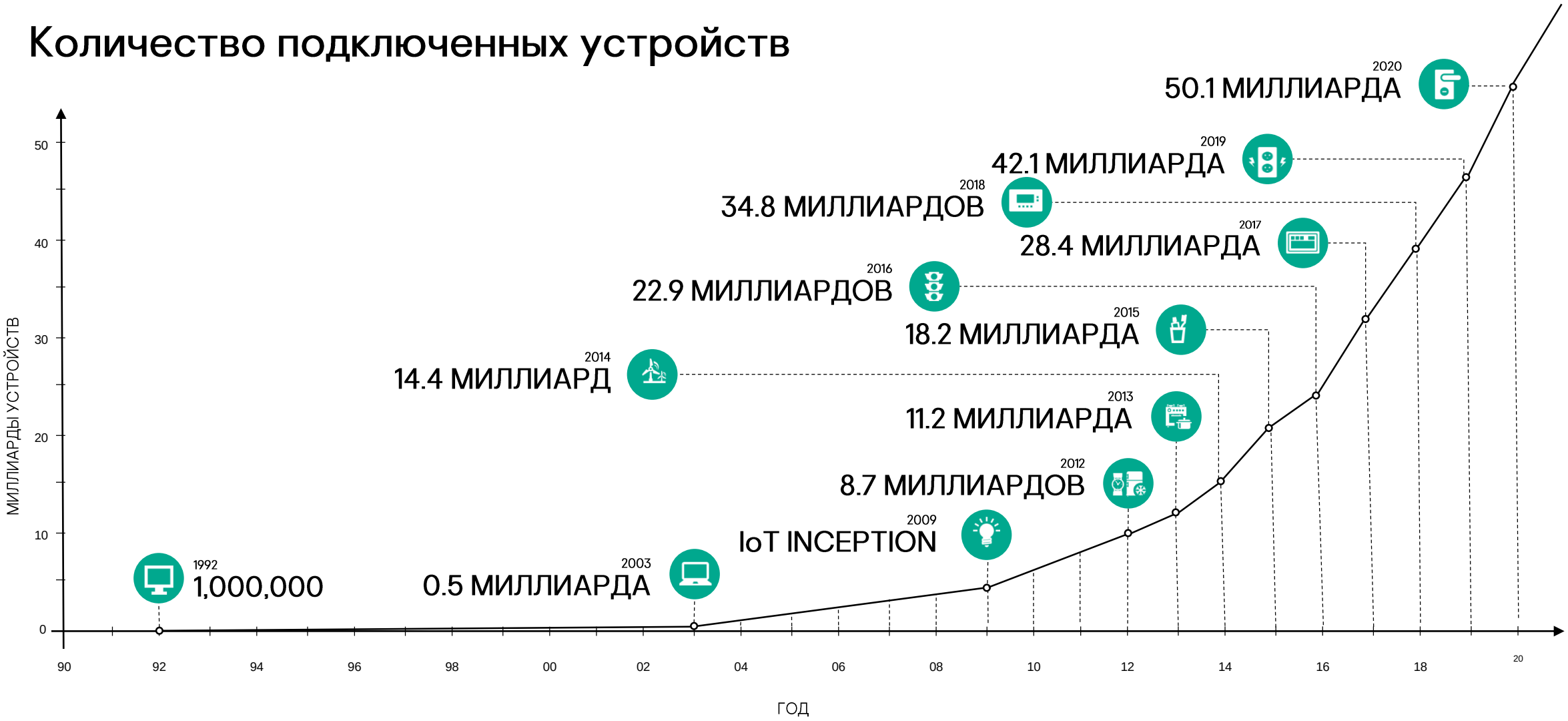
Будущее для безопасности интернета вещей и встраиваемых систем: Kaspersky Operating System

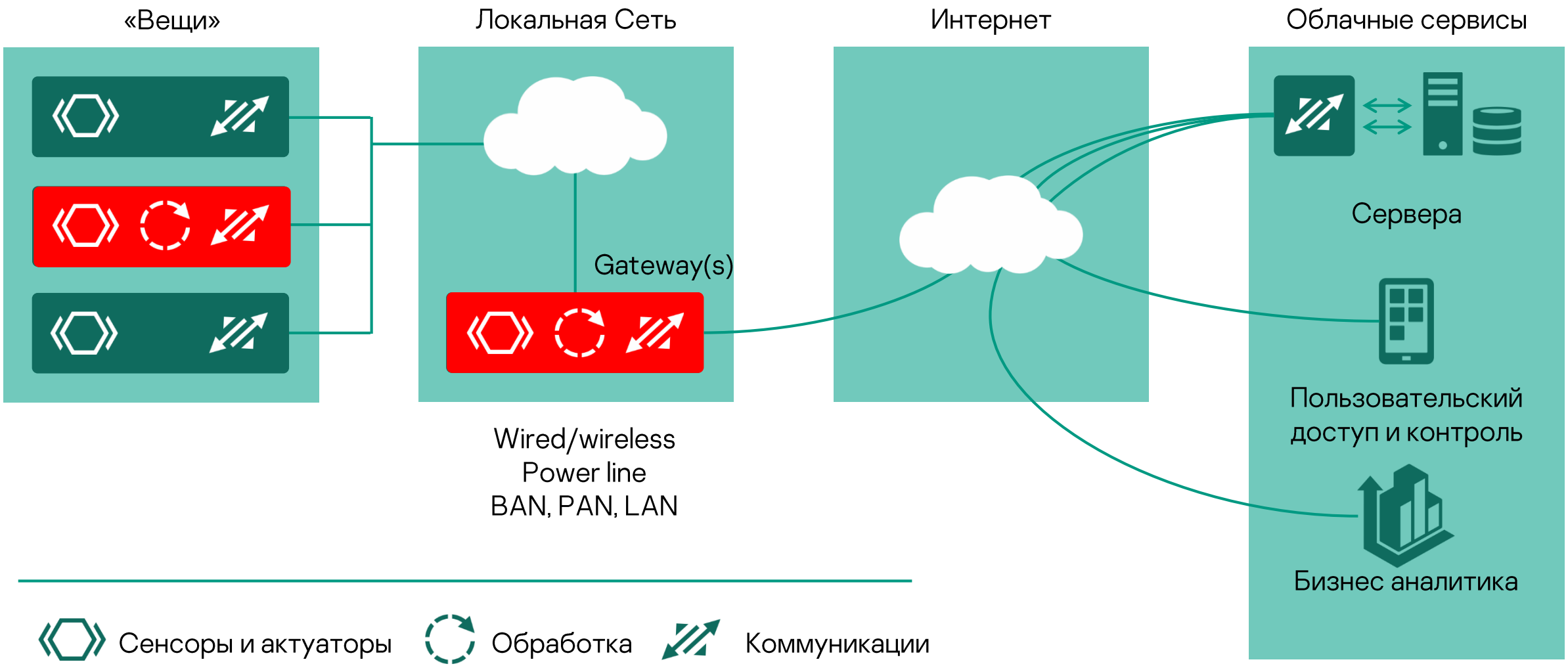
kaspersky

Интернет вещей

Количество подключенных устройств



Функциональные IoT устройства наиболее уязвимы



Атаки на IoT

MIRAI

Mirai был обнаружен в августе 2016, и наименование пошло от имени одного из модулей, который назывался “mirai.()”. Mirai – это исполняемый модуль Linux, и его основная цель – это камеры наблюдения DVRs, роутеры, Linux сервера и другие устройства, которые используют Busybox, распространённую библиотеку для IoT устройств.

