kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Дмитрий Митюшин

Менеджер по развитию бизнеса,
АО «Лаборатория Касперского»

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

kaspersky

Применение решений на базе KasperskyOS в промышленности

Дмитрий Митюшин
Менеджер по развитию бизнеса KasperskyOS
CISSP, CISM

Kaspersky Industrial Cybersecurity Conference 2020

> Я верю, что концепция кибериммунитета – это будущее защиты OT и IoT

Евгений Касперский

Строим безопасный мир

Реализация принципа кибериммунности

О концепции
Наше видение нового подхода к киберзащите

О платформе KasperskyOS
Основные принципы построения защищенных систем на доверенной платформе

О первых решениях
Направления разработки и первые решения, готовящиеся к выпуску

kaspersky

Концепция кибериммунности

Подход, обеспечивающий надежную защиту от любых атак — известных и пока неизвестных

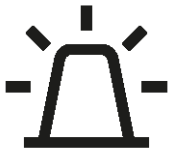
Текущее состояние борьбы с IT-угрозами: обобщенный сценарий

Злоумышленник находит уязвимость

К сожалению, это не очень сложно

Уязвимость становится публичной

Средства распространения информации дешевы и общедоступны



ИБ-сообщество реагирует мгновенно

Это сложно, дорого, долго и зачастую невозможно

Злоумышленники действуют в легких условиях и определяют правила игры.
ИБ-индустрия всегда реактивно отвечает на действия злоумышленников.

kaspersky

Правила игры меняются

Наложенные и реактивные меры защиты менее эффективны, чем встроенная защита

Необходимо создать окружение, которое

- не позволит программам исполнить недекларируемые возможности (код)
- предотвратит эксплуатацию уязвимостей

Идеальные условия для создания защищенных решений

Действительно надежную систему можно построить только на доверенном фундаменте

- Минимальный объем доверенной кодовой базы среды исполнения

- Механизмы безопасности – часть доверенной кодовой базы:
  - Должны быть максимально простыми
  - Отделены от функциональных компонентов
  - Могут применяться ко всем операциям
  - Не ограничивают реализацию необходимых мер защиты
  - Позволяют адаптироваться под новые угрозы на всем жизненном цикле
  - …

Безопасность должна основываться на описании корректного поведения, а не на запрете некорректного

kaspersky

Кибериммунность – способ построения безопасной ИС

Требуется использовать методологию создания доверенных решений:

- Формулирование целей предположений безопасности
- Анализ угроз и рисков
- Проектирование архитектуры:
  - разделение функциональности по доменам
  - определение интерфейсов, удобных для контроля
  - задание политик безопасности
- Валидация и верификация итогового решения

Архитектурное проектирование и опора на встроенные механизмы – основные инструменты для достижения кибериммунности

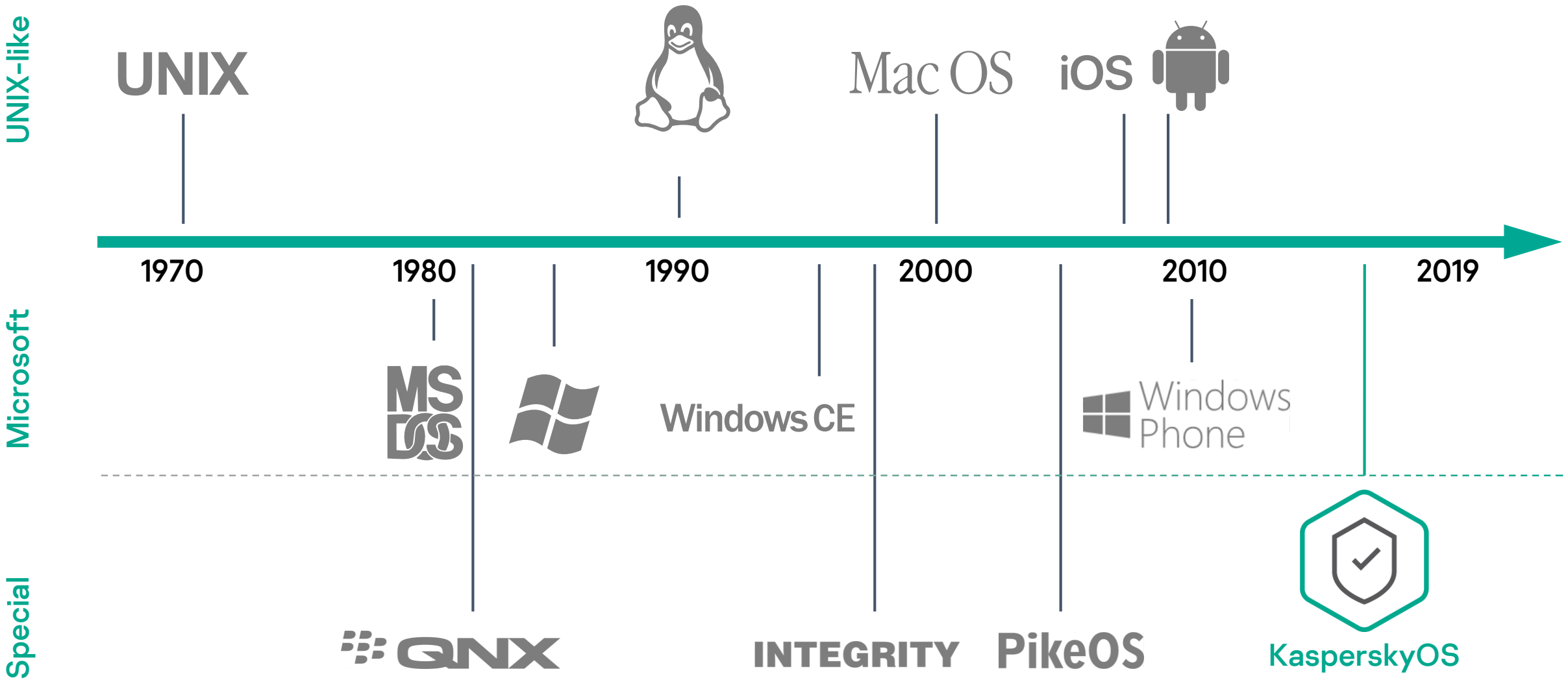
Наш подход позволяет разрабатывать безопасные решения с существенными гарантиями дешевле, чем при использовании других подходов

kaspersky

KasperskyOS

Построение безопасной среды, в которой
уязвимости и ошибки не будут представлять угрозы

KasperskyOS – операционная система специального назначения



KasperskyOS – основа кибериммунных систем будущего

- Минимально возможный размер кода позволяет получить очень высокий уровень гарантий защищенности
- Минимизация уязвимостей в ключевом элементе информационной системы
- Исключение риска целых классов кибератак
- Надежность и прогнозируемость работы

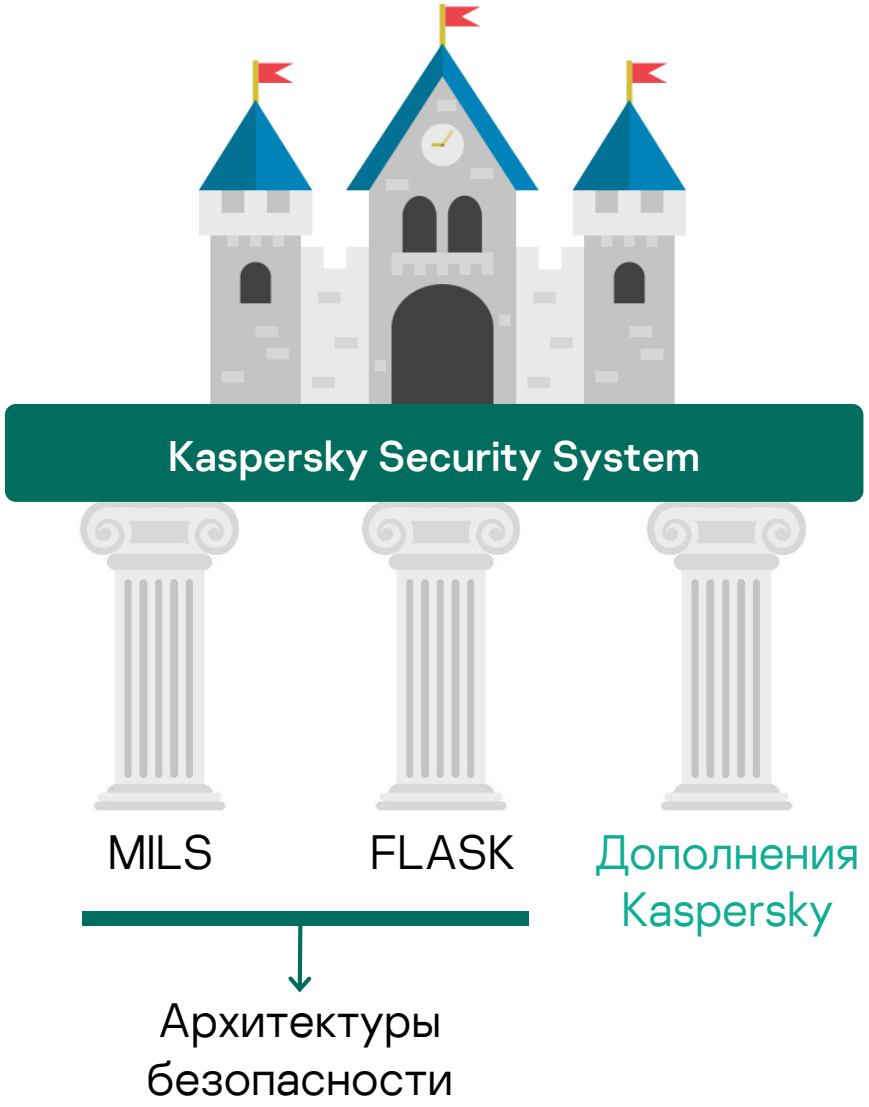
Полностью отечественная разработка без использования сторонних библиотек и кода в ядре

