Современные технологии защиты от передовых угроз

kaspersky

Новая реальность

Неопределенность. Больше рисков. Поиск решения

Интерактивная карта киберугроз

https://cybermap.kaspersky.com/

Усложнение атак

Количество киберинцидентов в российских компаниях увеличилось в 4 раза

Киберагрессия

Россия номер 1 в мире среди атакуемых стран

Срочное замещение

Ряд различных защитных ИБ решений становятся менее эффективными, риски пропустить сложную кибератаку значительно повышаются

Ежегодно

Усложняется ландшафт угроз,
киберпреступники совершенствуют свои методы

Расширяется поверхность атаки
и количество точек входа злоумышленников

Усиливаются требования регуляторов,
особенно в отношении обеспечения защиты КИИ

+ Добавилось

Наступила эра хактивизма
и целевой киберагрессии

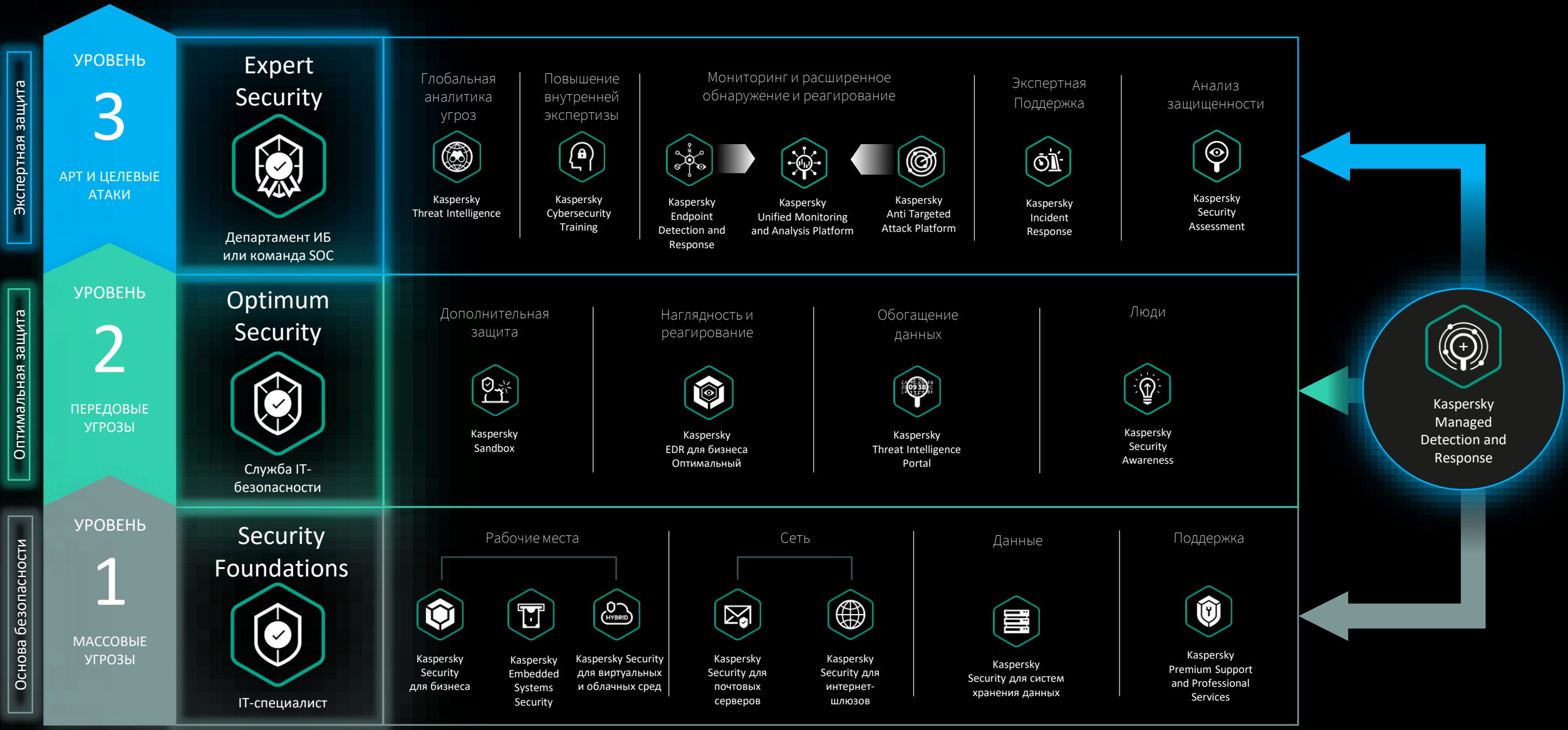
Больше лазеек
из-за полного ухода ИБ-вендоров или
приостановки обновлений их решений

Началась активная фаза
импортонезависимости

Ступенчатый подход «Лаборатории Касперского» к кибербезопасности

Наш подход направлен на борьбу с киберугрозами разного типа и сложности и подходит для организаций любой величины и отрасли

Портфолио «Лаборатории Касперского»



Kaspersky Endpoint Security для Бизнеса – линейка из шести решений

Kaspersky Security for Business Стандартный

Kaspersky Security for Business Расширенный

Kaspersky EDR for Business Оптимальный

Kaspersky Total Security for Business

Kaspersky Symphony Security (Универсальный)

Kaspersky Total Security Plus for Business

KESB Расширенный преимущества:

- ✓ Адаптивный контроль аномалий
- ✓ Шифрование данных
- ✓ Развертывание ОС и программ
- ✓ Патч-менеджмент

Линейка решений Kaspersky Security для бизнеса содержит несколько уровней с нарастающим функционалом. Для перехода на новый уровень не требуется переустановка защитного ПО, а для управления используется одна и та же консоль.

https://b2b-compare.kaspersky.ru

*KESB Стандартный позволяет осуществлять поиск уязвимостей, но отсутствует возможность установки исправлений. Стандартный позволяет проводить инвентаризацию ПО и оборудования, но без учета стороннего ПО и инвентаризации сетевого оборудования.

Kaspersky EDR Оптимальный

Kaspersky Endpoint Security for Business

- IT-департамент
- Задачи безопасности в IT
- Компании с распределенной структурой офисов без выделенных специалистов на местах

Kaspersky EDR Optimum

- Информационная безопасность в составе IT
- Небольшой security департамент
- Нет планов по расширению security-штата