BASHLITE

Заражает Linux системы и использует их для организации DDoS атак. В 2014 BASHLITE использовал для распространения уязвимость Shellshock для заражения устройств с BusyBox. В 2016 было около 1 миллиона устройств, зараженных BASHLITE.

Основная проблема IoT с точки зрения кибербезопасности

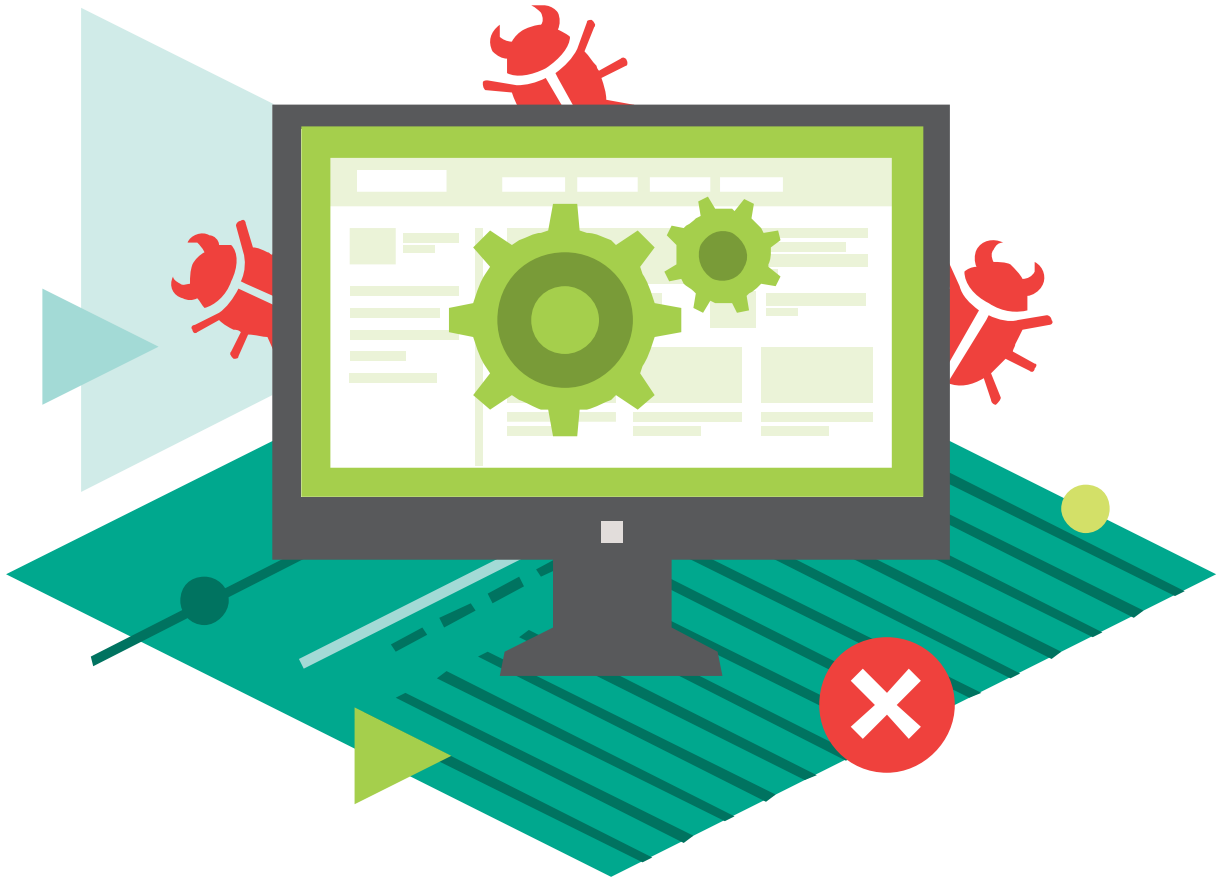
Уязвимости

- ✓ Ошибки людей
- ✓ Использование сторонних библиотек и приложений
- ✓ Сложность программного обеспечения (Значительное увеличение количества строк кода)

Небезопасный дизайн

- ✓ Желание вывести продукт на рынок как можно быстрее

Небезопасность операционных систем общего назначения



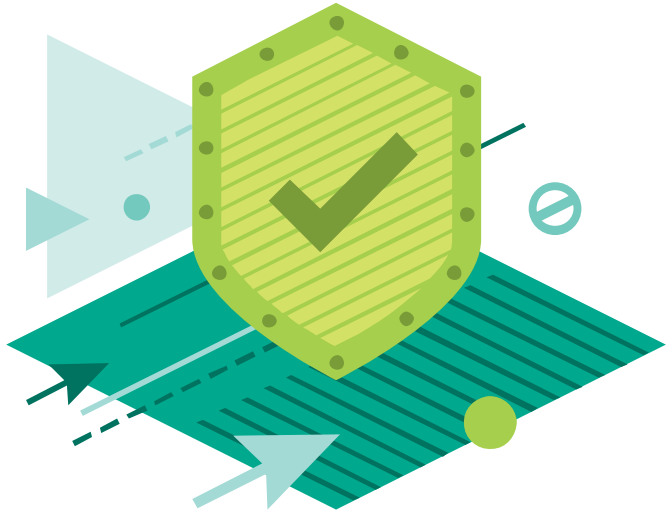
Почему ос общего назначения небезопасны

- Монолитная система позволяет любому модулю вызывать напрямую любой другой модуль
- Эксплуатируя уязвимость есть возможность вызвать другой модуль, несмотря на настройки безопасности
- Использование стороннего кода
- Есть возможность получить контроль над системой целиком после эксплуатации всего одной уязвимости
- Слабые настройки безопасности по разным причинам (недостаток опыта или времени, лень)
- Огромная поверхность атаки

Как нам обезопасить встраиваемые системы

Как решить проблему

Создать такое окружение, которое просто не позволит программам исполнить недекларируемые возможности (код) и предотвратит эксплуатацию уязвимостей.