KasperskyOS®

Микроядро нашей ОС состоит всего из нескольких десятков тысяч строк кода

kaspersky

Реализация подсистемы безопасности



Декларативное описание архитектуры решения и разрешенных взаимодействий

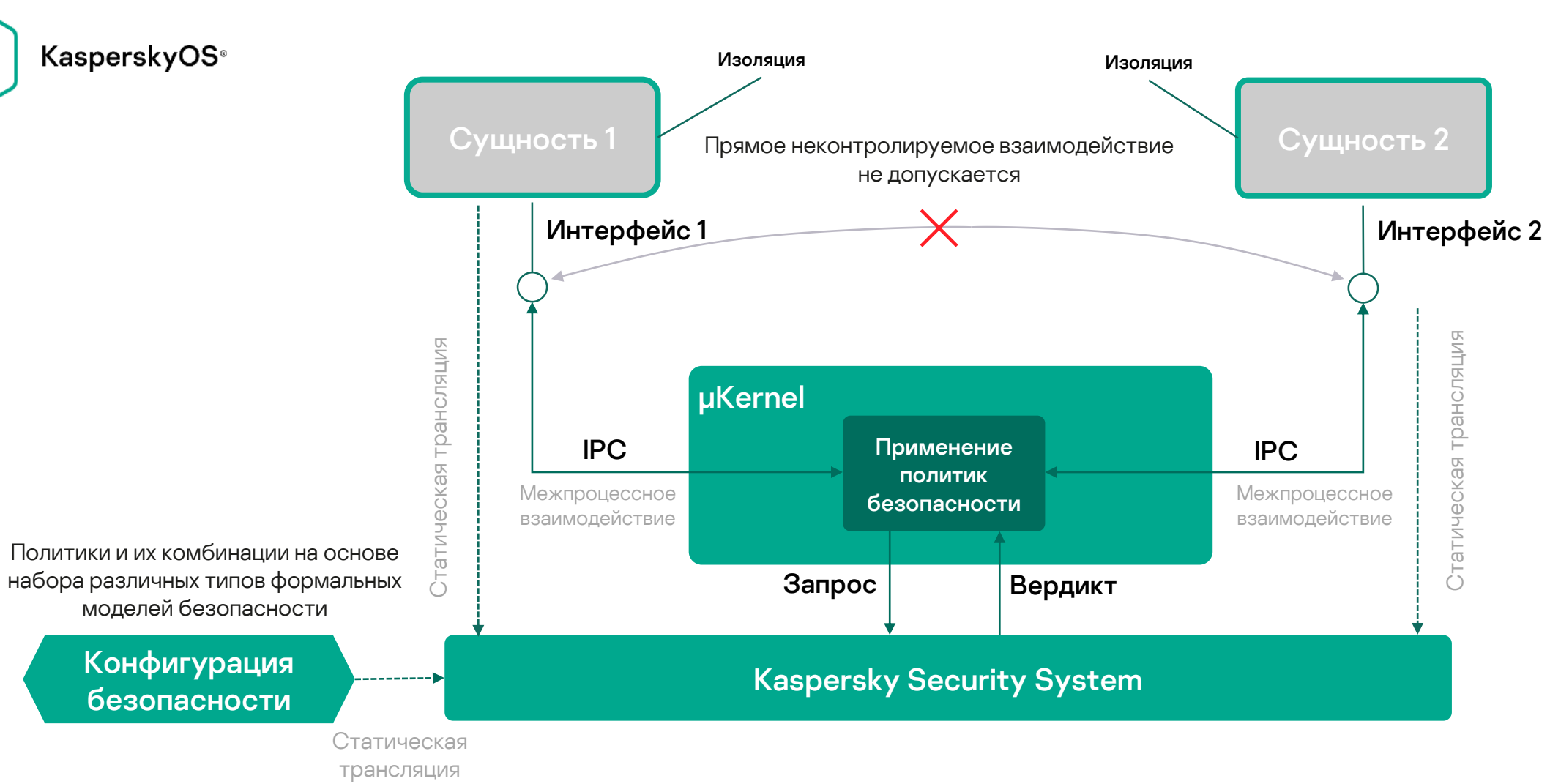
Типизированные интерфейсы межпроцессного взаимодействия (IPC)

Гибкая архитектура политик безопасности, функции безопасности отделены от функциональной логики ИС

Генерация кода компонента принятия решений безопасности на основе заданных политик

kaspersky

Основные принципы архитектуры KasperskyOS



kaspersky

Архитектура приложений в KasperskyOS

KasperskyOS разработана **для встроенных ИС** с высокими требованиями к безопасности.
Одна из целей – обеспечение безопасности сложных систем с использованием минимума доверенных компонентов.

Запрещено все, что не разрешено

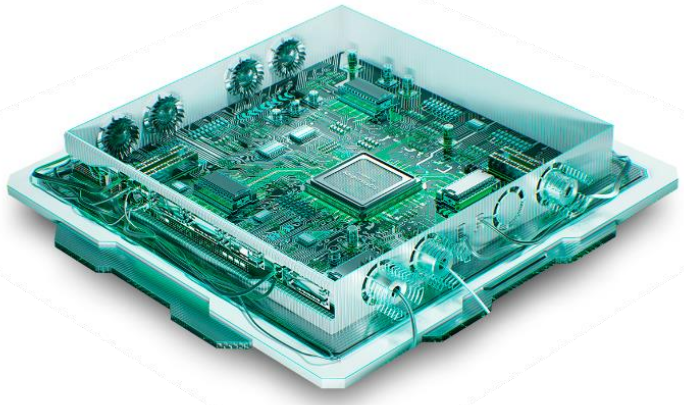
kaspersky

KasperskyOS: направления развития и применение

ПРИМЕНЕНИЕ:

- Интернет вещей (IoT) и умный город
- Транспорт и транспортная инфраструктура
- Промышленная инфраструктура
- Телекоммуникационное оборудование
- Инфраструктура виртуальных рабочих столов (VDI)
- Корпоративные экранные устройства для сотрудников