Kaspersky Anti Targeted Attack Platform

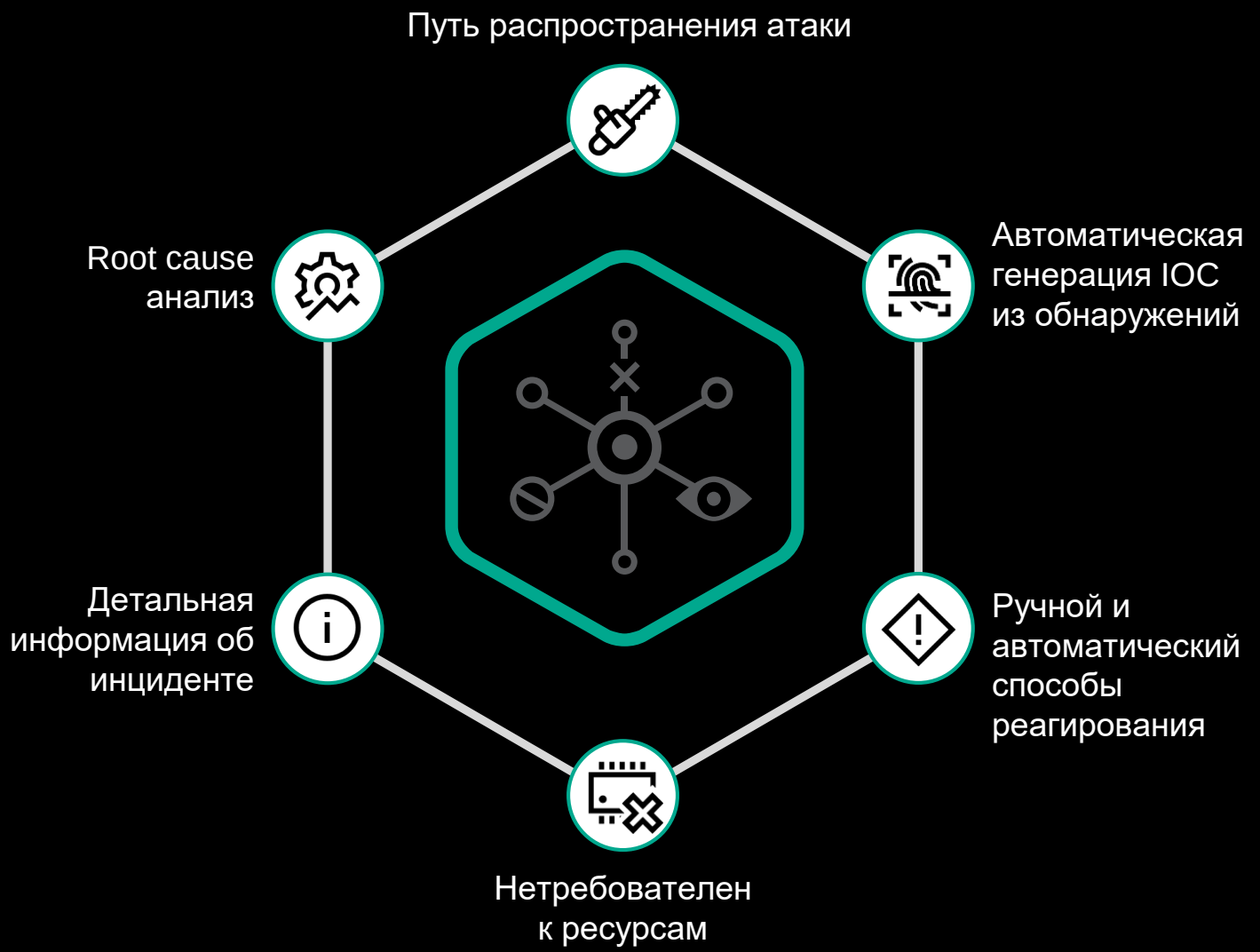
Kaspersky EDR Expert

- Полновесный security-департамент
- SOC/CERT/CSIRT
- Группа расследования инцидентов

Kaspersky EDR Оптимальный

Преимущества решения:

- Простота в установке и использовании
- Обогащение обнаружений KES для возможностей расследования
- Функции реагирования на инциденты
- Реагирование в один клик



Мифы: EDR сложный и затратный

Сложные угрозы

Миф:

Нужен для защиты от сложных угроз, которые актуальны только для больших компаний

Реальность:

- Помогает защититься от различных типов угроз
- Скрытые угрозы атакуют даже малый бизнес

Высокая цена

Миф:

У нас нет бюджета ни для чего кроме антивируса

Реальность:

Мы предлагаем единое решение с простой модернизацией – построенное на нашем EPP

Затратно по времени

Миф:

Специалист не может себе позволить тратить на это время

Реальность:

Правильный инструмент наоборот экономит время, которое иначе пришлось бы тратить на расследование в ручную. А автоматизация и реагирование сразу на группу ПК помогает быть ещё эффективнее.

Kaspersky Security для почтовых серверов

О продукте

Kaspersky Security для почтовых серверов защищает корпоративную почту от вредоносного ПО, программ-вымогателей, спама, фишинга и BEC-атак

Ключевые возможности

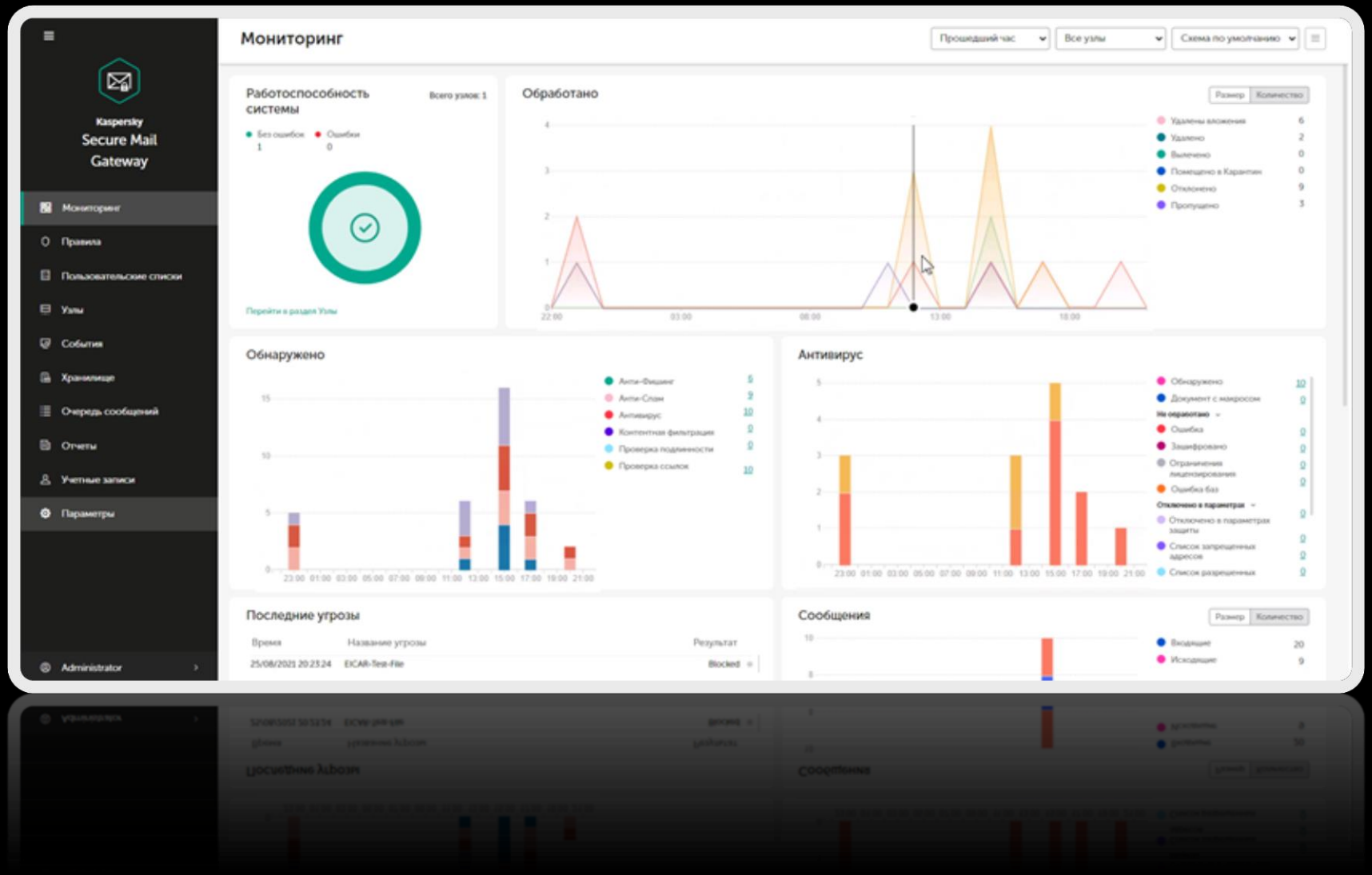
- Продвинутые технологии блокирования вредоносных объектов (интеграция с KATA)
- Защита от фишинга, спама и компрометации корпоративной электронной почты
- Фильтрация почтовых вложений
- Предотвращение попыток обмануть пользователей с помощью методов социальной инженерии
- Соответствие требованиям регуляторов, поддержка отечественных ОС (KLMS)

KSMG 2.0.1

- Дайджест Хранилища – почтовая сводка, которая рассылается по расписанию и содержит информацию о последних полученных письмах, помещенных в персональное Хранилище пользователя.
- Кластерная архитектура для масштабирования решения
- Ролевое разграничение прав доступа, интеграция с AD
- Усилены технологии детектирования (IP-репутация, look-like, выявление спуфинговых атак и т.д.)