Основные принципы безопасной ОС

- ✓ Безопасность, заложенная в архитектуру (Secure by design system)
- ✓ Использование MILS подхода с монитором обращений
- ✓ Микроядро
- ✓ Удовлетворяет специальным требованиям к ОС для встраиваемых систем

Требование к ОС для встраиваемых систем

Небольшой размер и минимальное использование ресурсов

Большинство встраиваемых систем ограничены в ресурсах (RAM, ROM, CPU)

Стабильная работа даже во время атаки

Решение должно быть продумано с т.з. кибербезопасности и векторов потенциальных атак

Решение из коробки

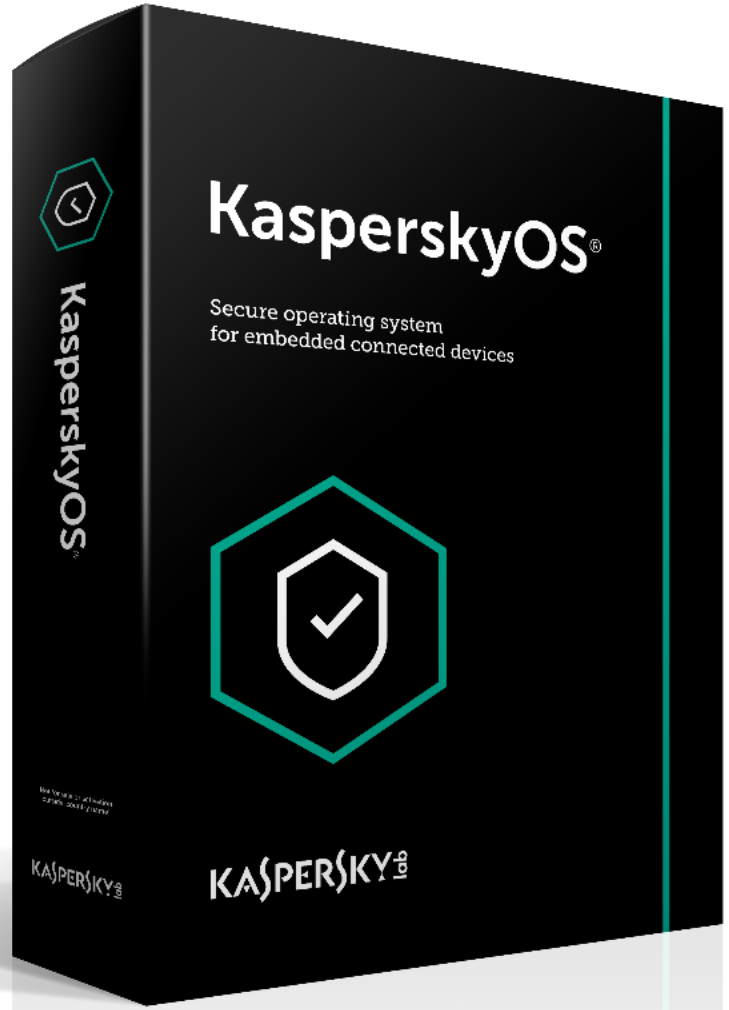
Большинство встраиваемых систем имеют (почти) уникальные требования к кибербезопасности. Необходимо поддержать эти требования и при этом уменьшить время разработки нового продукта

Соответствие индустриальным стандартам

Решение должно быть создано и разработано в соответствии с индустриальными стандартами функциональной и кибербезопасности.

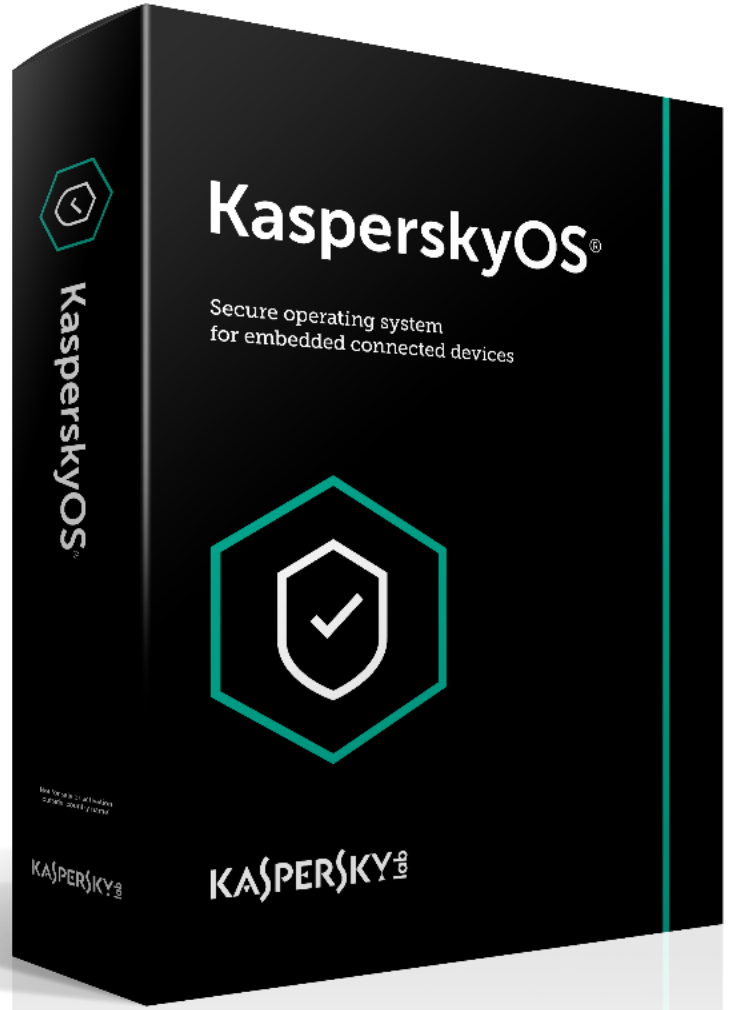
KasperskyOS // Первый взгляд

- Разработана для встраиваемых, подключенных к сети Интернет устройств со специфическими требованиями к кибербезопасности
- Основана на микроядре, которое гарантирует контроль всех внутренних коммуникаций
- Поведение всех модулей описано в политиках безопасности
- MILS архитектура
  - ✓ Разделение и изоляция доменов безопасности
  - ✓ Гибкий контроль междоменных коммуникаций посредством Kaspersky Security System (KSS)



KasperskyOS // Спецификация

- Микроядерная операционная система, разработанная с нуля в Лаборатории Касперского
- Статическая конфигурация безопасности
- MILS архитектура
- Разделение функционала приложения и функций кибербезопасности (упрощается разработка приложений, уменьшается время разработки и улучшается качество продукта)
- Максимальный уровень контроля всей системы благодаря уменьшению гранулярности доменов безопасности (каждое приложение, драйвер, библиотека могут быть отдельным доменом безопасности)
- Совместима с POSIX API (~98% API)
- Поддерживает Intel x86, x64 и ARM (v6, v7, v8)



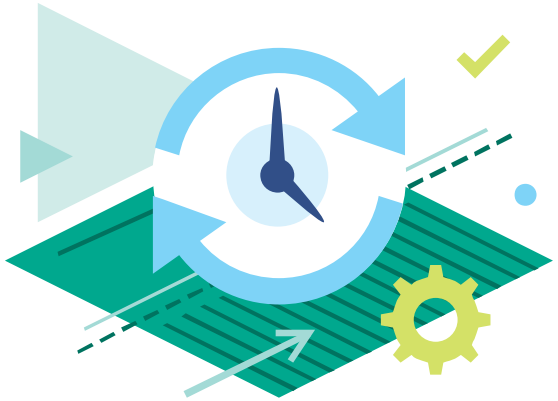
KasperskyOS – Доверенная. Гибкая. Безопасная.