KasperskyOS®



- Умные города, IoT, энергетика, дорожное движение
- Автомобили, автобусы, поезда
- IoT-гейтвеи, IIoT, SCADA, PLC
- Коммутаторы, маршрутизаторы, Wi-Fi, МЭ
- Тонкие клиенты
- Мобильные телефоны, планшеты
- OEM

kaspersky

Первые продукты на базе KasperskyOS для промышленности

Kaspersky
IoT Secure Gateway β*

Kaspersky
Thin Client β*

* *Текущие версии продуктов предназначены для некоммерческого тестирования и пилотирования*

kaspersky

Kaspersky IoT Infrastructure Security

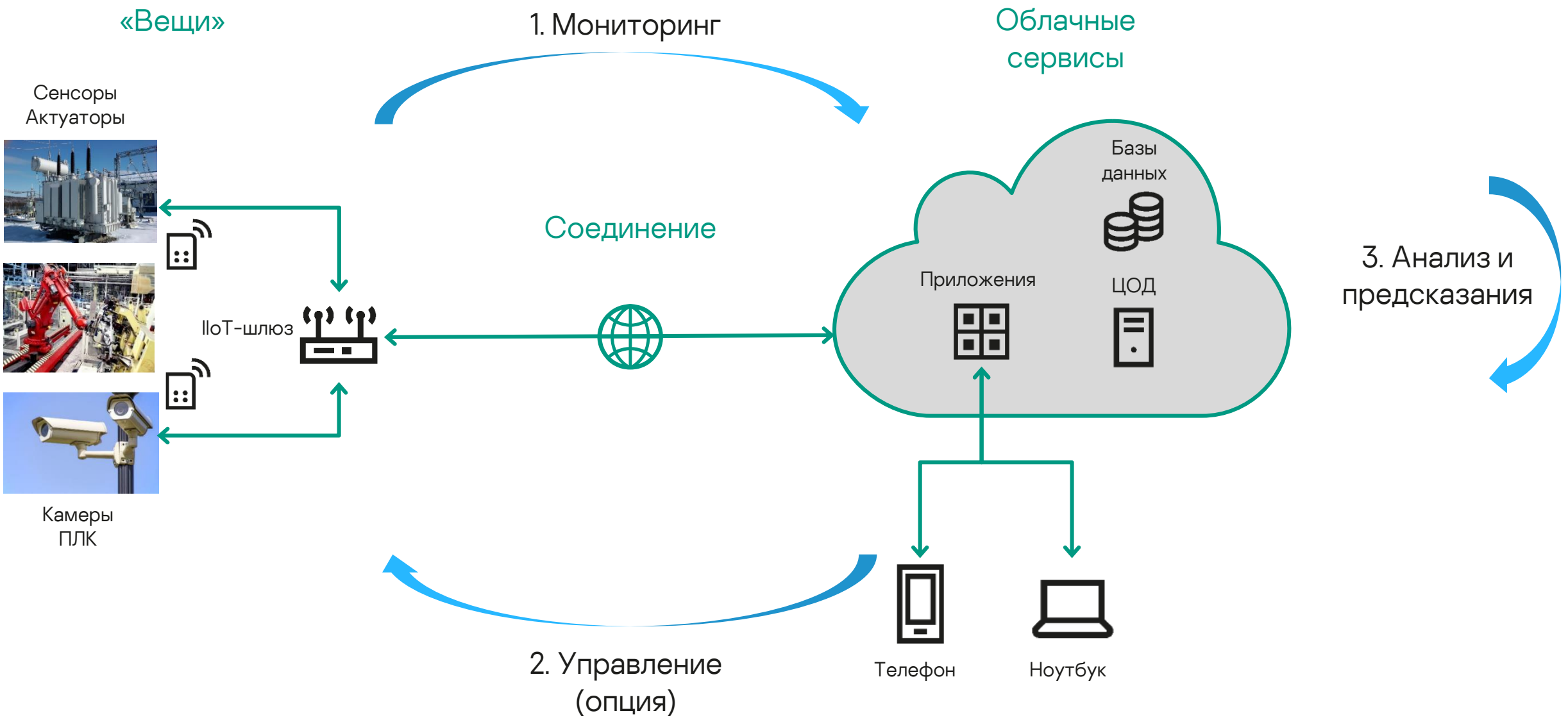
Решение на базе KasperskyOS для построения защищенной IoT-инфраструктуры

Почему нужно обеспечивать защиту IoT/IIoT

Последствия атак:

- Потеря приватности
- Кража личных данных
  и конфиденциальной информации
- Финансовые потери
- Промышленный шпионаж
- Аварии на объектах инфраструктуры
- Потеря контроля над устройствами
  (включение в ботнеты и майнинг криптовалюты)
- Использование IoT-устройств в качестве
  бэкдоров для доступа к корпоративной сети
- Потери производительности
- Перерасход ресурсов
- Потеря качества товара

