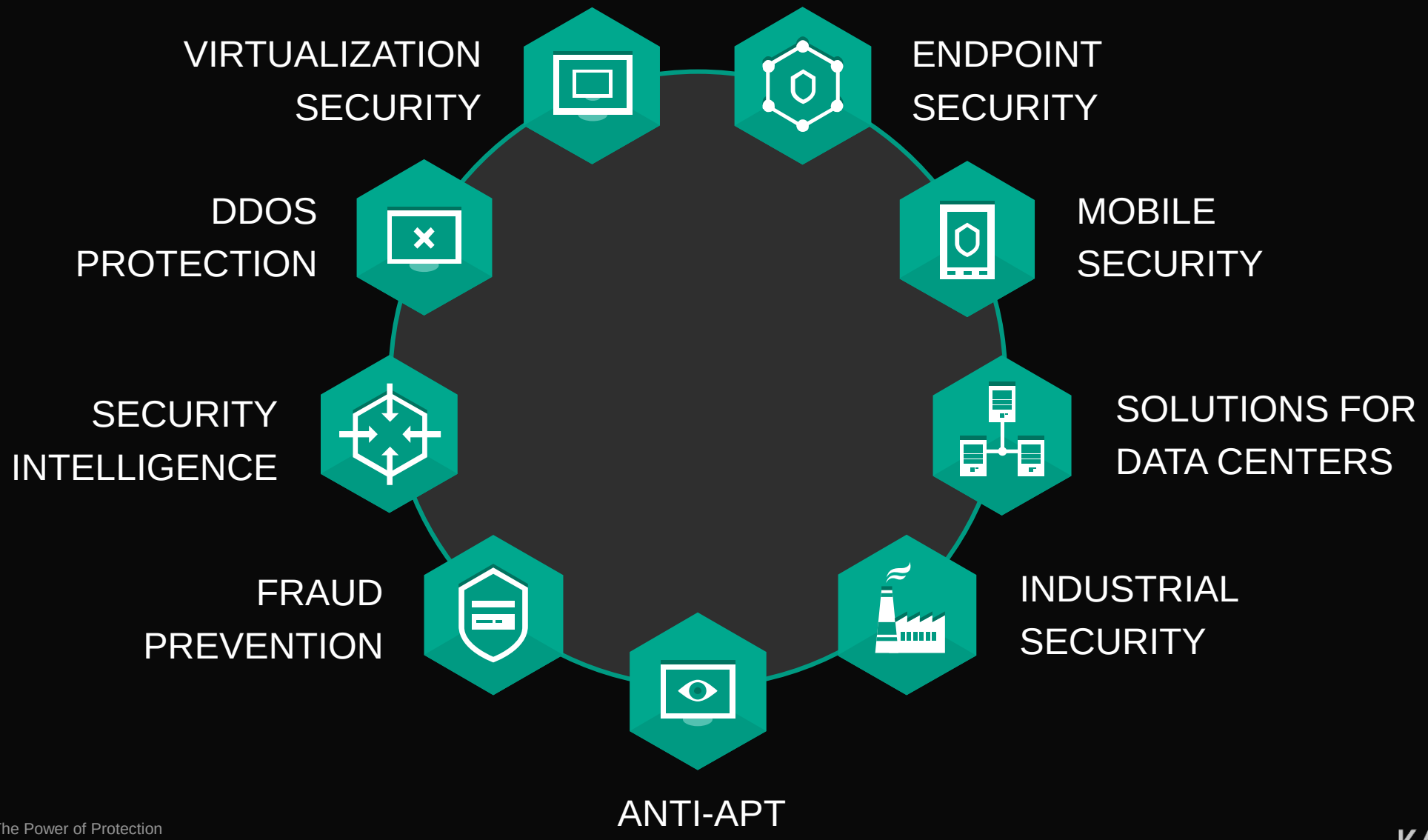
Kaspersky
SECURITY DAY

Использование KasperskyOS в российском оборудовании

KASPERSKY lab

ЧТО МЫ ЗАЩИЩАЕМ СЕГОДНЯ



ЧТО МЫ БУДЕМ ЗАЩИЩАТЬ ЗАВТРА?