Доверенная

KasperskyOS может выступать основой для построения доверенной системы в силу своих архитектурных особенностей: ОС не допускает исполнения функций приложений, не декларированных в политиках безопасности

Гибкая

Благодаря возможности использования любого типа политик безопасности, возможно использовать KasperskyOS для любых задач. Разработав один раз политику для приложения или модуля, ее можно использовать вновь в будущем



Безопасная

Благодаря разделению функций безопасности и функциональной части приложения, возможна параллельная работа над этими частями, что экономит время

Позволяет улучшить функциональную безопасность системы за счет использования политик безопасности, в которых описан алгоритм работы

Плюсы KasperskyOS

Врожденная безопасность

Операционная система KasperskyOS создана безопасной со стадии дизайна и останется таковой за счет использования лучших практик из мира кибербезопасности

Гибкие настройки безопасности

Средства разработки позволяют легко создавать правила поведения системы и комбинировать разные типы политик для контроля взаимодействий.

Универсальная модульная архитектура

Система построена из слабо связанных модулей, что позволяет легко модифицировать набор модулей и минимизировать время на разработку доверенных модулей

Разделение безопасности и функциональной части модулей

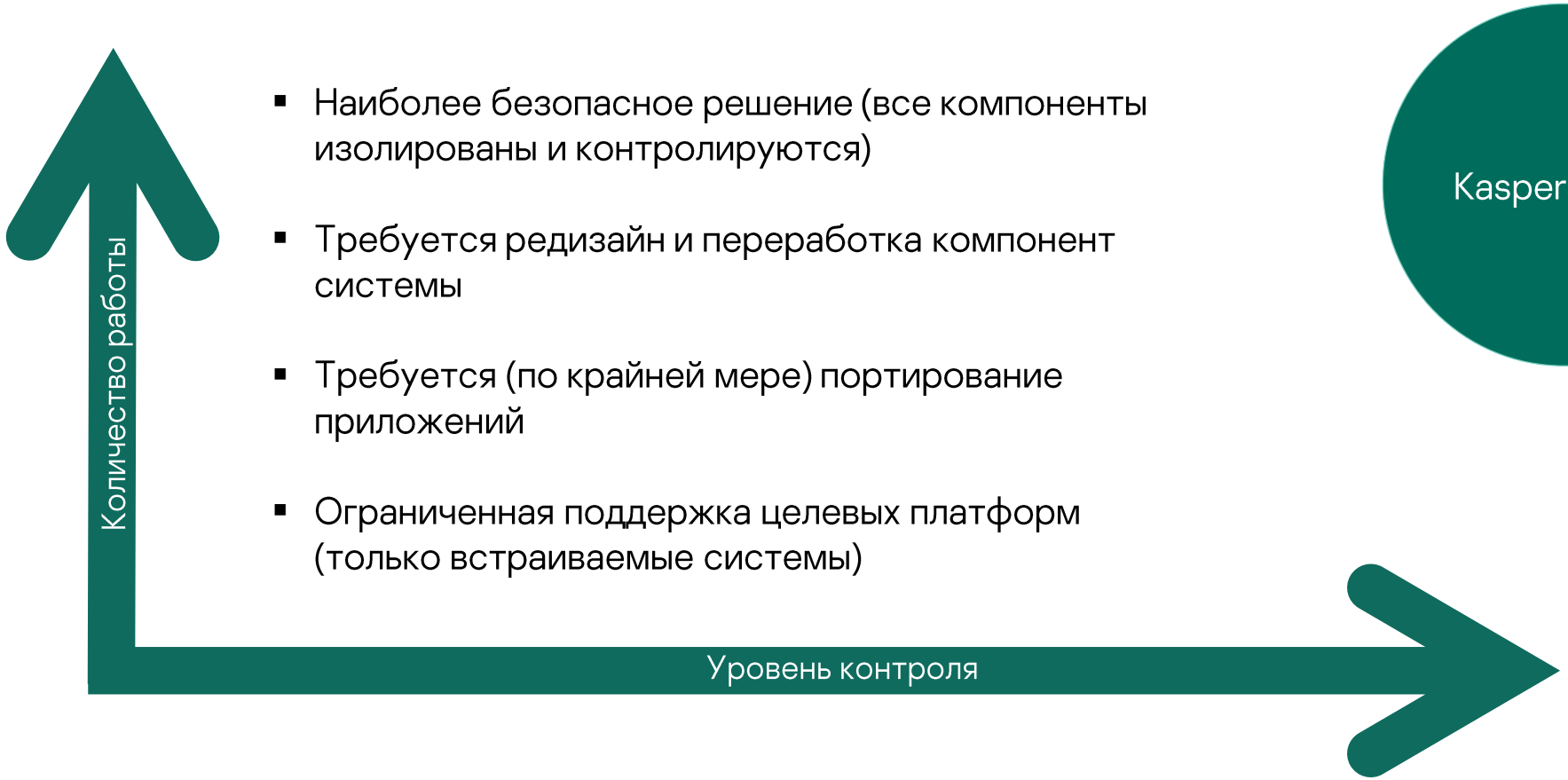
Безопасная архитектура спроектирована таким образом, чтобы отделить функции безопасности от бизнес-логики приложений; благодаря этому настройка политик безопасности и разработка приложений становятся проще

Реализации KasperskyOS

Мы разработали набор продуктов, которые подходят разным клиентам с различными потребностями. При этом все продукты построены на основе одних и тех же принципов безопасности (разделение и изоляция доменов безопасности и жесткий контроль коммуникаций между ними)

- ✓ KasperskyOS
- ✓ Kaspersky Secure Hypervisor
- ✓ Kaspersky Security System для Linux