KSMG 2.0.1 Веб-интерфейс

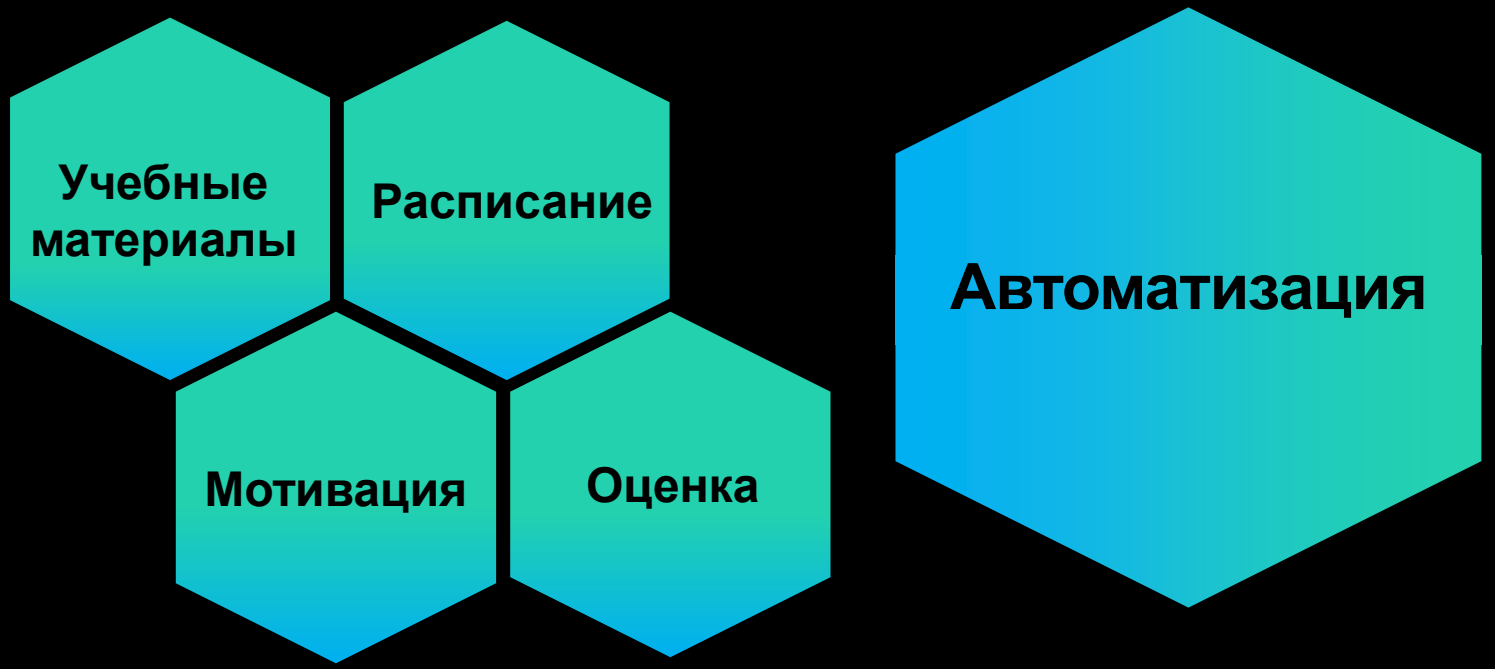
- Панель мониторинга с подробной информацией, видимой сразу
- Управление кластером и его мониторинг
- Защита и настройка MTA События обнаруженные в почтовом трафике
- Статистика обработки трафика
- Раздел резервного копирования сообщений
- Управление ролями и учетными записями
- Реализован Дайджест - почтовая сводка, рассылаемая по расписанию и содержащая информацию о последних полученных письмах, помещенных в Хранилище.



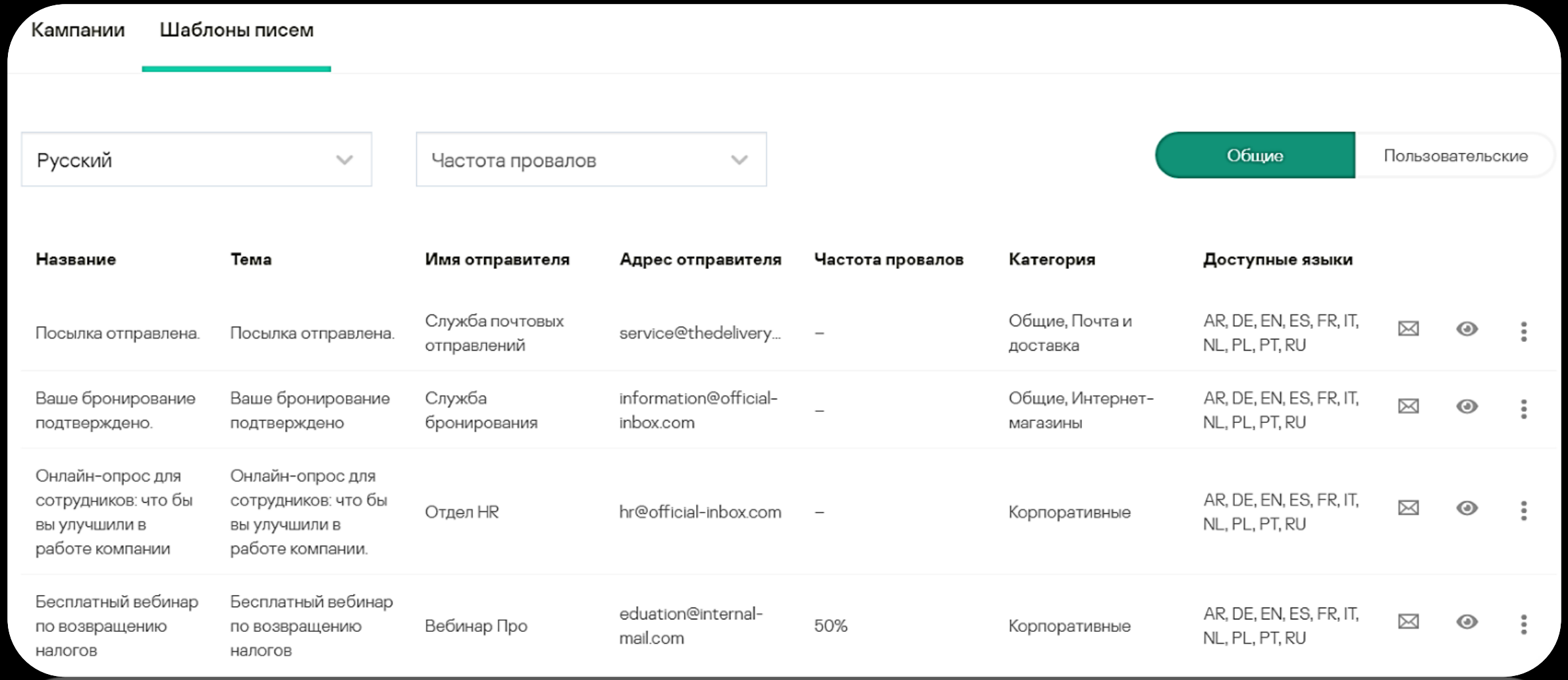
Платформа Kaspersky Automated Security Awareness Platform

Решение, сочетающее в себе эффективность обучения и простоту управления –

www.k-asap.com/ru



Фишинговый симулятор



Название	Тема	Имя отправителя	Адрес отправителя	Частота провалов	Категория	Доступные языки
Посылка отправлена.	Посылка отправлена.	Служба почтовых отправлений	service@thedelivery...	–	Общие, Почта и доставка	AR, DE, EN, ES, FR, IT, NL, PL, PT, RU
Ваше бронирование подтверждено.	Ваше бронирование подтверждено	Служба бронирования	information@official-inbox.com	–	Общие, Интернет-магазины	AR, DE, EN, ES, FR, IT, NL, PL, PT, RU
Онлайн-опрос для сотрудников: что бы вы улучшили в работе компании	Онлайн-опрос для сотрудников: что бы вы улучшили в работе компании.	Отдел HR	hr@official-inbox.com	–	Корпоративные	AR, DE, EN, ES, FR, IT, NL, PL, PT, RU
Бесплатный вебинар по возвращению налогов	Бесплатный вебинар по возвращению налогов	Вебинар Про	eduation@internal-mail.com	50%	Корпоративные	AR, DE, EN, ES, FR, IT, NL, PL, PT, RU

Kaspersky Anti Targeted Attack (KATA)