Типовая структура IoT/IIoT

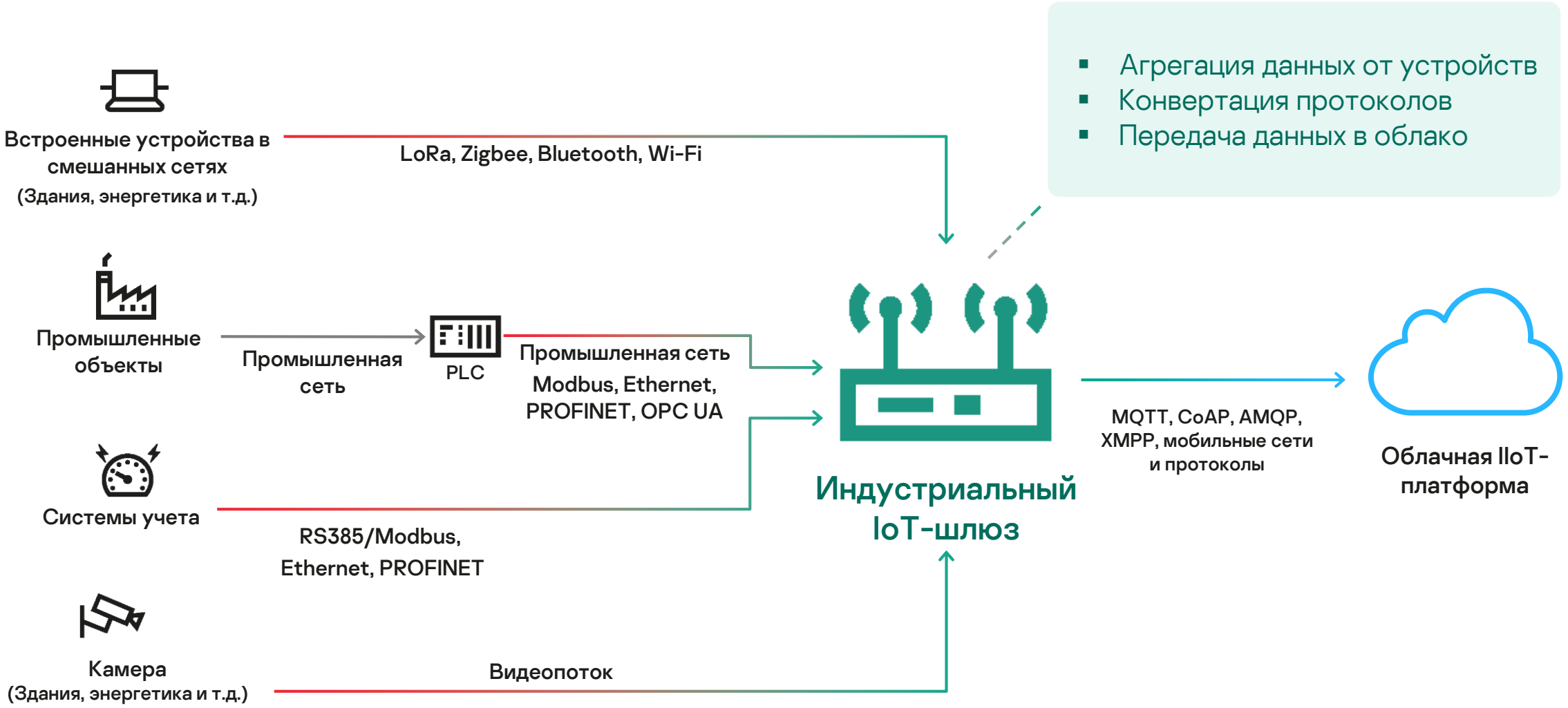


kaspersky

Потенциальные направления атак на IoT/IIoT

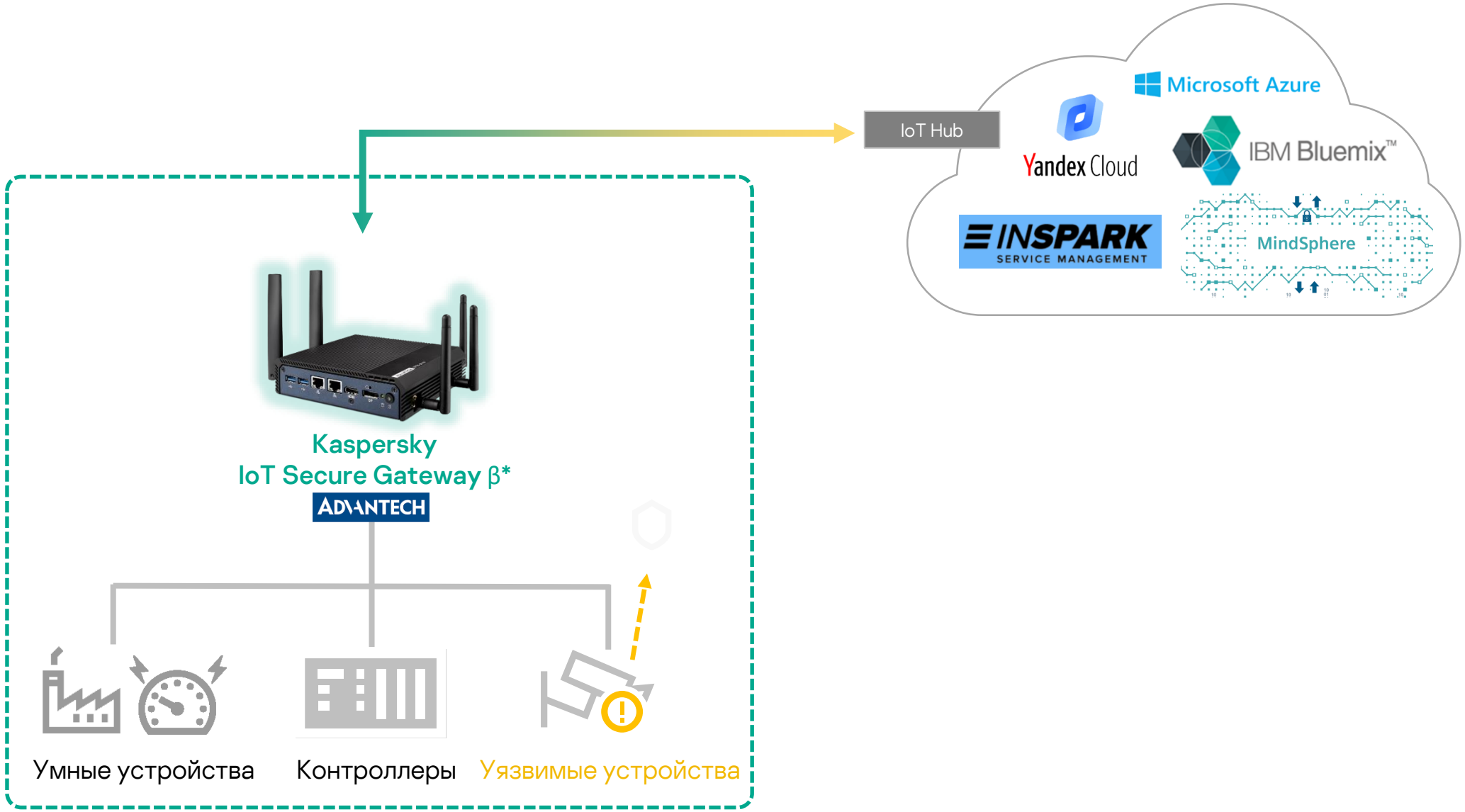
kaspersky

Что такое IoT-гейтвей?



kaspersky

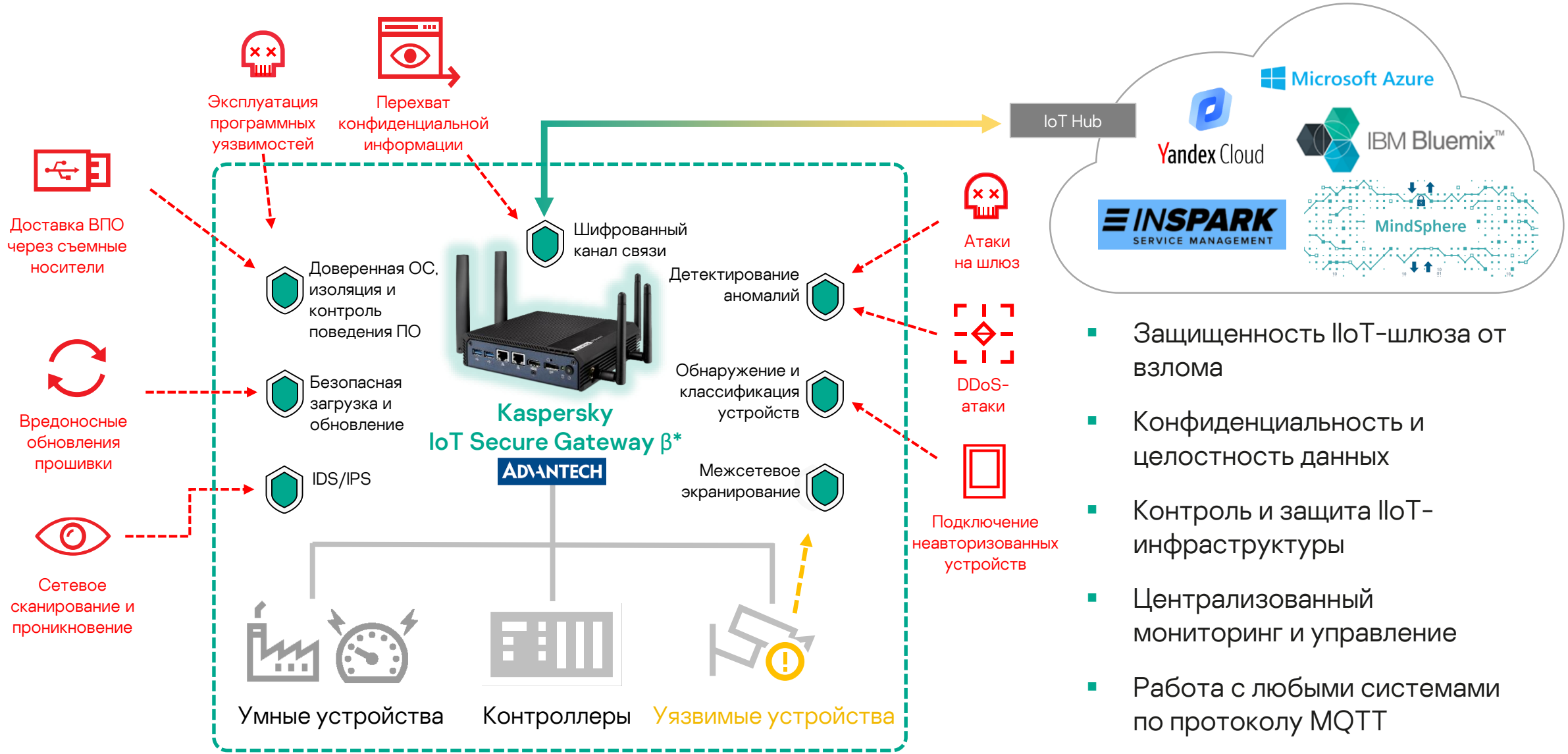
Kaspersky IoT Secure Gateway β*



* Текущая версия продукта предназначена для некоммерческого пилотирования

kaspersky

Kaspersky IoT Secure Gateway β*



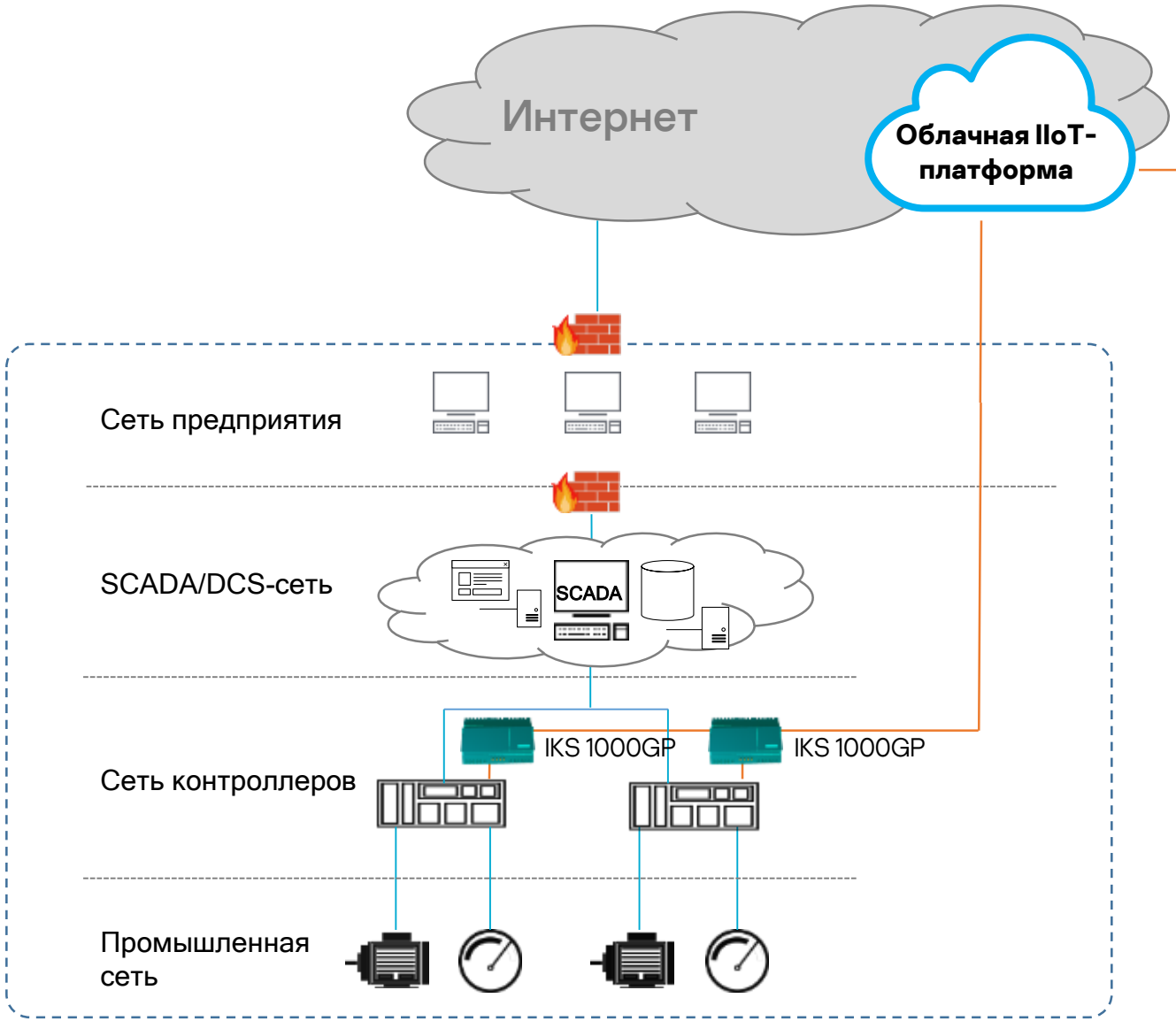
- Защищенность IIoT-шлюза от взлома
- Конфиденциальность и целостность данных
- Контроль и защита IIoT-инфраструктуры
- Централизованный мониторинг и управление
- Работа с любыми системами по протоколу MQTT

