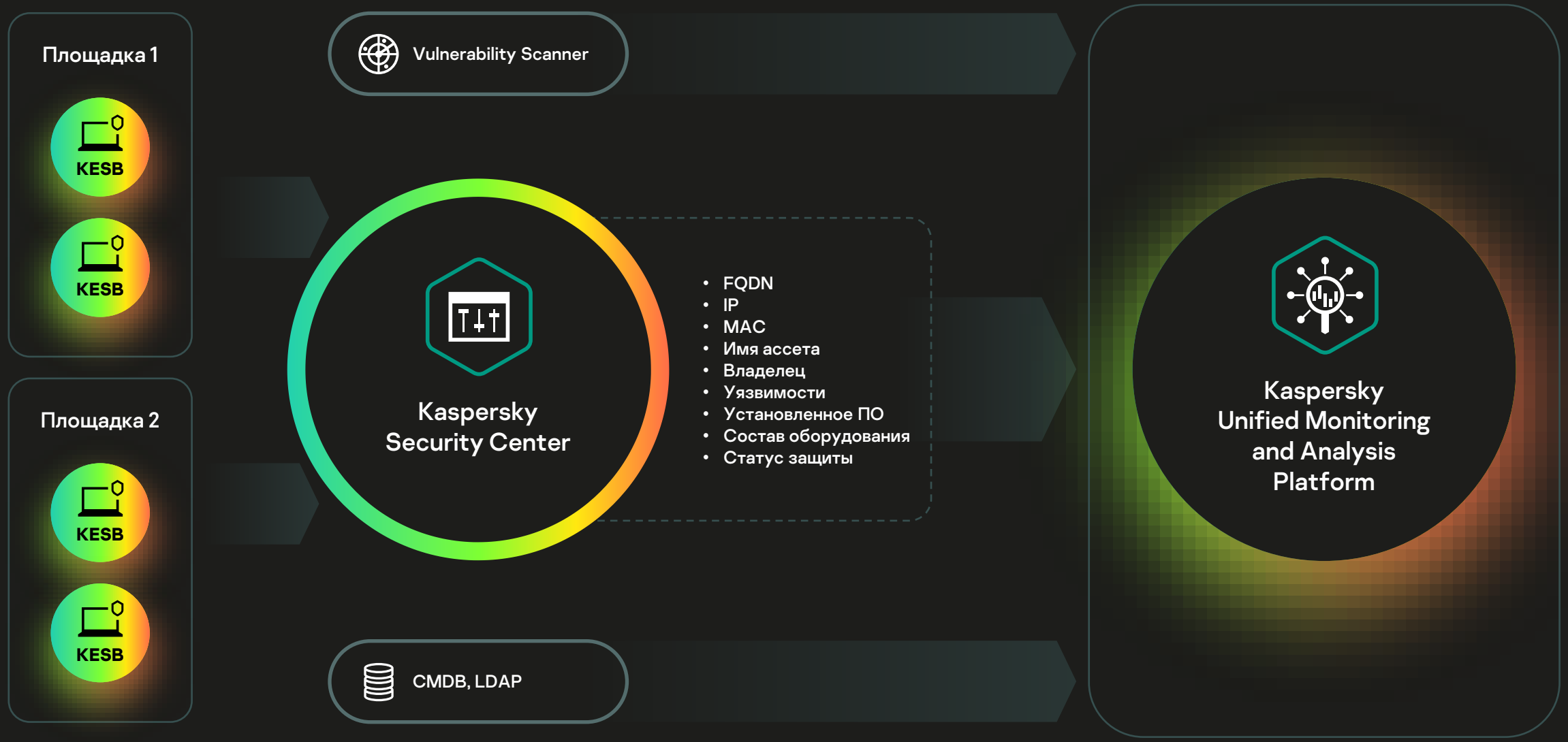
Архитектура KUMA

Пример 1. Сбор и анализ расширенной