О продукте

Решение класса NTA/NDR для обнаружения, расследования и реагирования на сложные угрозы и целевые атаки на уровне сети

Ключевые возможности

- Различные варианты интеграции в инфраструктуру (inline, mirror)
- Быстрое масштабирование, поддержка различных схем развертывания
- Встроенный инструментарий для написания своих собственных правил обнаружения(Yara, IDS)
- Дополнение EDR-решений экспертного уровня до класса XDR (защитой уровня сети (NDR))
- Получение по API объектов на проверку из сторонних систем
- Автоматическое и ручное реагирование (Response) на веб и почтовых шлюзах (интеграция с KSMG и KWTS)
- Продвинутые технологии обнаружения на уровне сети (AM-движок, IDS Sandbox)

KATA 5.1

- Для компонента Sandbox поддержана установка пользовательских образов операционных систем Windows и анализ объектов в пользовательских средах.
- Central Node может быть развернут в виде отказоустойчивого кластера.
- В Sandbox поддержана установка операционной системы Astra Linux 1.7 и запуск объектов в этой операционной системе

ПАКЕТ ФУНКЦИЙ	KASPERSKY SECURITY ДЛЯ БИЗНЕСА	KASPERSKY EDR ДЛЯ БИЗНЕСА ОПТИМАЛЬНЫЙ	KASPERSKY EDR (KEDR Expert)*	ПЛАТФОРМА KATA с KEDR
Передовой антивирусный движок	●	●	●	●
Поведенческий анализ, защита от эксплойтов	●	●	●	●
Различные контроли и защита данных	●	●	●	●
Управление уязвимостями и обновлениями	●	●	●	●
Адаптивный контроль аномалий	●	●	●	●
Песочница	●	●	● ●	●
Обнаружение на основе IoC и пользовательских правил		●	●	●
Видимость и анализ первопричин		●	●	●
Поддержка различных мер по реагированию		●	●	●
Сбор и хранение “сырых” данных			●	●
Доступ в портал Kaspersky Threat Intelligence			●	●
Обнаружение угроз на основе сравнения с матрицей MITRE ATT&CK			●	●
Расследование & реагирование на основе рекомендаций			●	●
Базовый инструментарий цифровой криминалистики			●	●
Проактивный поиск угроз и ретроспективный анализ			●	●
Возможности интеграции			●	●
Анализ трафика				●
Обнаружение почтовых и веб-угроз				●
Видимость на уровне сети и рабочих мест				●
Автоматическое реагирование на уровне шлюзов				●

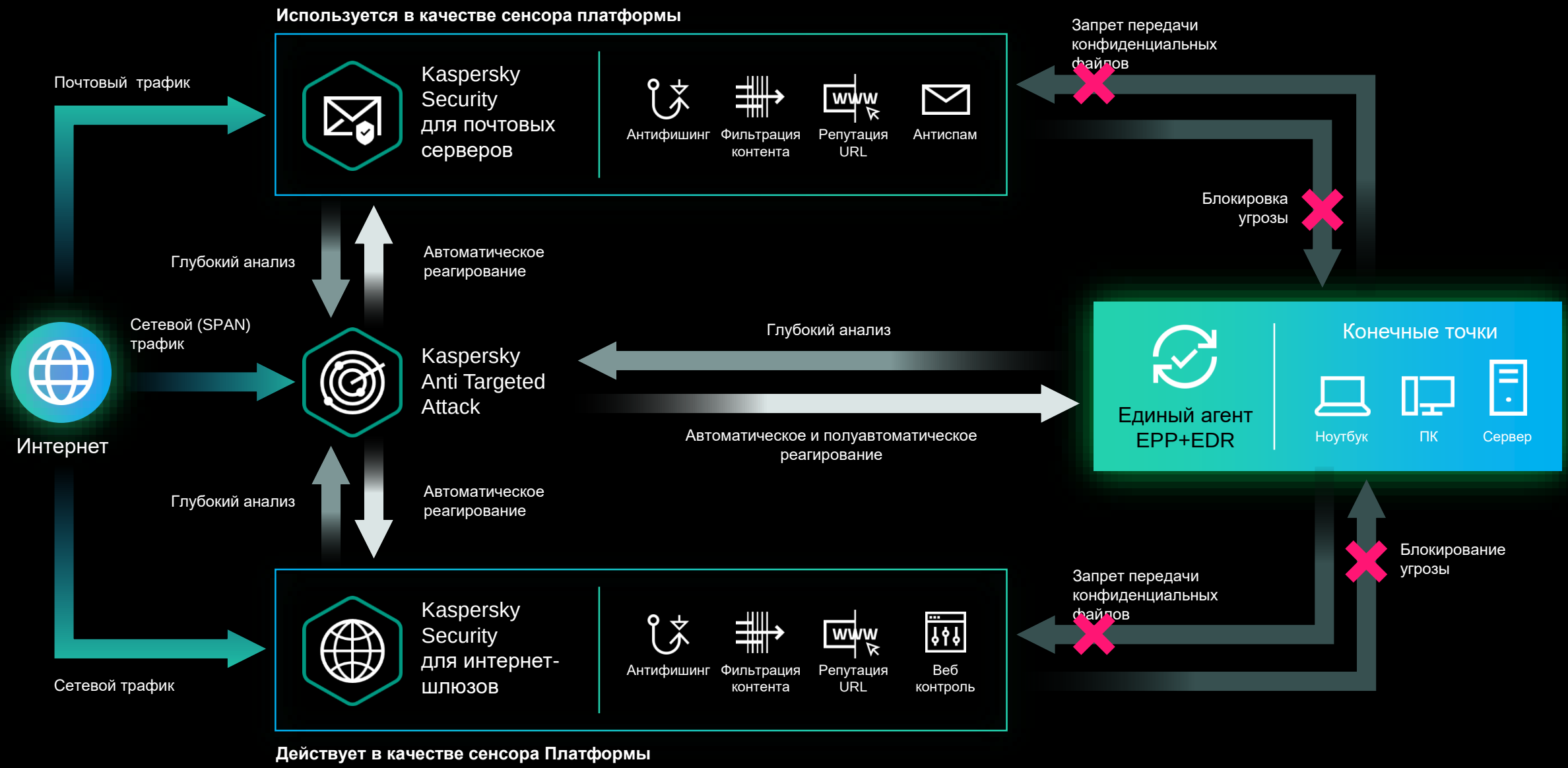
*KEDR имеет два тира в прайс листе Standard и Advanced и одно лишь между ними отличие в функционале – это то, что в первом нет включенной Песочницы