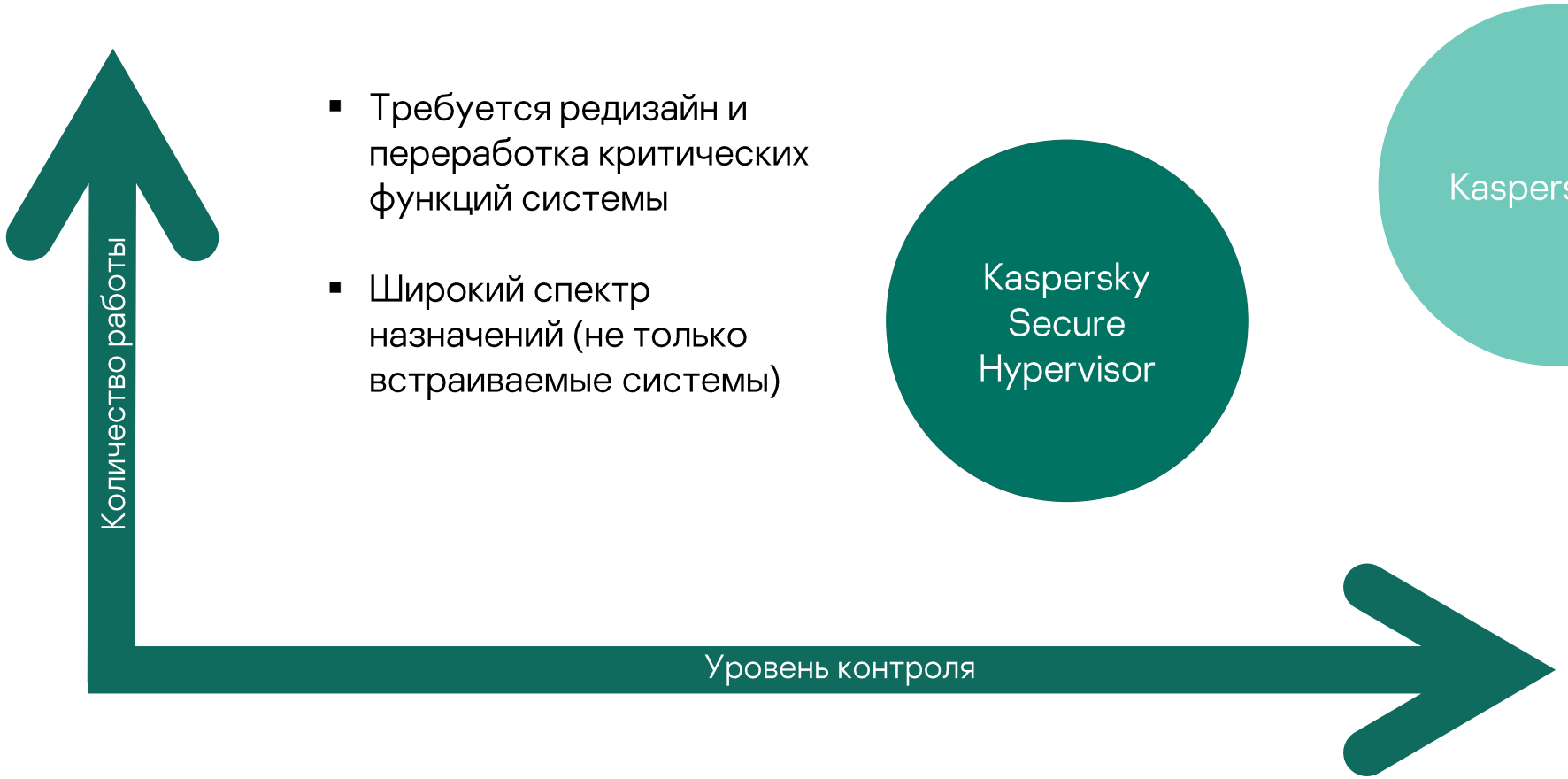
Технологии кибербезопасности, которые подходят для разных применений



- Наиболее безопасное решение (все компоненты изолированы и контролируются)
- Требуется редизайн и переработка компонент системы
- Требуется (по крайней мере) портирование приложений
- Ограниченная поддержка целевых платформ (только встраиваемые системы)

KasperskyOS

Технологии кибербезопасности, которые подходят для разных применений



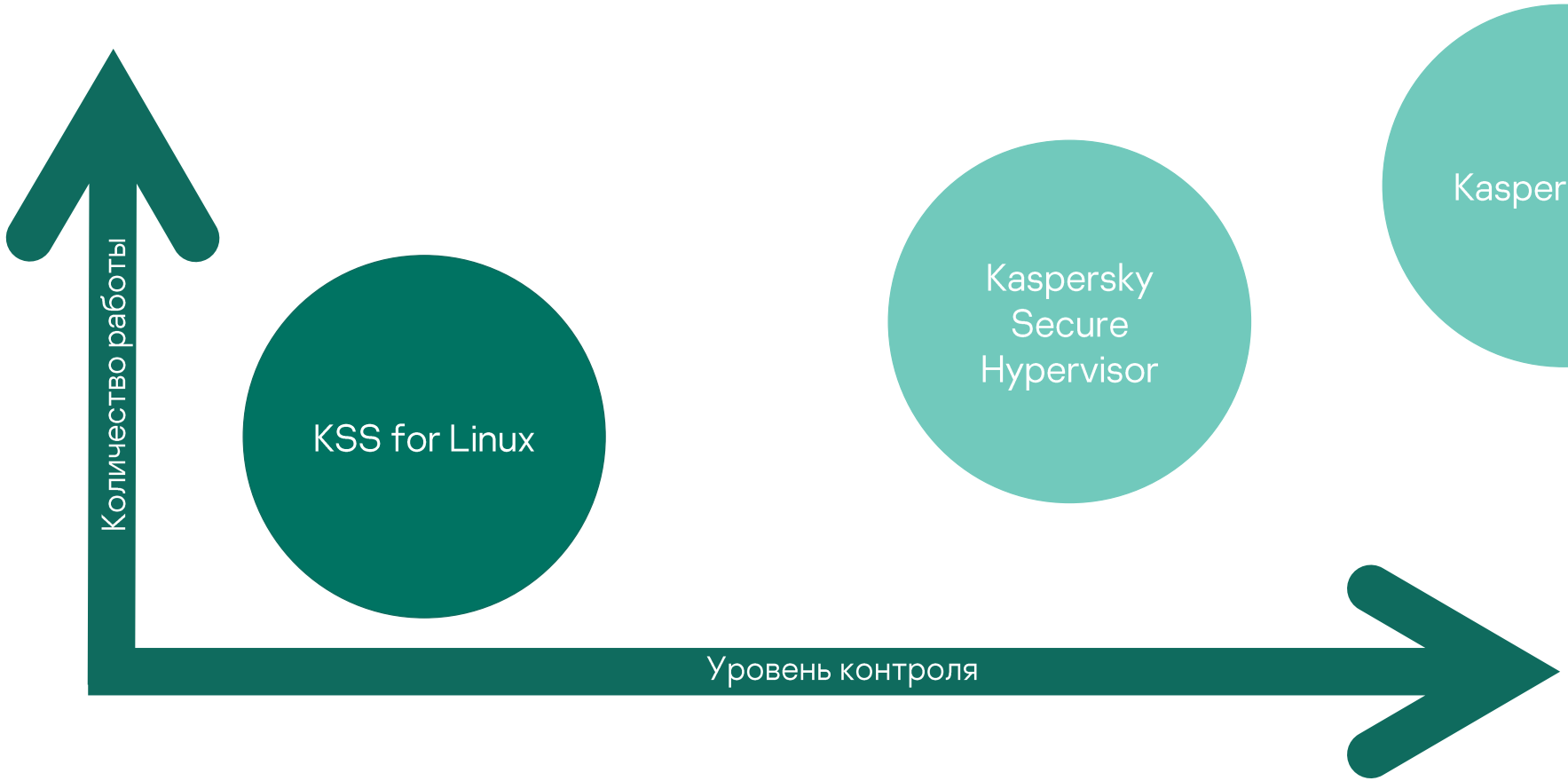
- Требуется редизайн и переработка критических функций системы
- Широкий спектр назначений (не только встраиваемые системы)