телеметрии

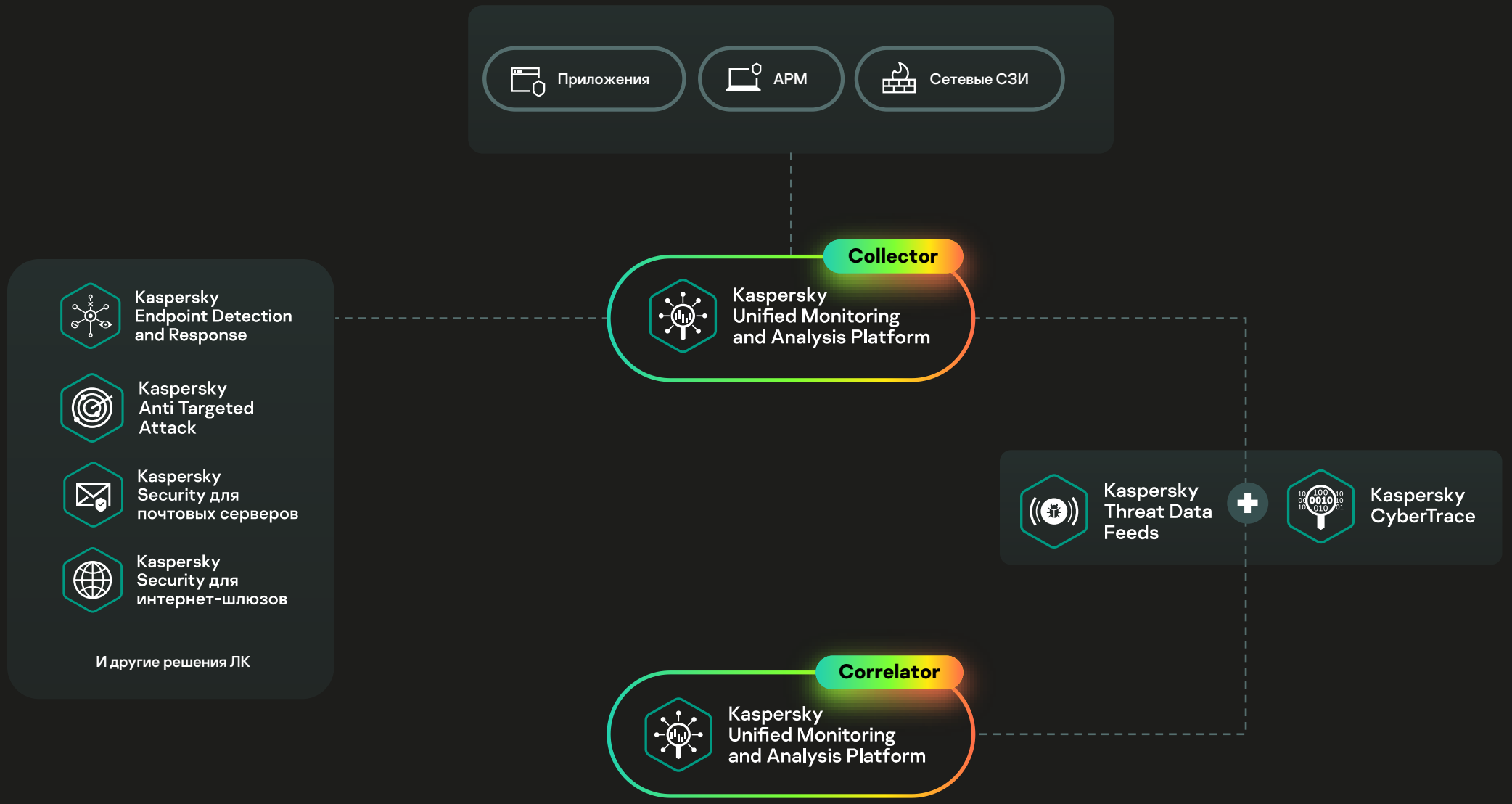
Пример 2. Анализ сетевого трафика