● Включенная функциональность

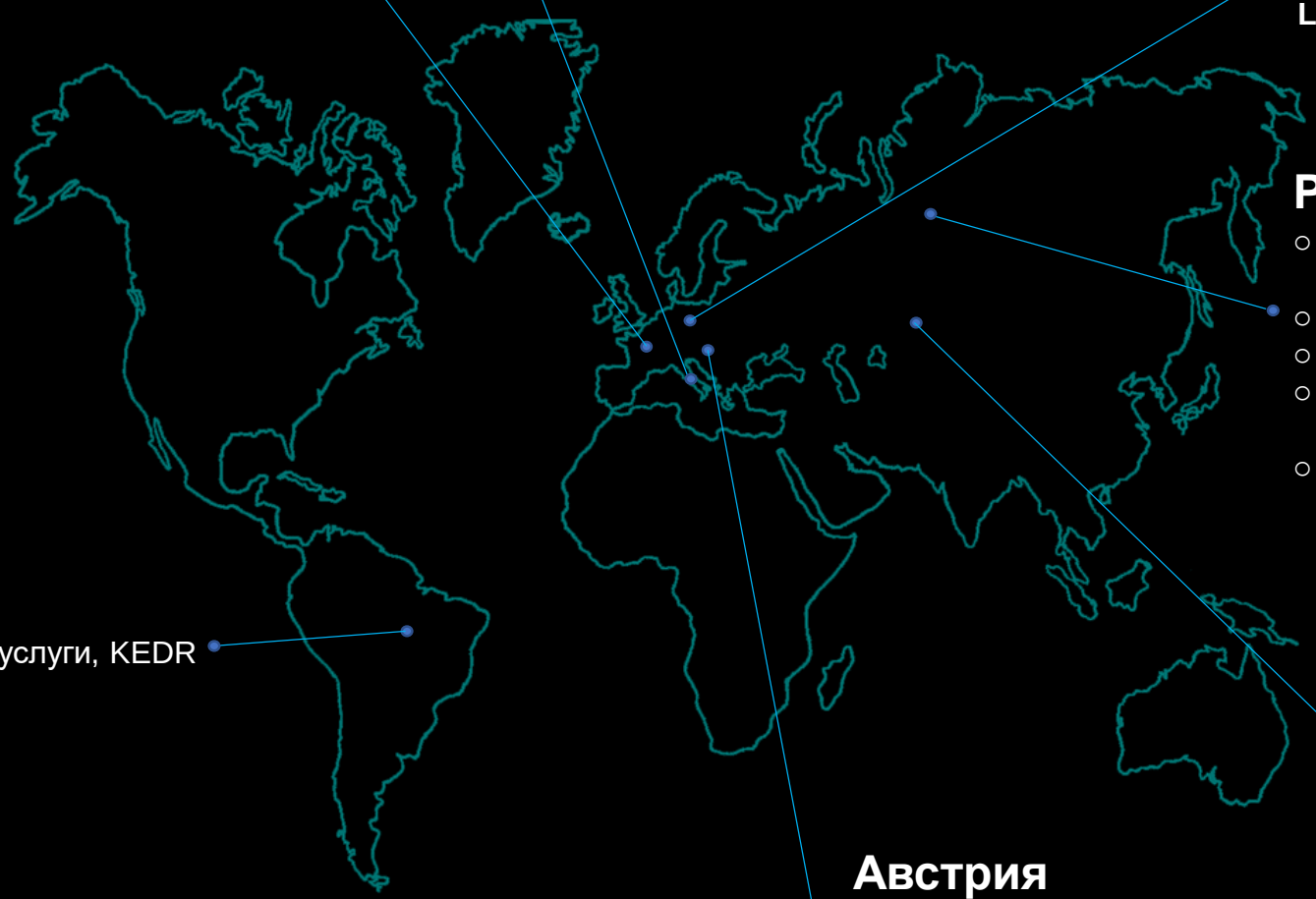
● Расширенная включенная функциональность

● Дополнительно приобретаемый функционал

Автоматическое реагирование с помощью шлюзов



Публичные истории успеха KATA и KEDR



Франция
Weodeo – ИТ и телеком, KEDR

Италия
Ansaldo Energia – энергетика, KEDR
Banca Popolare di Sondrio – финансы и услуги, KATA

Германия
Levigo systems – ИТ и телеком, KEDR

Россия
- **Московский кредитный банк** – финансы и услуги, KATA
- **Магнит** – розничная торговля, KATA
- **РТИ Системы** – промышленность, KATA
- **Правительство Ростовской области** – гос. структуры, KATA
- **Центральная пригородная пассажирская компания** – транспорт, KATA

Бразилия
NEO – финансы и услуги, KEDR

Киргизия
Оптима Банк – финансы и услуги, KATA

Австрия
Donau Chemie Group – промышленность, KEDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

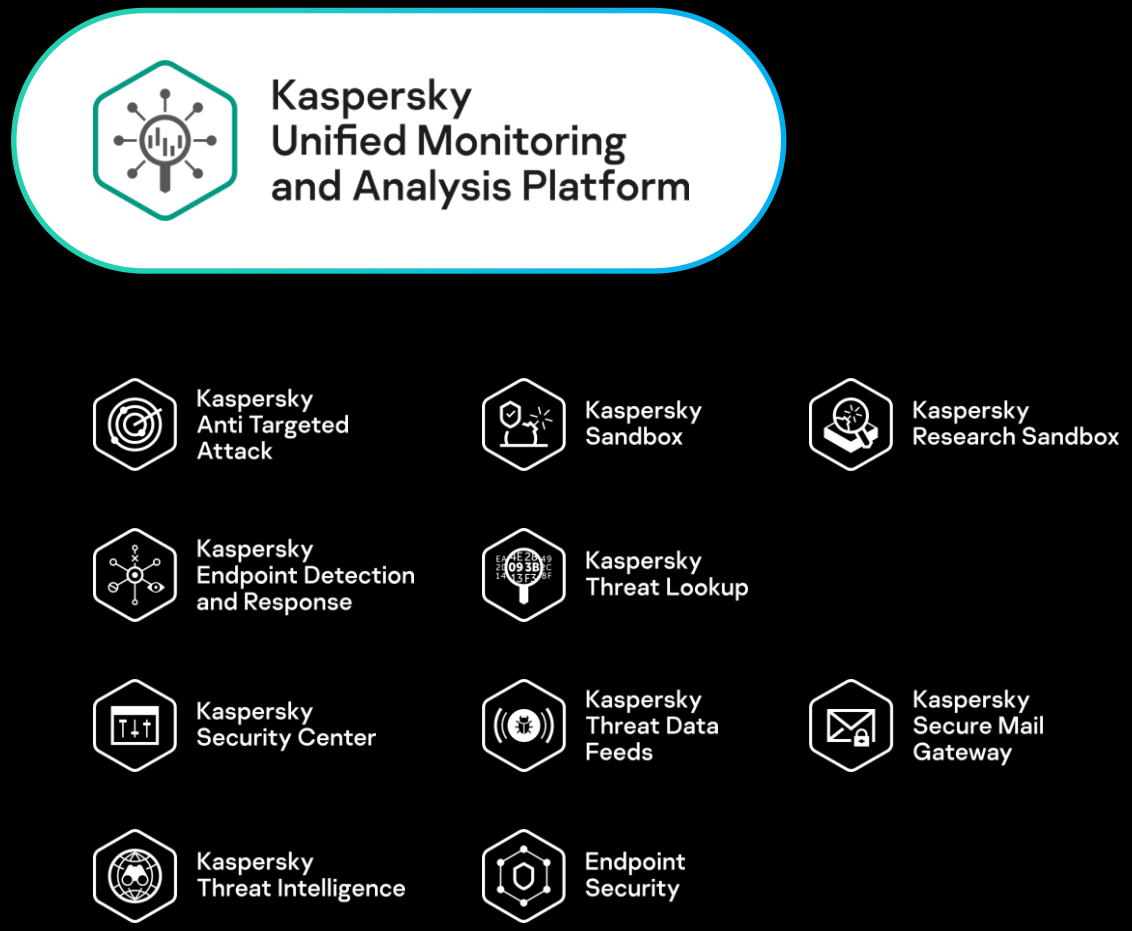
О продукте

KUMA SIEM - это центральный элемент единой платформы безопасности от «Лаборатории Касперского», который взаимодействует как с решениями ЛК, так и с разработками сторонних поставщиков

Ключевые возможности

- Ситуационная осведомлённость и аналитика - дашборды и отчёты по актуальному состоянию ИБ для отслеживания трендов (C-level) и операционной работы по поиску аномалий
- Мониторинг безопасности - непрерывная корреляция потока событий от источников для выявления инцидентов ИБ
- Реагирование на инциденты - единая консоль позволяет обогатить карточки инцидентов дополнительной информацией (по индикаторам компрометации, активам, пользователям) и запустить задачи реагирования через KES, EDR, ASAP и другие решения
- Поддержка отечественной ОС (Astra Linux)
- Проактивный поиск угроз - быстрый поиск ClickHouse по всей собранной информации с использованием возможностей SQL-запросов или применение ретроспективной корреляции для выявления подозрительных цепочек событий
- Соответствие требованиям - KUMA имеет сертификат ФСТЭК, свидетельство о регистрации, включена в реестр отечественного ПО и позволяет выполнять требования 187-ФЗ, приказа ФСТЭК России № 239, рекомендаций ЦБ и других НПА. Интеграция с НКЦКИ.
- Автоматическое обновление репозитория для получения пакетов с новыми правилами корреляции и коннекторами к источникам логов.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



- **Производительность**

  300k+ EPS на одну ноду

- **Низкие системные требования**

- **Гибкая архитектура**

  Современная микросервисная архитектура

- **Интеграция «из коробки»**

  С решениями «Лаборатории Касперского» и сторонних поставщиков

Истории успеха

ФОСАГРО®

Крупнейший поставщик всех видов удобрений на российском рынке

“ Благодаря комплексному подходу нам удалось не только построить надежную систему безопасности, в основе которой отечественные технологии, но и достигнуть главной цели – заложить основу ситуационного центра