Kaspersky Secure Hypervisor

KasperskyOS

- Хороший уровень безопасности (изоляция ВМ и контроль коммуникаций между ними)
- Требуется редизайн и переработка архитектуры компонент системы

Технологии кибербезопасности, которые подходят для разных применений



- Хороший уровень безопасности (изоляция контейнеров Linux, контроль коммуникаций между контейнерами)
- Требуется лишь редизайн архитектуры приложений
- Минимум доработок
- Работает на всех версиях Linux с поддержкой контейнеризации

Технологии кибербезопасности, которые подходят для разных применений

KasperskyOS

- Наиболее безопасное решение (все компоненты изолированы и контролируются)
- Требуется редизайн и переработка компонент системы
- Требуется (по крайней мере) портирование приложений
- Ограниченная поддержка целевых платформ (только встраиваемые системы)

Secure Hypervisor

- Хороший уровень безопасности (изоляция ВМ и контроль коммуникаций между ними)
- Требуется редизайн и переработка архитектуры компонент системы и критических функций системы
- Широкий спектр назначений (не только встраиваемые системы)

KSS for Linux

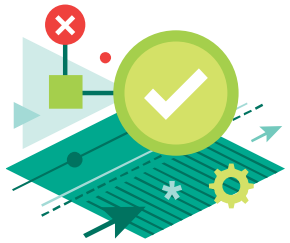
- Хороший уровень безопасности (изоляция контейнеров Linux, контроль коммуникаций между контейнерами)
- Требуется лишь редизайн архитектуры приложений
- Минимум доработок
- Работает на всех версиях Linux с поддержкой контейнеризации