* Текущая версия продукта предназначена для некоммерческого пилотирования

kaspersky

Решения для Industry 4.0 & IIoT

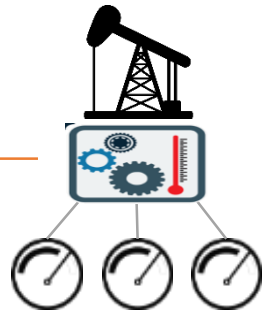
АДАПТИВНЫЕ ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ



Удаленный мониторинг промышленного оборудования

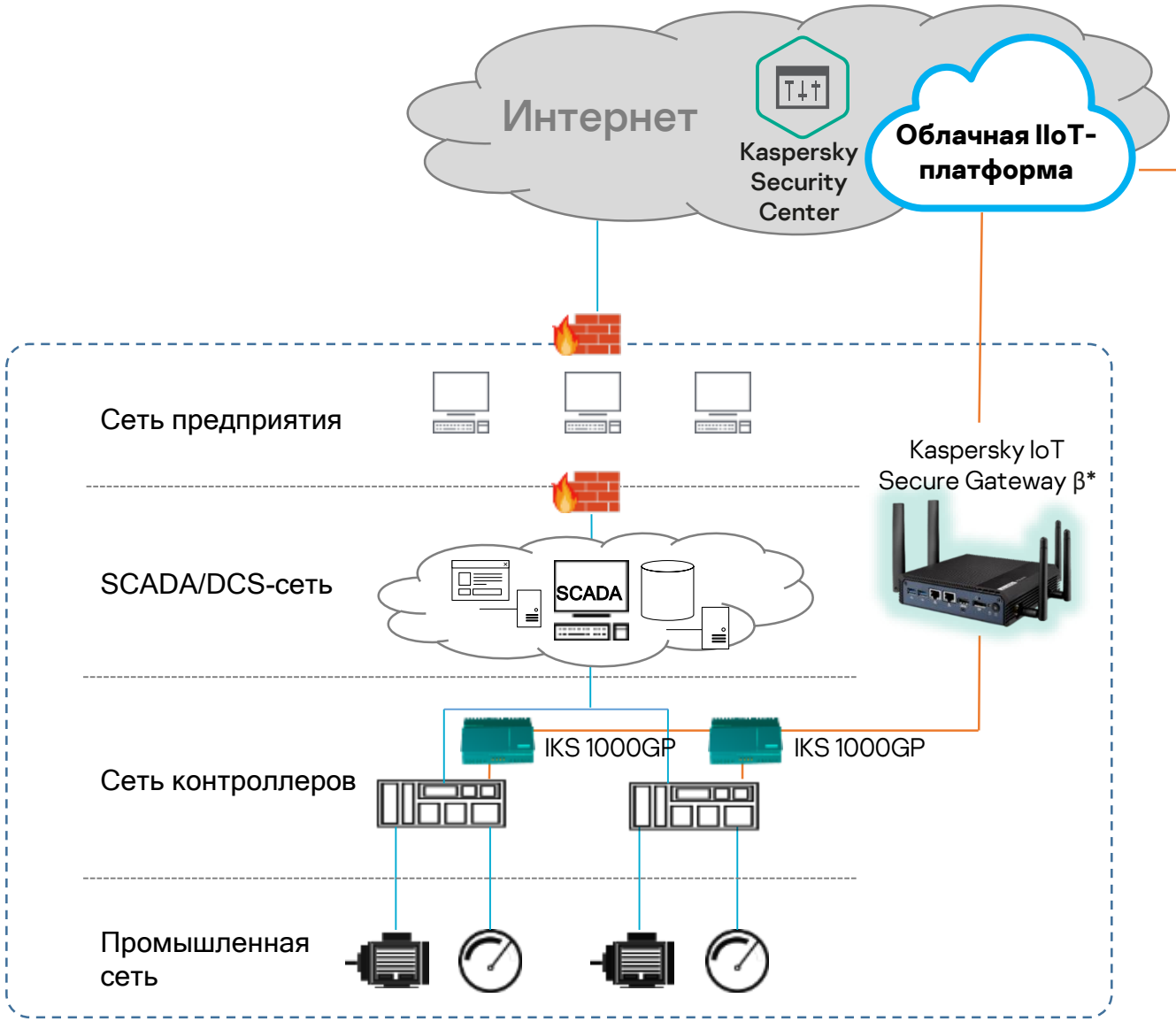
- Независимое безопасное подключение к уровню ПЛК

Удаленное производство



kaspersky

Решения для Industry 4.0 & IIoT



Kaspersky IoT Secure Gateway

АДАПТИВНЫЕ ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ

Удаленный мониторинг промышленного оборудования

- Независимое безопасное подключение к уровню ПЛК
- Защита ПЛК и конверторов протоколов от внешних и внутренних атак средствами **Kaspersky IoT Secure Gateway β***

* Текущая версия продукта предназначена для некоммерческого пилотирования

kaspersky

Kaspersky Secure Remote Workspace

Решение для надежной и управляемой инфраструктуры тонких клиентов на базе KasperskyOS

Что такое VDI и зачем она нужна?

Аббревиатура VDI расшифровывается как **Virtual Desktop Infrastructure** — инфраструктура виртуальных рабочих столов.
Это компьютеры, к которым пользователи подключаются удаленно для выполнения своих рабочих задач.

VDI подразумевает существование виртуальных машин, работающих на физическом узле. Каждый пользователь получает свою и может подключаться к ней практически с любого устройства. Чаще всего для этого используются **тонкие клиенты**.

Плюсы перехода на VDI:

- Автоматизация процесса создания новых рабочих мест
- Защищенный доступ к виртуальному рабочему месту
- Уход от хранения и обработки данных на рабочих местах сотрудников
- Быстрое восстановление рабочих станций после инцидентов
- Централизованное администрирование и управление рабочими станциями
- Снижение рисков от атак на инфраструктуру через пользовательские рабочие станции

CITRIX XenDesktop
Microsoft Terminal Services
vmware Horizon View
HUAWEI
...

kaspersky

Почему для VDI выбирают тонкий клиент?