Сергей Черкасов, заместитель директора по экономической безопасности АО «Апатит» (группа ФосАгро)

ТГК-2 ТЕРРИТОРИАЛЬНАЯ ГЕНЕРИРУЮЩАЯ КОМПАНИЯ №2

Одна из крупнейших теплоэнергетических компаний Северо-Западного и Центрального округов России

“ По своим техническим возможностям KUMA не уступает продуктам мировых лидеров SIEM, быстро разворачивается, легко масштабируется и управляется из единой консоли

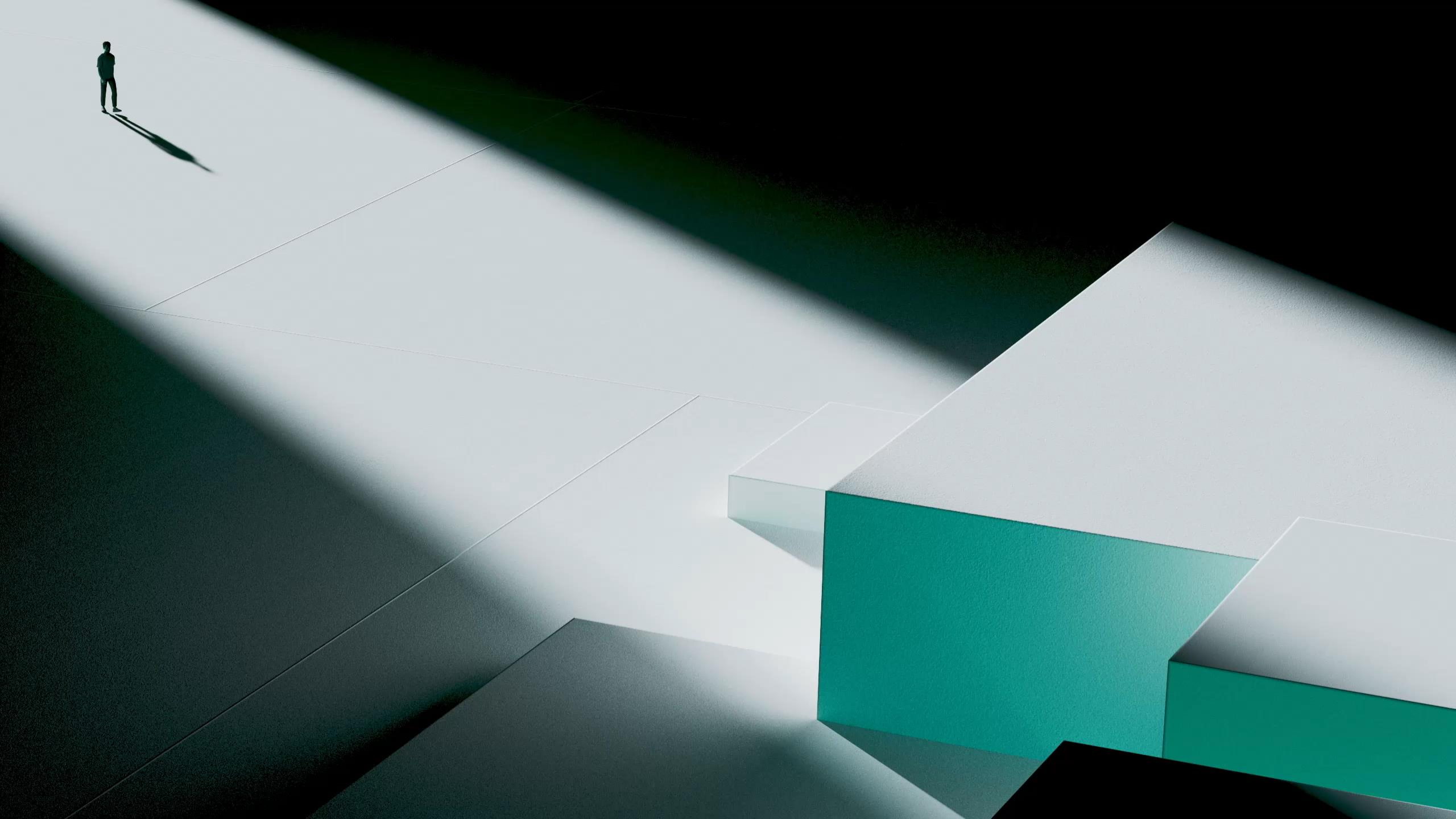
Александр Суворов, начальник отдела информационной безопасности ПАО «ТГК-2»

НОВОСТАЛЬ-М

Металлургический холдинг, основными активами которого являются Абинский Электрометаллургический Завод и Металлургический Завод Балаково

“ Использование двух взаимосвязанных линеек решений для корпоративного и промышленного сегмента от одного вендора позволило нам получить синергетический эффект в укреплении безопасности и простоте управления

Артём Садовский, начальник управления информационной безопасности холдинга «Новосталь-М»