Примеры использования

Сетевое и телекоммуникационное оборудование

IoT и индустриальный IoT

Современные автомобили



PC

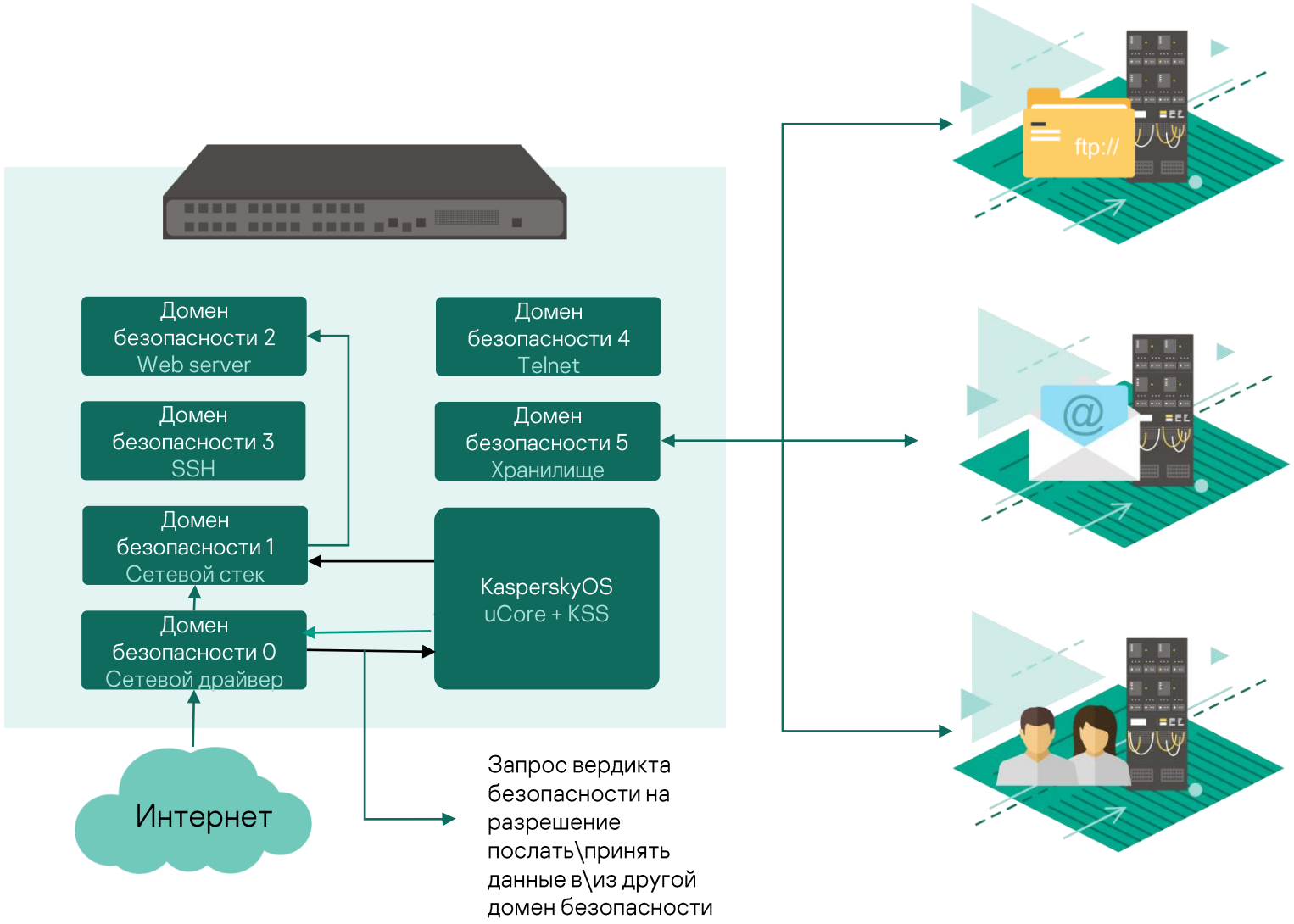
POS терминалы

Расширение безопасности для Linux

Примеры использования – телекоммуникационное оборудование

KasperskyOS

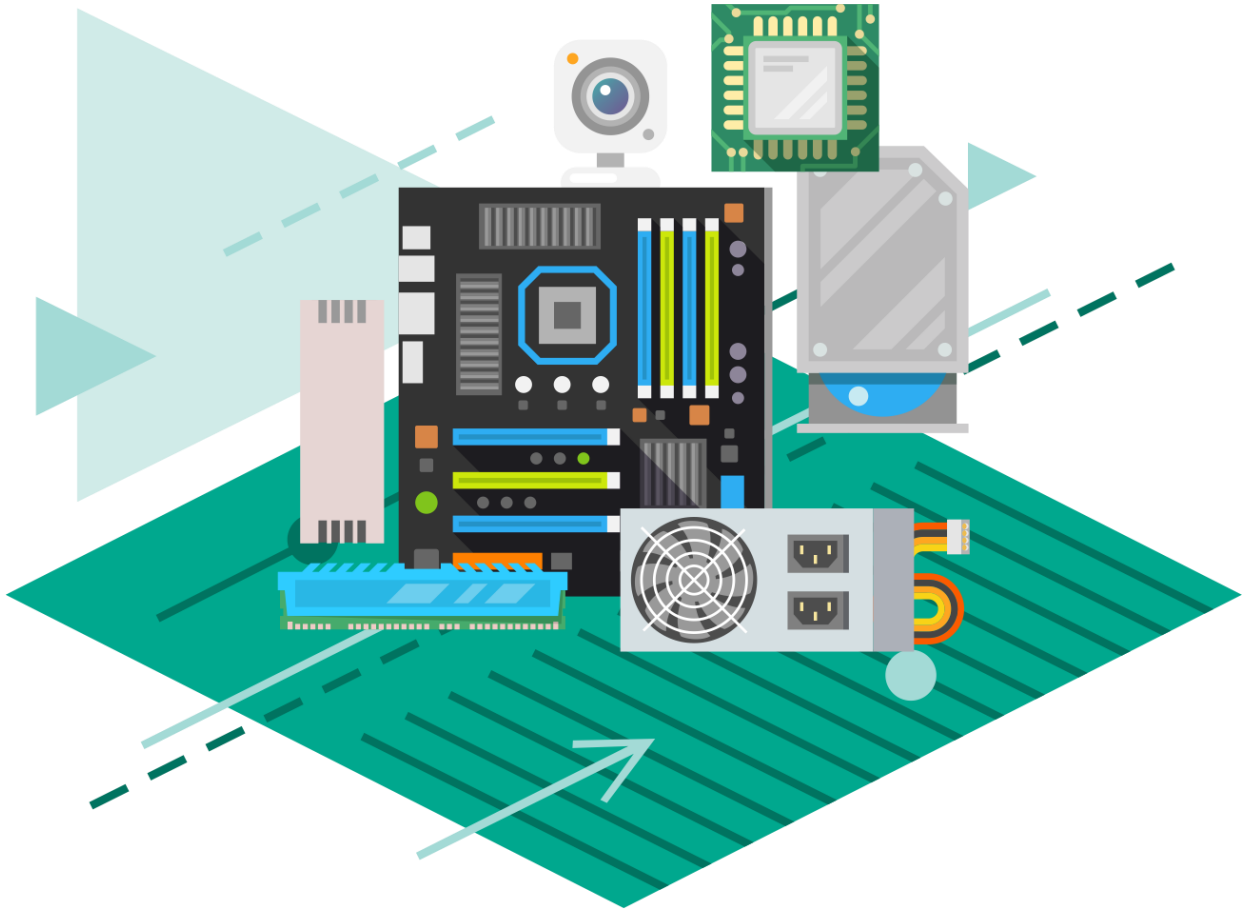
- Доверенная платформа
- Безопасность с самого начала:
  - ✓ Безопасная загрузка гарантирует целостность ОС и приложений
  - ✓ Изоляция всех компонентов и приложений
  - ✓ Минимальный урон от эксплуатации уязвимостей, защита от вредоносного кода
  - ✓ Защита важных данных (ключей шифрования)
- Сетевые роутеры и свитчи, VPN серверы



Примеры использования – IoT

KasperskyOS

- Безопасность с нуля (единственный способ защитить IoT)
  - ✓ Изоляция всех доменов безопасности
  - ✓ Минимизация урона от уязвимостей
  - ✓ Защита важных данных (ключей шифрования)
  - ✓ Безопасная загрузка



Пример

✓ Подключенные к сети устройства с богатым функционалом (не основанные на MCU) :

1. Умные камеры наблюдения (CCTV) (обработка изображения на камере и передача не только картинки, но и результатов обработки)

2. Интернет хабы и гейтвеи

Примеры использования – connected автомобили

KASPERSKY SECURE HYPERVISOR

- Безопасность с нуля
  - ✓ Изоляция информационно-развлекательной системы от критических компонент (advanced driver assistance systems, AUTOSAR)
  - ✓ Минимизация урона от эксплуатации уязвимости в одном из доменов
  - ✓ Защита важных данных (ключи шифрования, сертификаты, телеметрия, логи) от несанкционированного доступа
  - ✓ Безопасная загрузка и защита от несанкционированного изменения компонентов системы
- Может быть использован в головном блоке, гейтвее или в ECU