Безопасность

Рабочая станция пользователя — одна из самых распространенных целей для атаки злоумышленником или вредоносным программным обеспечением. Использование тонких клиентов значительно снижает риск кибератаки через рабочее место сотрудника

Гибкость

Тонкие клиенты проще в администрировании и управлении по сравнению с традиционными персональными компьютерами

Цена

Стоимость тонкого клиента существенно ниже цены рабочей станции, а наработка на отказ и срок службы существенно больше

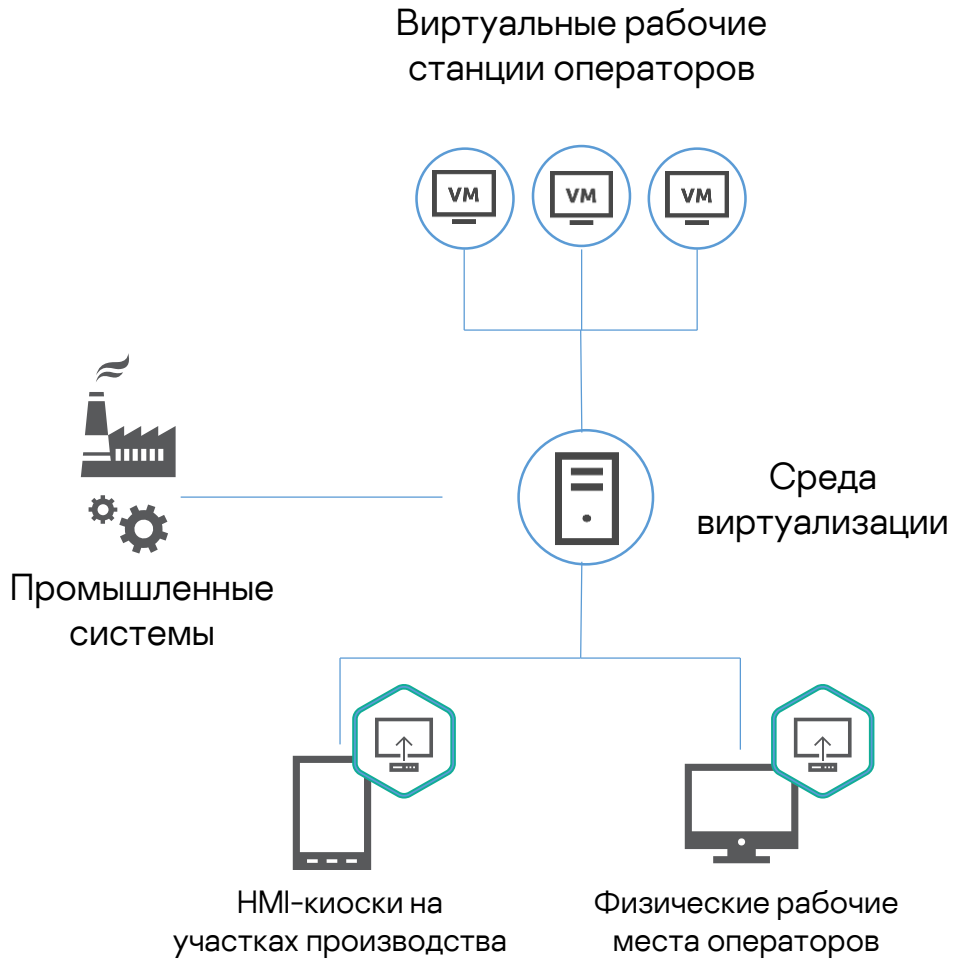
kaspersky

Применение тонких клиентов в промышленности

Индустриальный тонкий клиент и HMI – замена индустриальному ПК

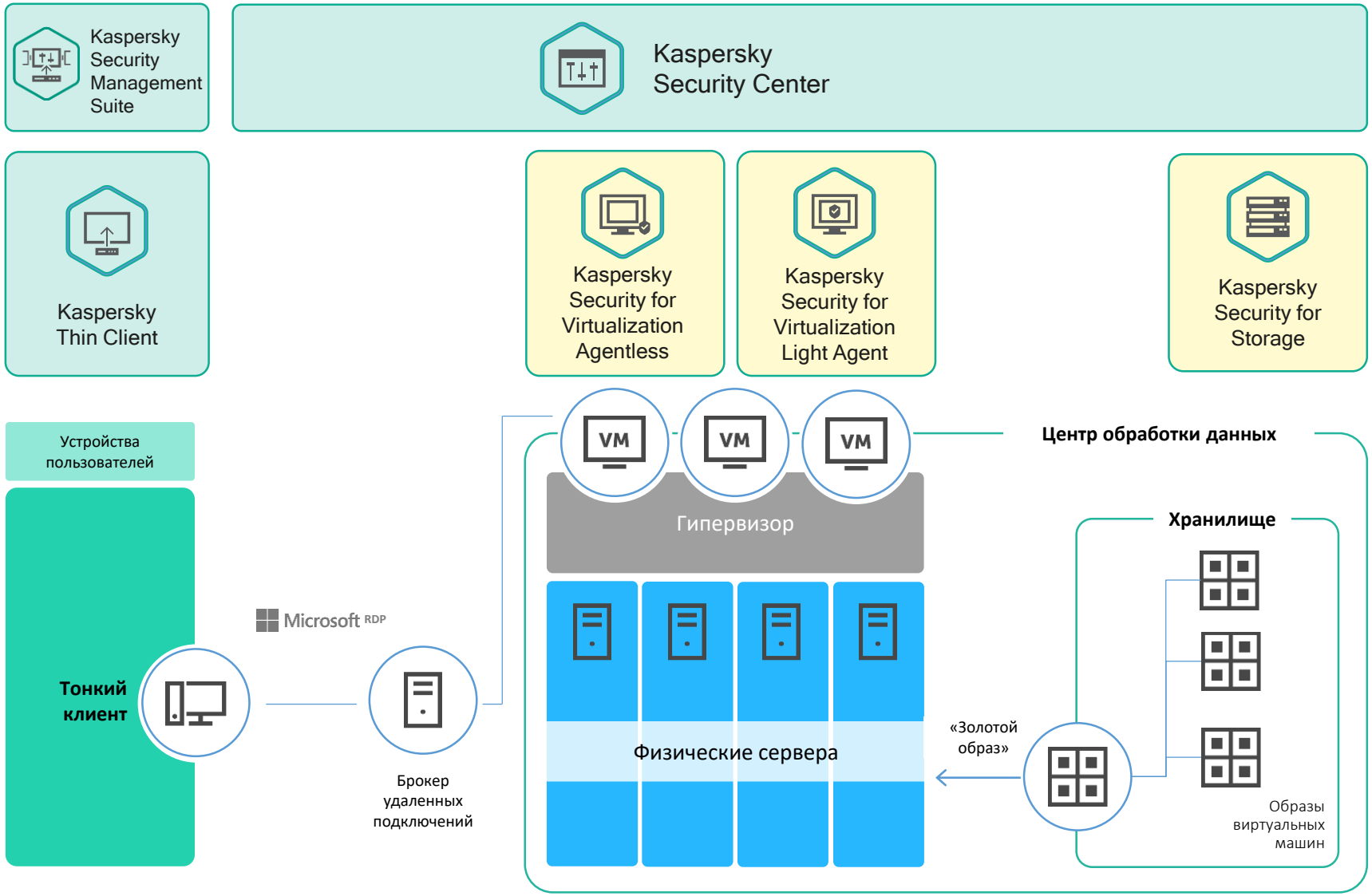
Основные достоинства:

- отсутствие подвижных частей;
- повышенная стойкость ко внешним воздействиям;
- простота ввода в эксплуатацию и замены тонкого клиента.



kaspersky

Как «Лаборатория Касперского» защищает VDI?