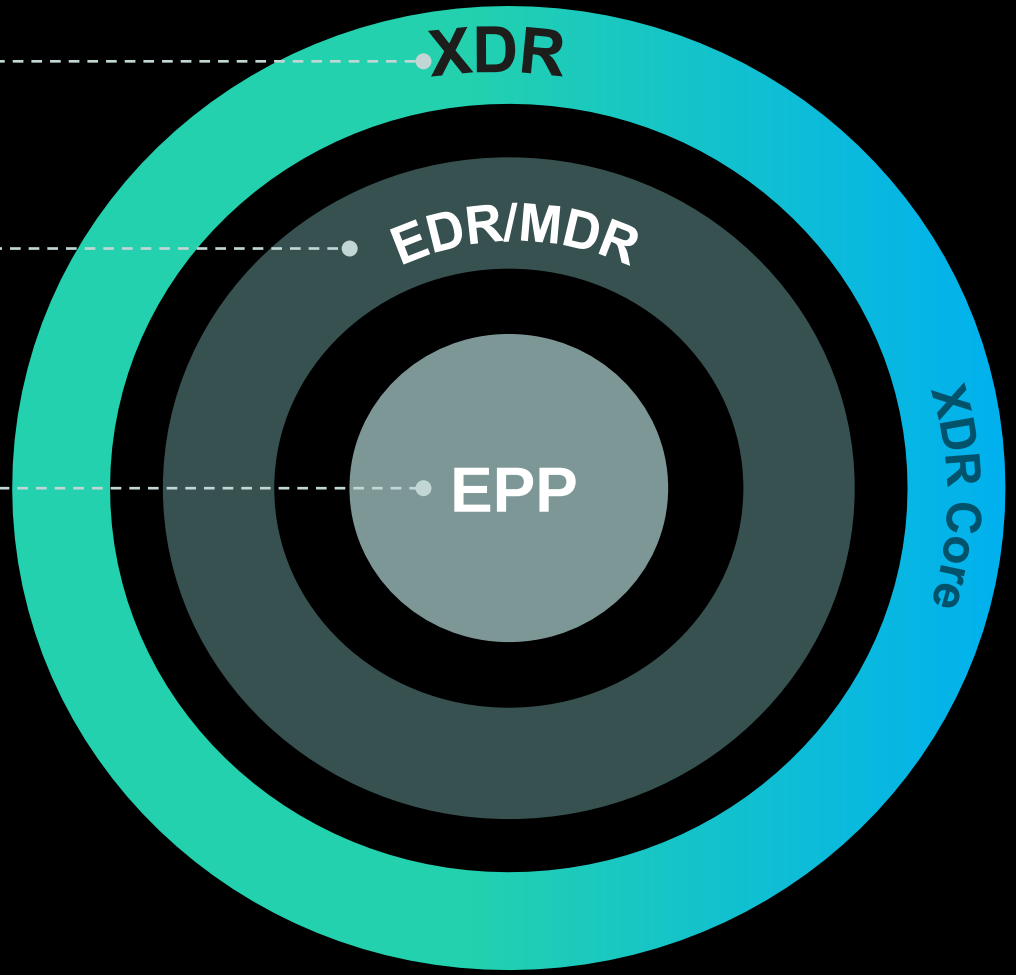


Kaspersky Symphony. Уровни защиты

Kaspersky Symphony
XDR

Kaspersky Symphony
EDR / MDR

Kaspersky Symphony
Security

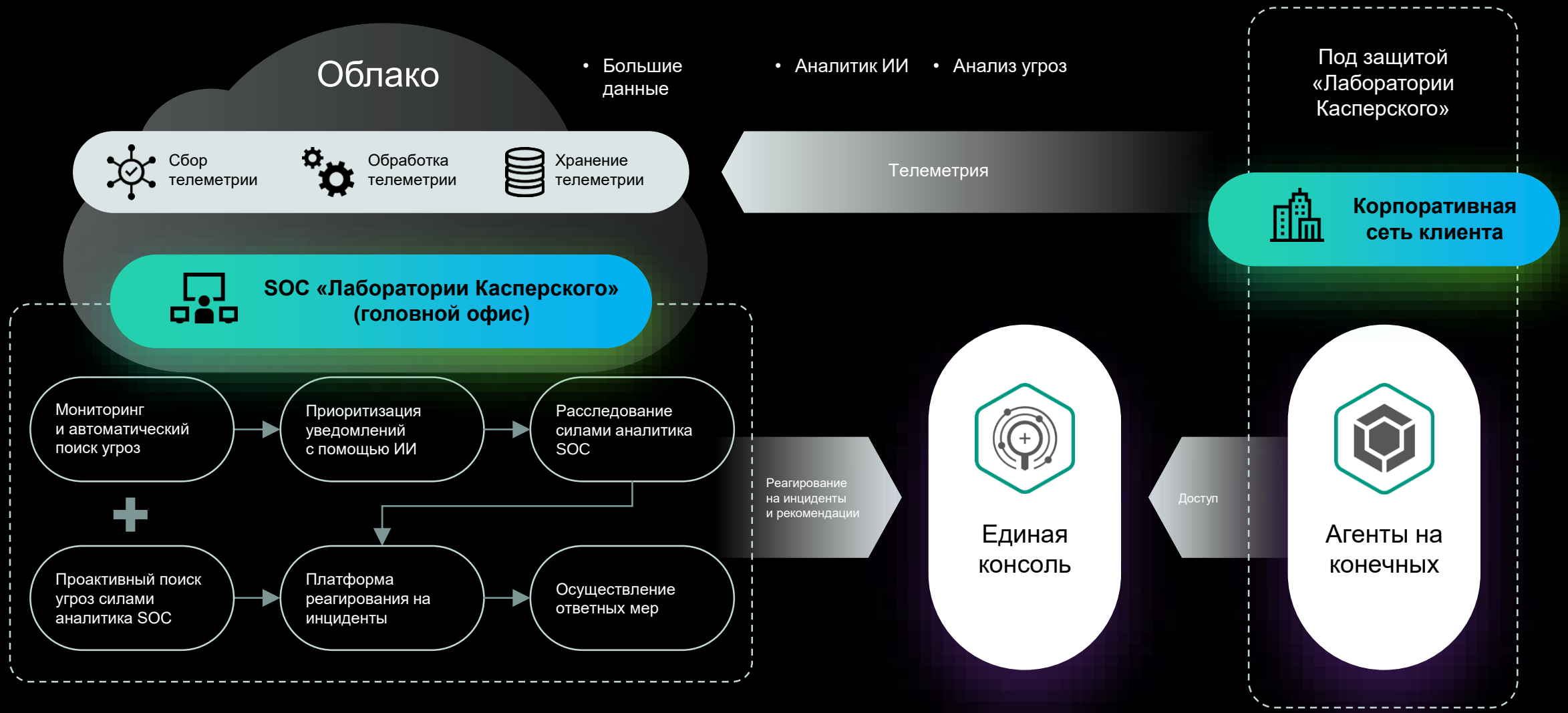


Функциональное сравнение уровней Kaspersky Symphony

Лицензирование по устройствам

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				●

Kaspersky Managed Detection and Response

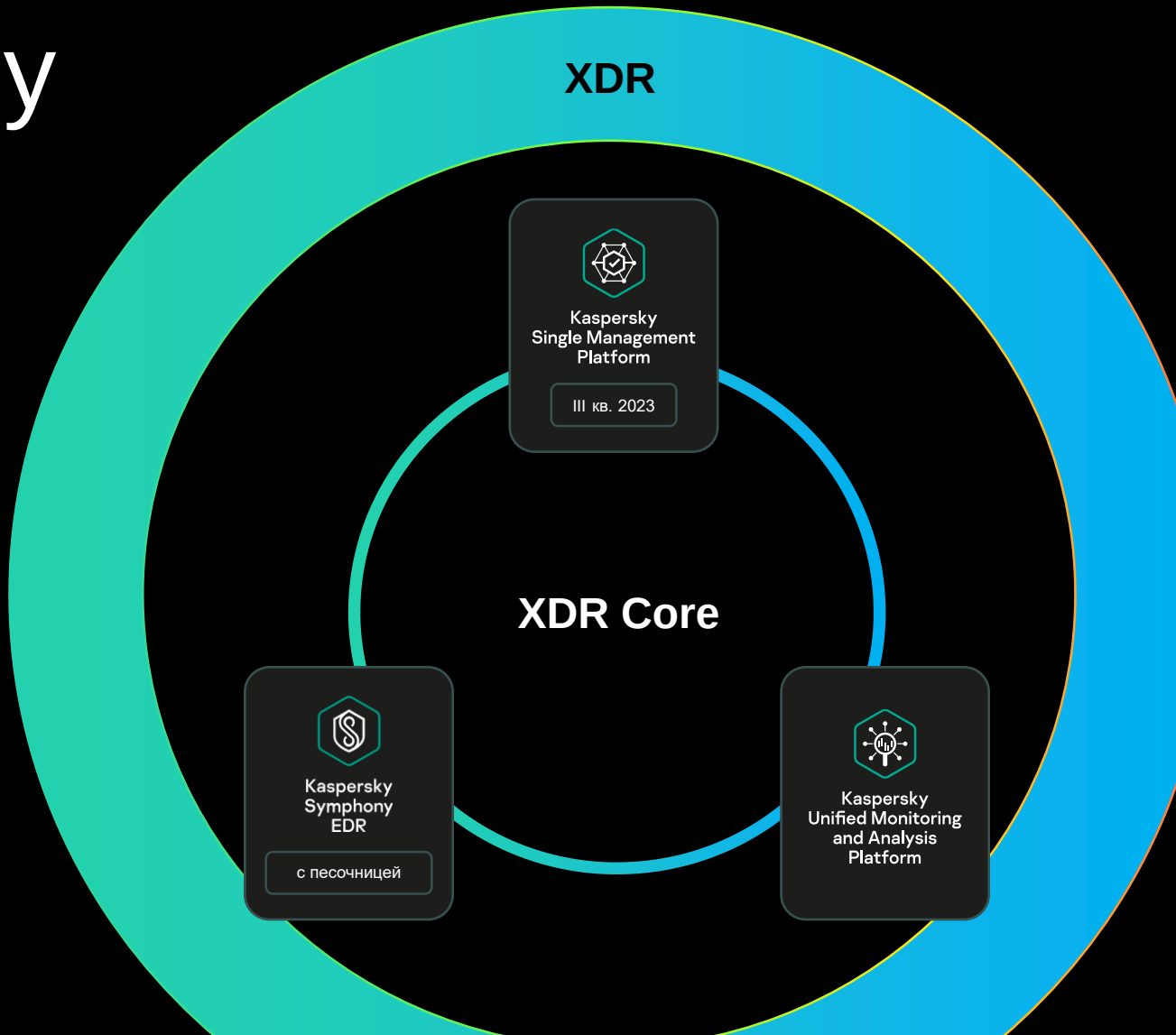


Kaspersky Symphony

Лицензирование по устройствам

Kaspersky Symphony XDR Core

Ядро комплексной платформы XDR, которое включает в себя ключевой набор продуктов для выстраивания защиты класса XDR. Решение идеально подходит организациям, для которых важна гибкость в построении мощной XDR защиты: как на базе всех продуктов от Kaspersky, так и добавления сторонних.