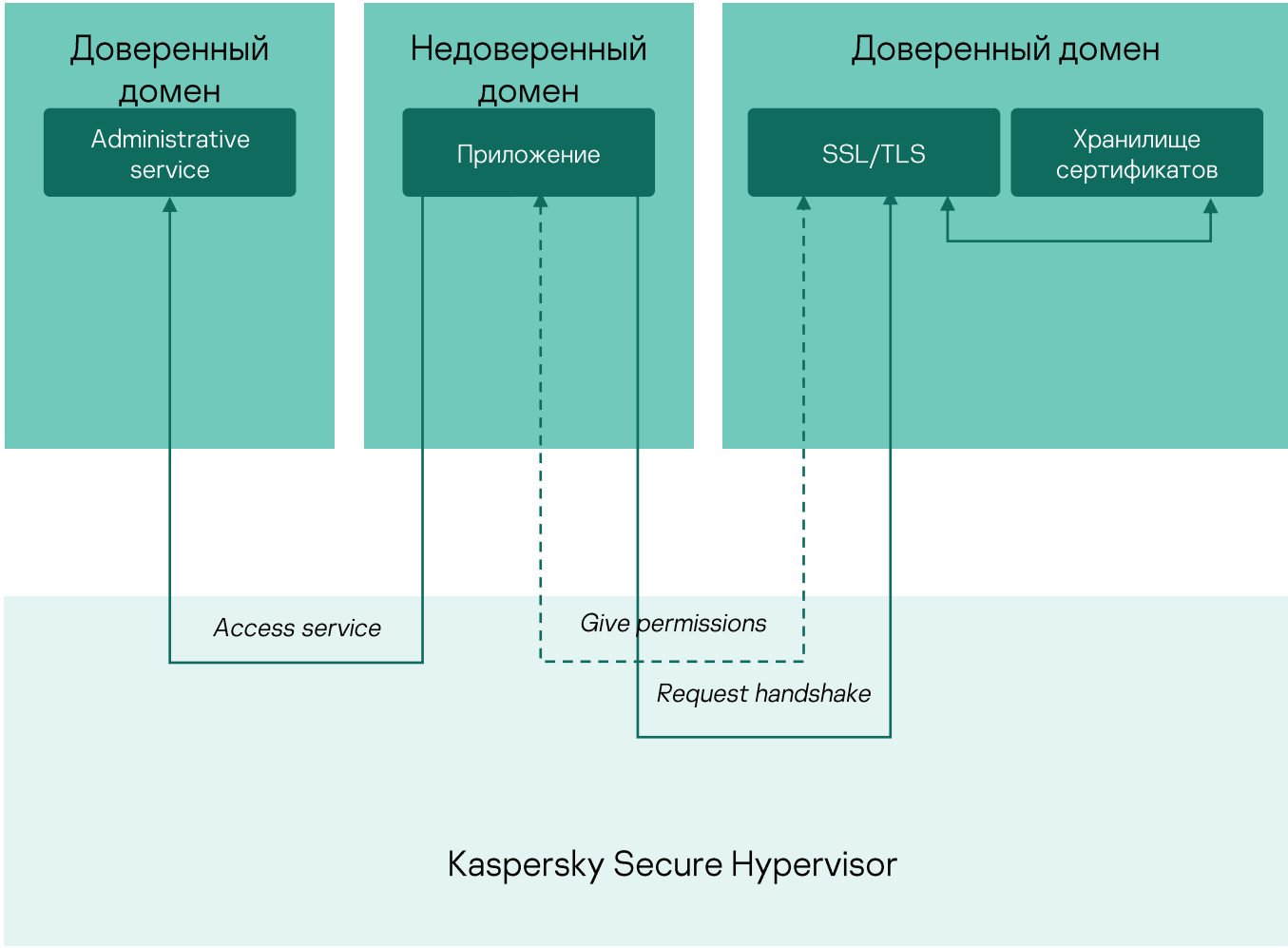
Примеры использования – PC и тонкие клиенты

Kaspersky Secure Hypervisor

- Две виртуальные машины
- Первая с доступом к конфиденциальной информации (внутренний домен)
- Вторая с доступом к Сети и публичным сервисам (внешний домен)

  ✓ Отсутствие или контролируемый обмен информацией между виртуальными машинами
  ✓ Контроль целостности программного обеспечения
  ✓ Доверенная загрузка
  ✓ Защита от Bootkit и rootkit
  ✓ Контроль доступа ко внешним устройствам
  ✓ Уменьшение стоимости владения (нужен один PC вместо двух)

  - Специальный компьютер с двумя жесткими дисками и сетевыми картами



Примеры использования – сетевое оборудование

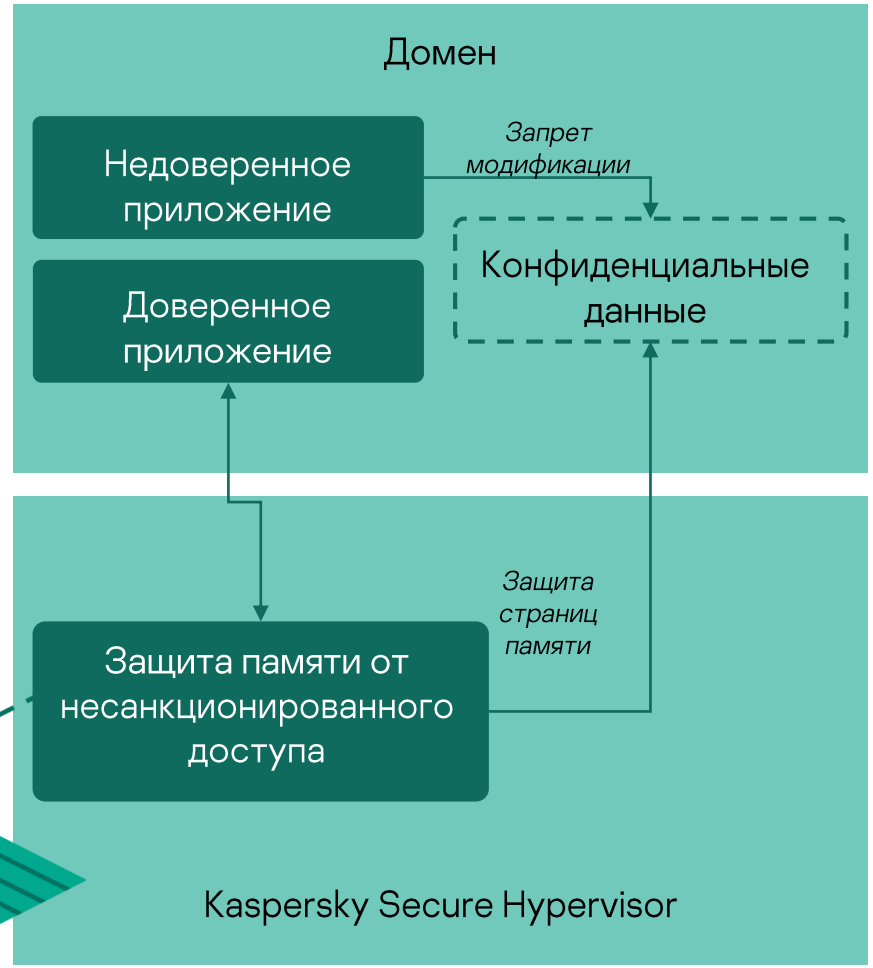
Kaspersky Secure Hypervisor

- ✓ Безопасное хранилище для ключей шифрования и сертификатов (защита от несанкционированного доступа как со стороны программного, так и со стороны аппаратного обеспечения)
- ✓ Разделение и менеджмент функциональных модулей, например web и почтовый антивирусы, контентная фильтрация, облачное хранилище (модули могут продаваться и активироваться отдельно с разными лицензиями)
- ✓ VPN серверы
- ✓ UTMs

Примеры использования – POS терминалы

Kaspersky Secure Hypervisor

- Перенос важных с т.з. кибербезопасности функций в отдельный безопасный домен
  - ✓ Обработка данных кредитных карт (защита от несанкционированного доступа к данным карт)
  - ✓ Коммуникации с банками и процессинговыми центрами
  - ✓ Безопасное хранилище (аудит, безопасная передача доверенных данных менеджменту или регулятору)
- Контроль целостности ПО POS терминала
  - ✓ Соответствие PA DSS



Примеры использования – улучшение безопасности для Linux

Kaspersky Security System

- Примеры использования:
  - ✓ Безопасное обновление ПО и конфигурации
  - ✓ Разделение обязанностей между компонентами и удаленными агентами
  - ✓ Сэндбокс для недоверенного ПО
  - ✓ Улучшение уровня кибербезопасности благодаря внедрению контроля междоменных коммуникаций
- PLCs / Устройства индустриального интернета вещей
- IoT оборудование