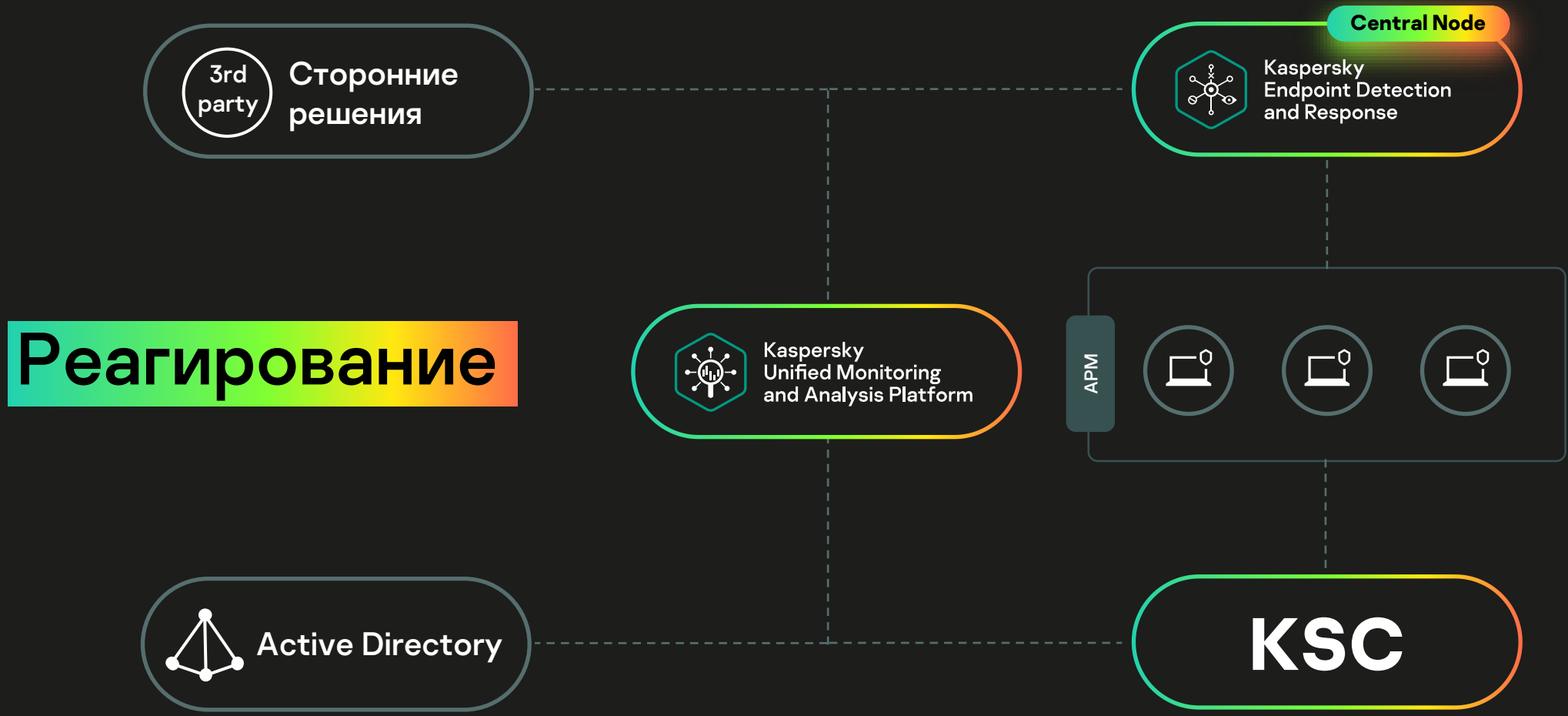
Пример 3. Инвентаризация информационных активов