kaspersky

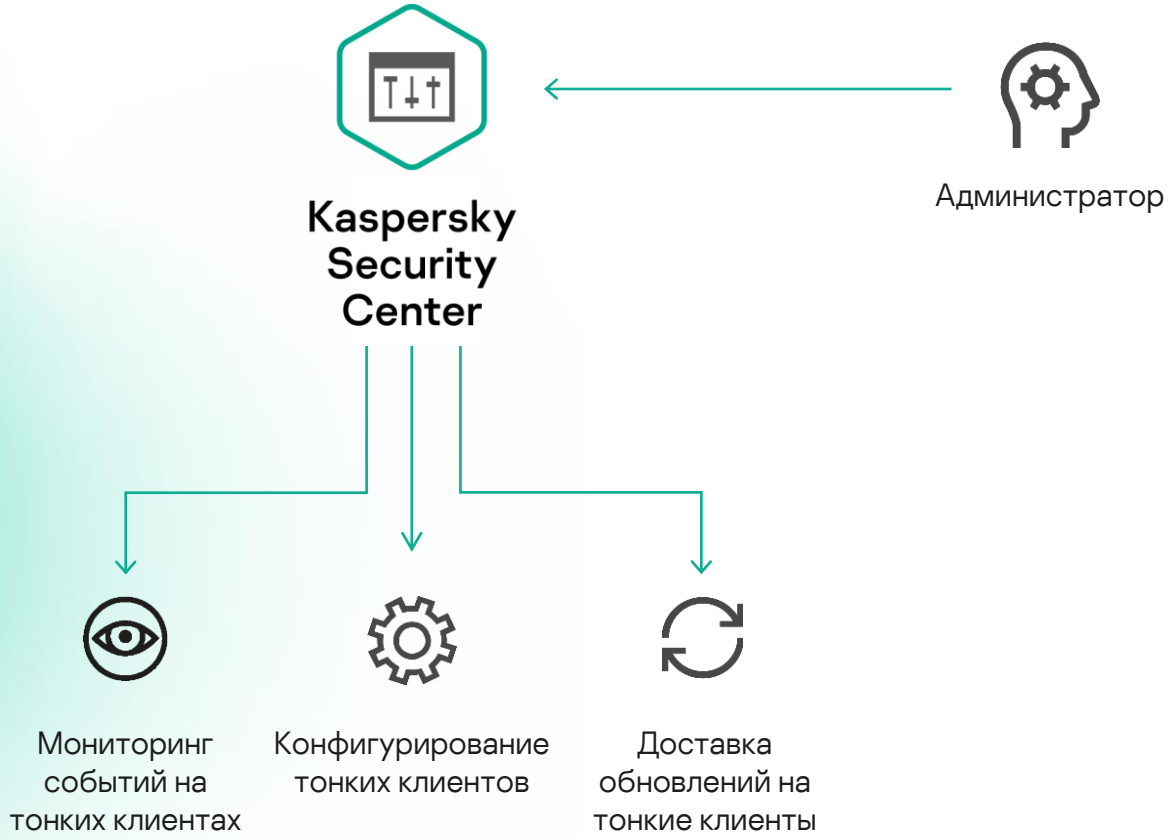
Централизованное управление с помощью Kaspersky Security Center

Kaspersky Secure Remote Workspace

Легкая миграция на тонкие клиенты

Не нужно развивать новые компетенции,
создавать процессы перехода на тонкие клиенты.

Все необходимое уже есть в Kaspersky Security Center



kaspersky

Интеграция с технологическими партнерами

Depo Sky 270

Тонкий клиент производства компании Depo Computers — первый среди поддерживаемых операционной системой KasperskyOS

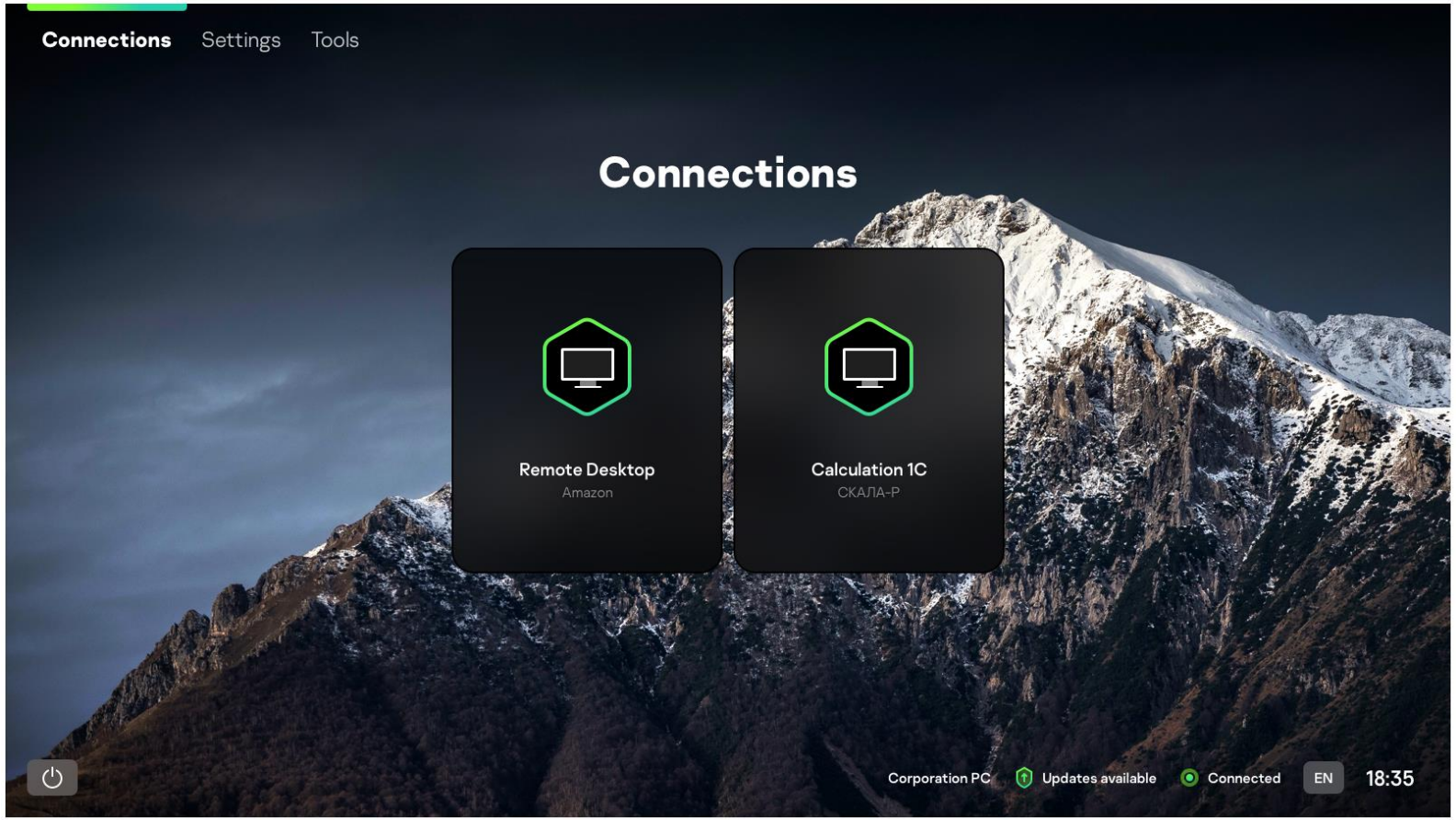
RDP и Скала-Р

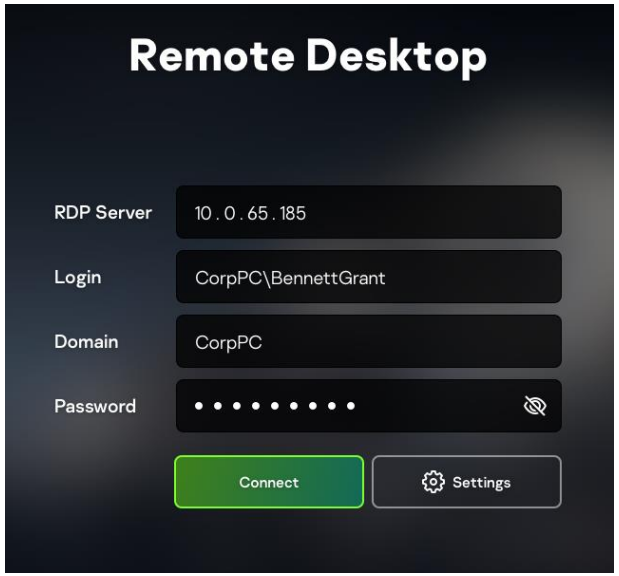
Поддержка не только «стандартного» RDP, но и отечественной системы виртуализации Скала-Р BPM производства компании IBS. Важно, что Скала-Р уже интегрирована с продуктом KSV.