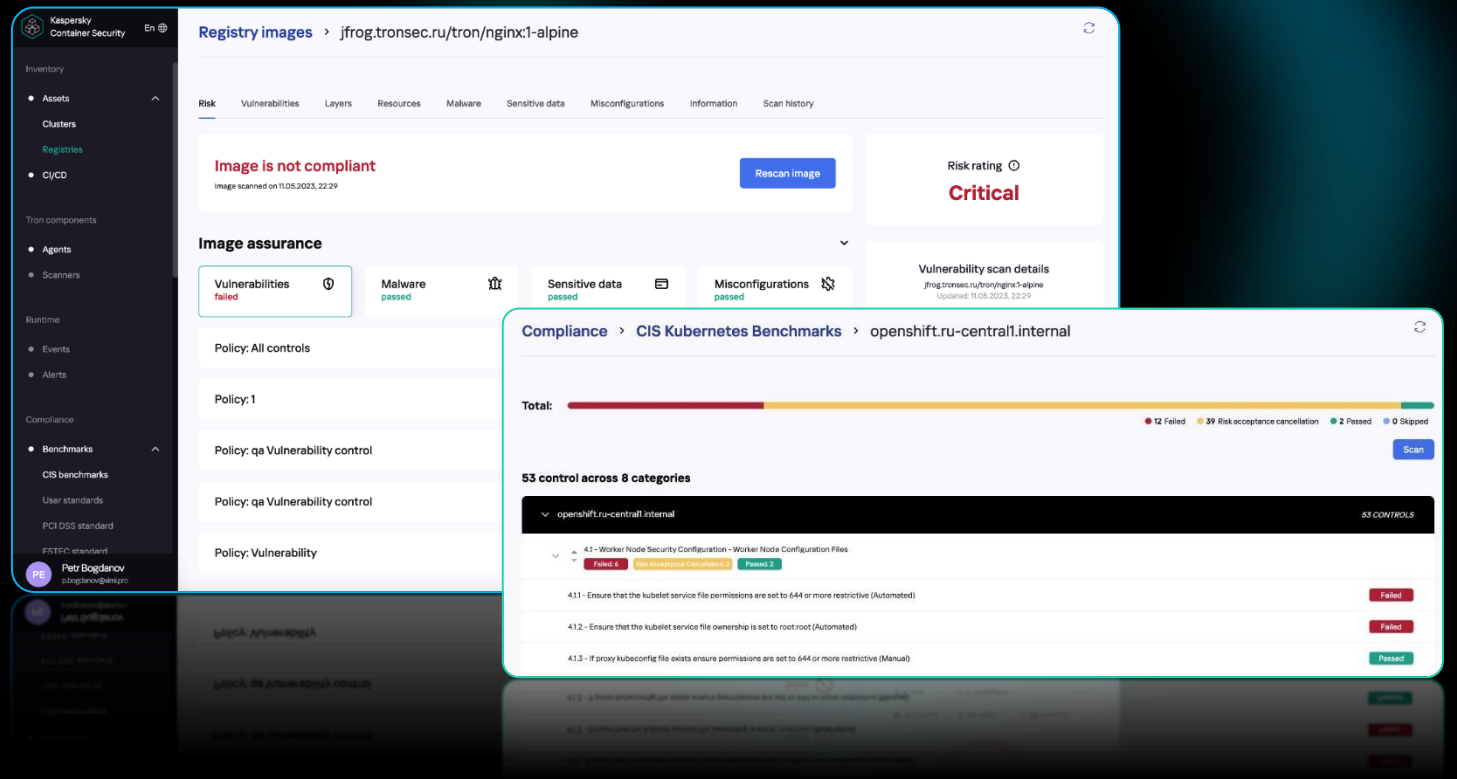


Другие решения для киберустойчивости бизнеса

- Kaspersky Threat Data Feeds
- Kaspersky Secure Mobility Management
- Kaspersky SD-WAN
- Kaspersky Scan Engine
- Kaspersky Antidrone
- Kaspersky Managed Detection and Response

Kaspersky Container Security

Решение контейнерной безопасности



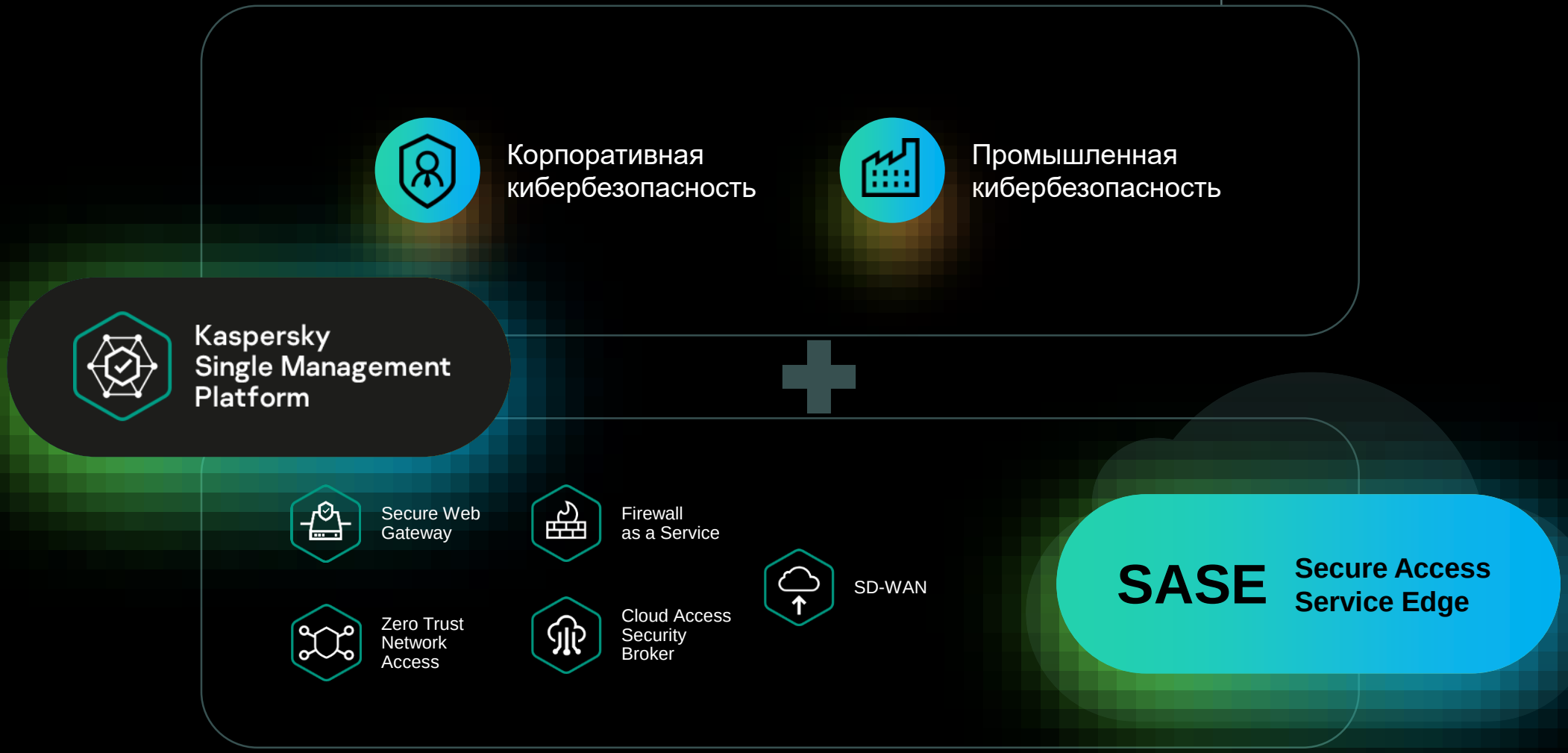
Закрывает проблемы безопасности контейнерных сред на всех этапах

KCS обеспечивает безопасность всех компонентов контейнерных платформ: образы, реестры образов, оркестраторы, контейнеры, ОС хоста

Позволяет интегрироваться в процессы безопасной разработки

Встраивается в CI pipelines и интегрируется в инфраструктуру

Наши дальнейшие планы



Спасибо!

kaspersky АКТИВИРУЙ БУДУЩЕЕ