Пример 4. Обогащение данными Threat Intelligence

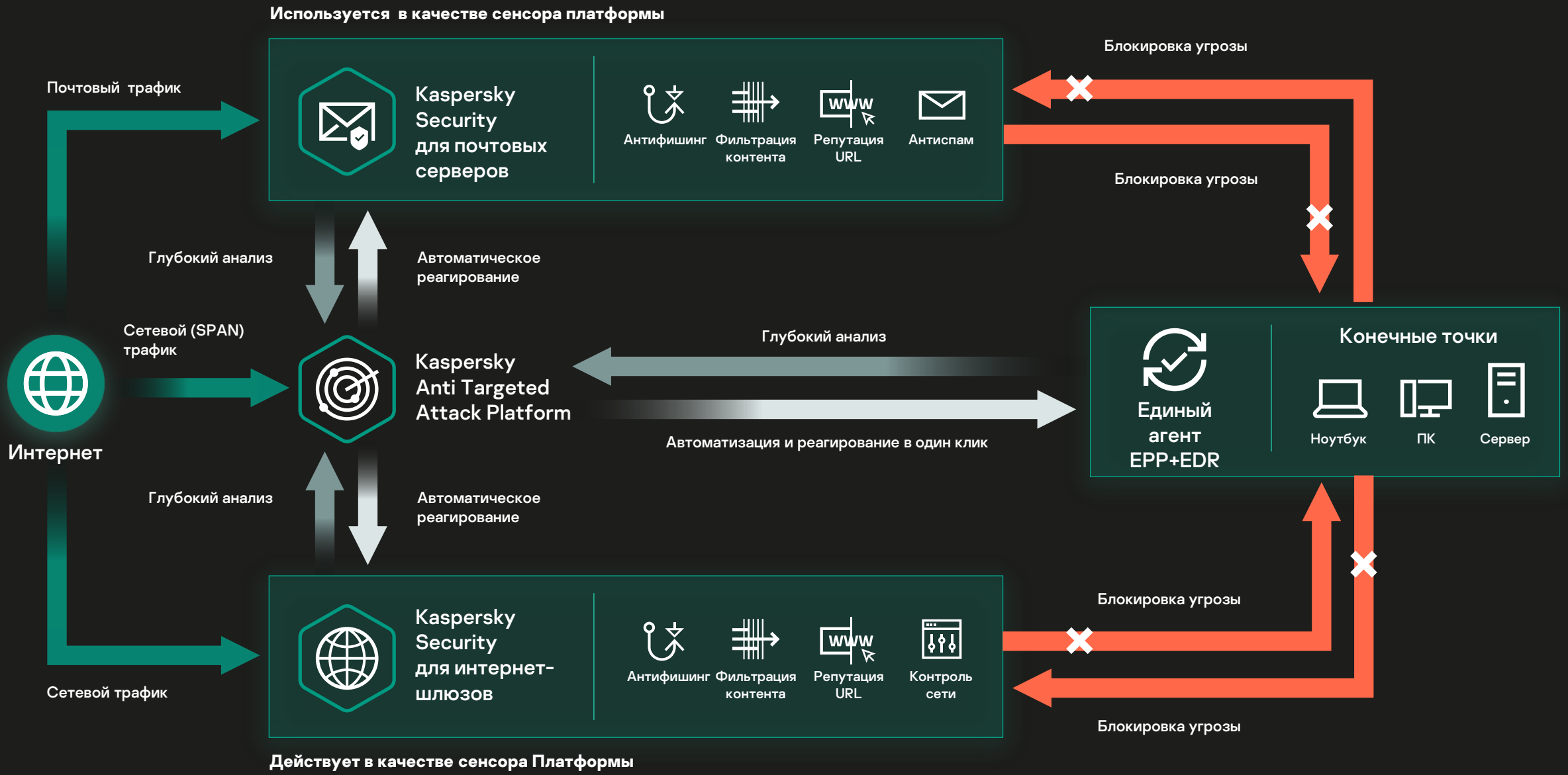


Пример 5. Автоматизированное реагирование на инциденты



* В ближайших планах разработки

Пример 6. Автоматизированное реагирование на инциденты



Kaspersky Symphony XDR — решение «Закона треугольника»

KSD 2022

Kaspersky Security Day

Спасибо!

kaspersky 25 лет