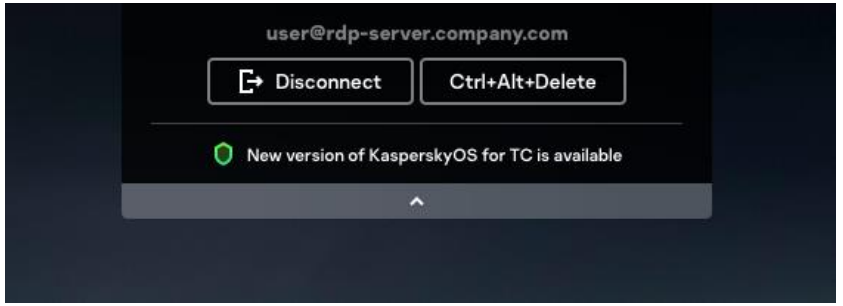
Список поддерживаемых подключений будет расти от версии к версии

Поддержка двухфакторной аутентификации — одно из основных требований бизнеса к тонкому клиенту.
В версии продукта 1.0 мы реализуем работу с наиболее распространенными носителями ключевой информации

Kaspersky Thin Client (пример пользовательского интерфейса)

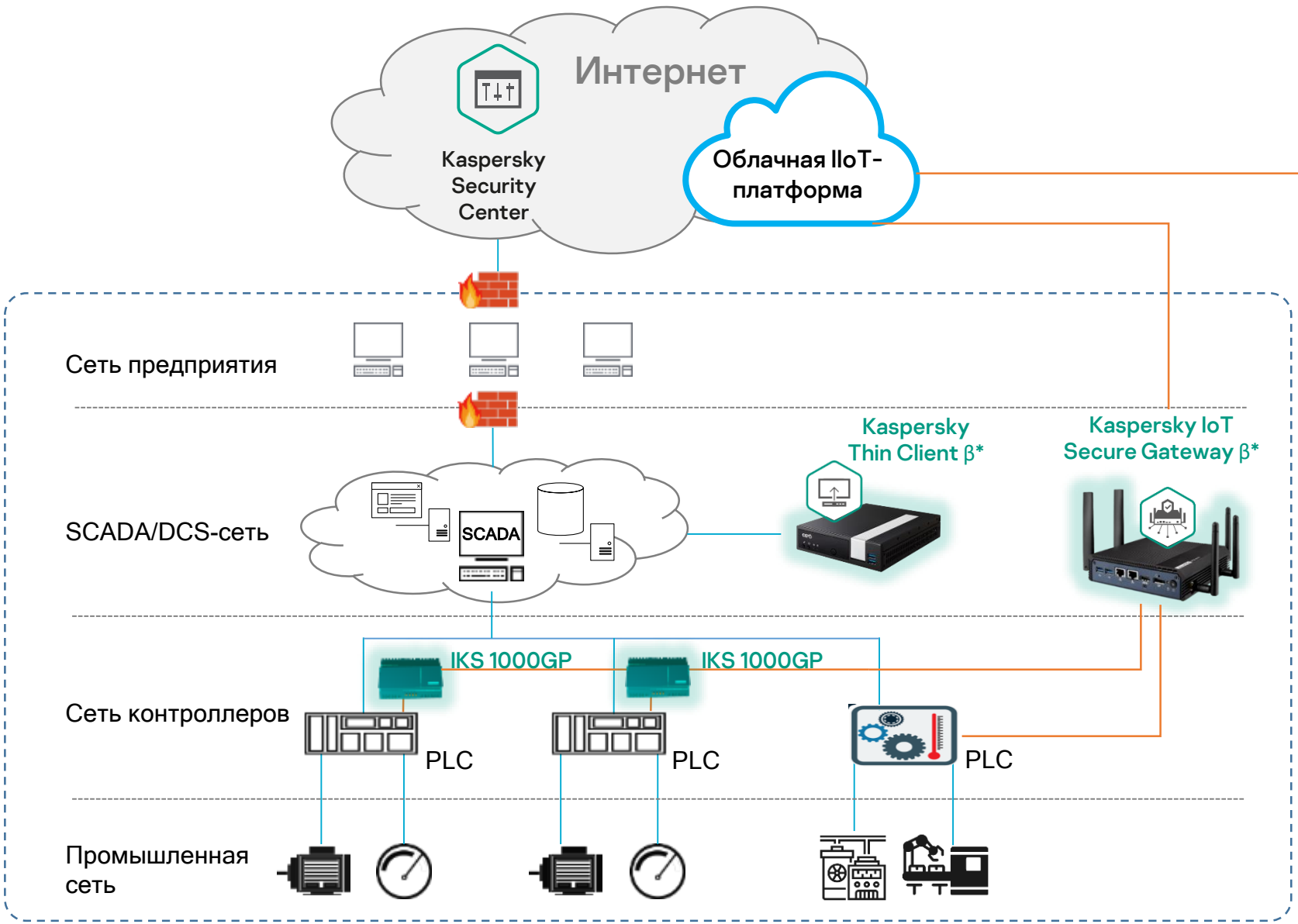




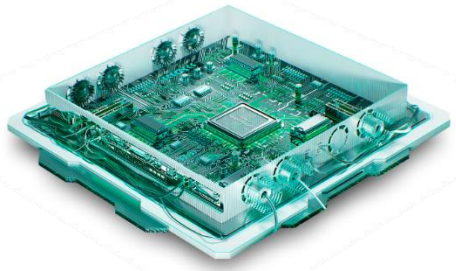


kaspersky

Первые элементы на KasperskyOS в промышленном контуре



KasperskyOS®

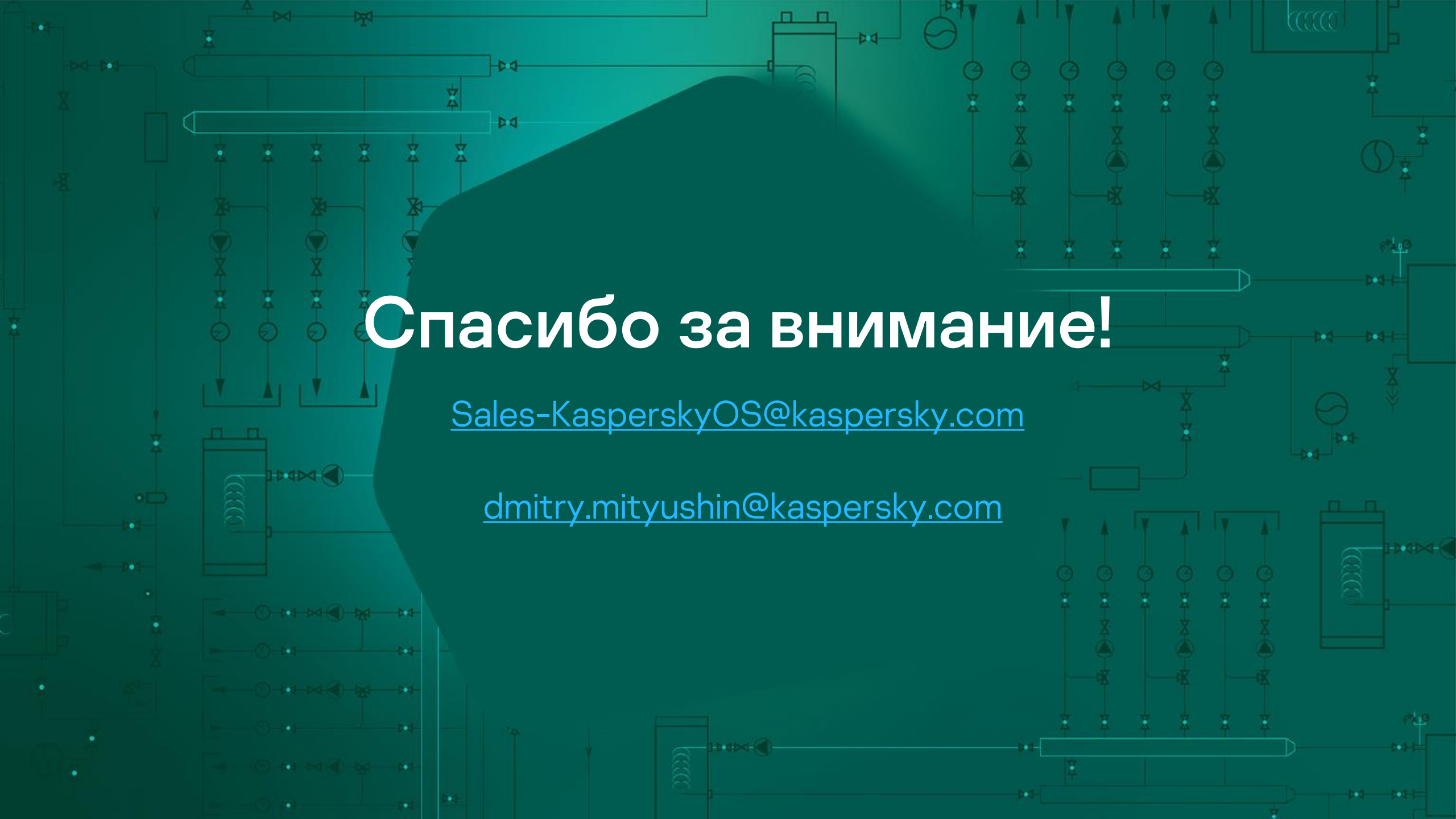


* *Текущие версии продуктов предназначены для некоммерческого тестирования и пилотирования*

kaspersky

Безопасное будущее начинается сегодня.

Давайте строить его вместе!



Спасибо за внимание!

Sales-KasperskyOS@kaspersky.com

dmitry.mityushin@kaspersky.com