ИНДУСТРИАЛЬНЫЕ ОБЪЕКТЫ

ТРАНСПОРТ И ТРАНСПОРТНЫЕ СИСТЕМЫ

МЕДИЦИНСКОЕ ОБОРУДОВАНИЕ

KasperskyOS

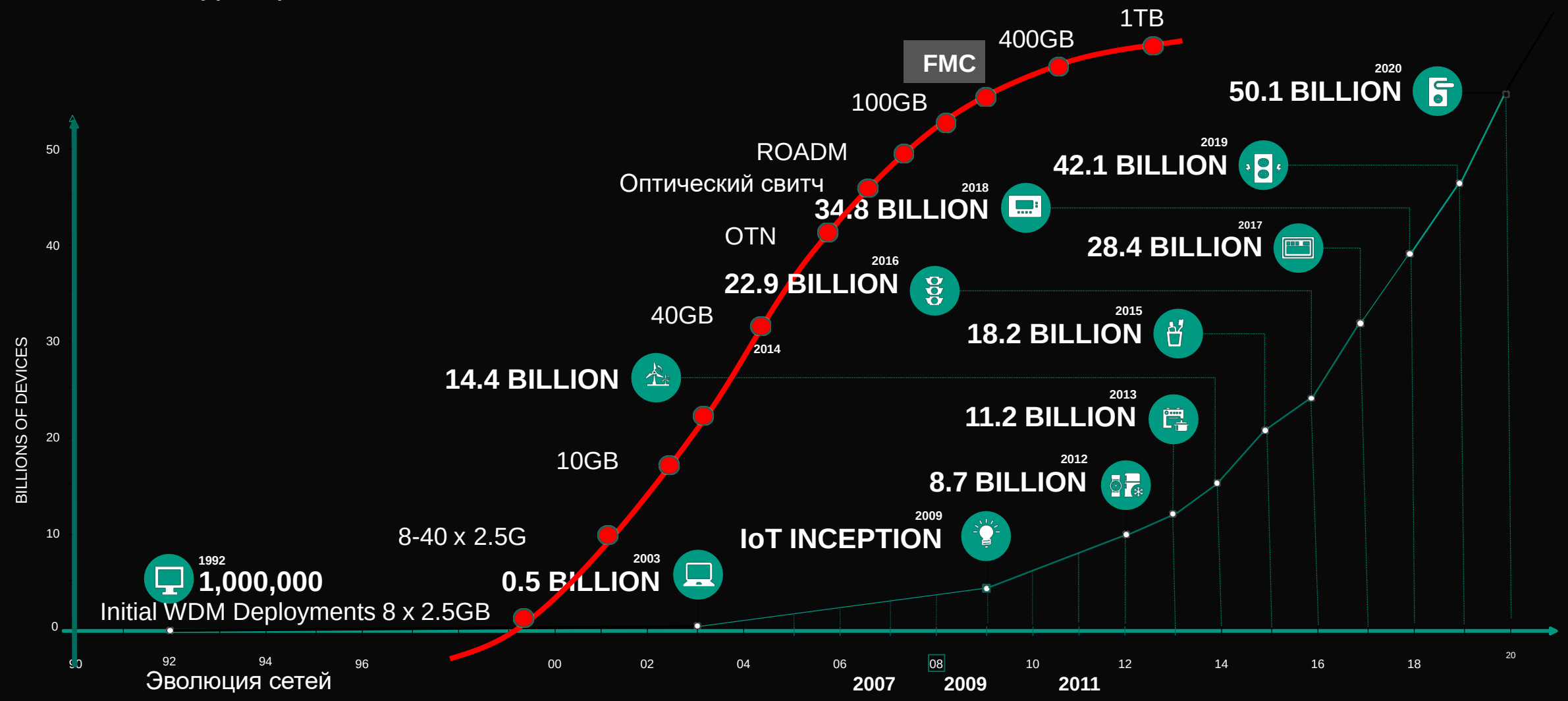
ВСТРАИВАЕМЫЕ УСТРОЙСТВА

БЫТОВАЯ ТЕХНИКА

ИНТЕЛЛЕКТУАЛЬНЫЕ ЗДАНИЯ

TEXT SLIDE

- *Закон Мура продолжает действовать в течение 50 лет*



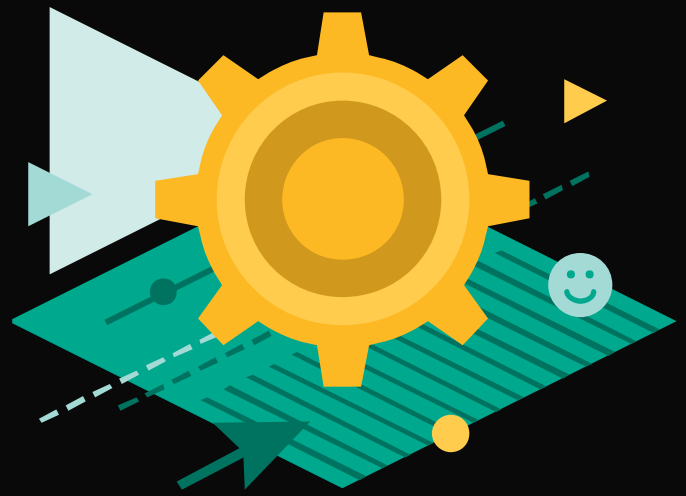
KASPERSKY lab

БЕЗОПАСНОСТИ МНОГО НЕ БЫВАЕТ

- *Затраты на безопасность должны быть пропорциональны ценности актива для злоумышленника*

- По мере утраты доверия начинается гонка «в глубину» между угрозами и средствами безопасности

КАК РЕШИТЬ ПРОБЛЕМУ?



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

ОСНОВНЫЕ ПРИНЦИПЫ БЕЗОПАСНОЙ OS

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

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)

KASPERSKY SECURE HYPERVISOR

- Kaspersky Secure Hypervisor это гипервизор 2-го типа, работающий на базе KasperskyOS.

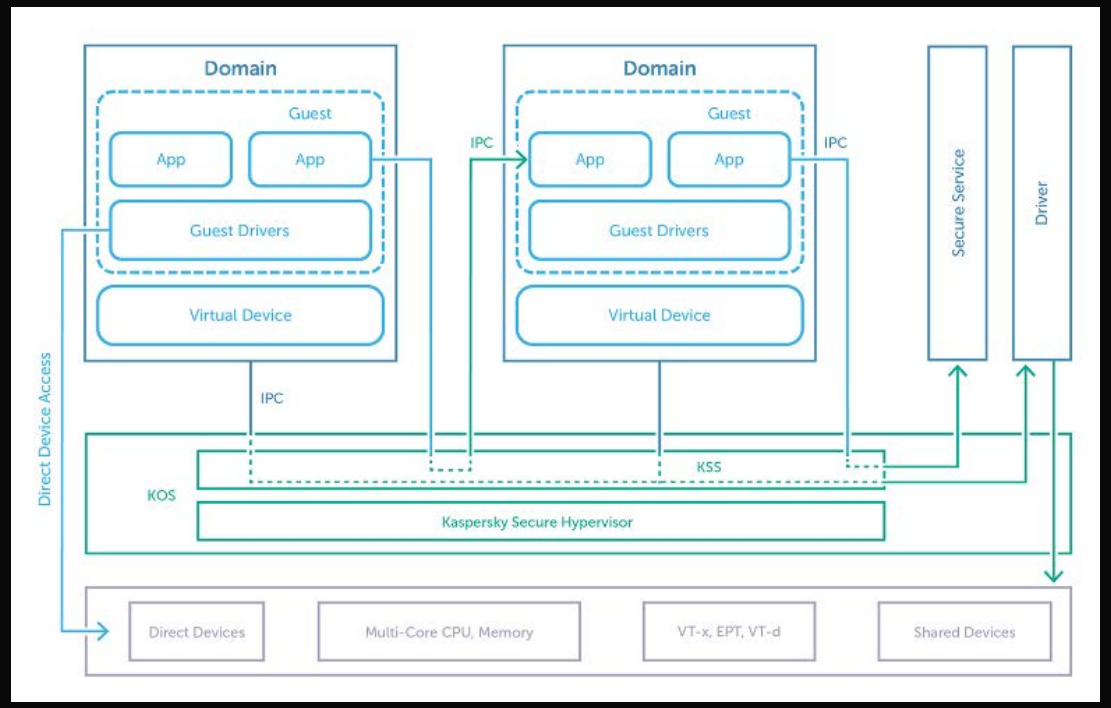
- KSH является частью безопасной платформы Лаборатории Касперского, направленной на минимизацию поверхности атаки небезопасного окружения. Предназначен для встраиваемых систем

Безопасный гипервизор состоит из трех основных компонентов:

- Привилегированный компонент уровня ядра отвечает только за управление аппаратными ресурсами (виртуализация ЦПУ, физической памяти, устройств).

- Компонент, исполняемый в пользовательском режиме, отвечает за основную поддержку окружения гостевых систем (конфигурацию окружения и эмуляцию необходимых устройств)

- третий компонент запускается в гостевой ОС и предоставляет приложениям в этой системе возможность безопасного взаимодействия с приложениями в других гостевых ОС, или безопасного доступа к окружению гостевой ОС и гипервизору.



KASPERSKYOS // ПРЕИМУЩЕСТВА

ВРОЖДЕННИЯ 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

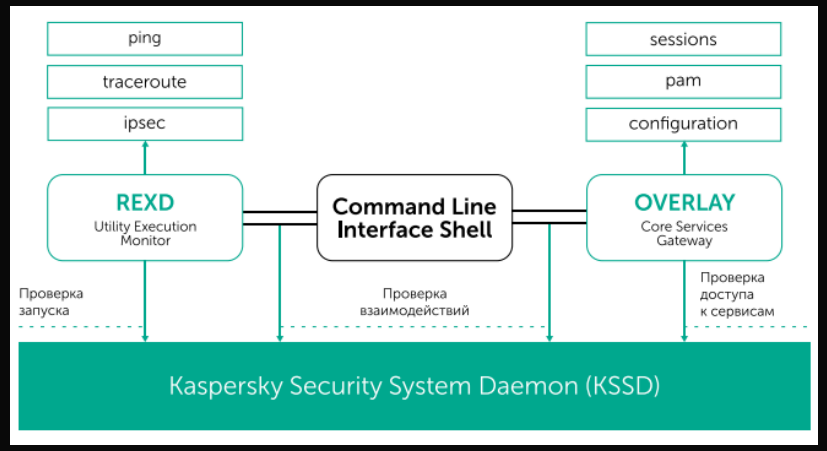
Безопасная архитектура спроектирована таким образом, чтобы отделить функции безопасности от бизнес-логики приложений; благодаря этому настройка политик безопасности и разработка приложений становятся проще

СЕРВИСНЫЙ МАРШРУТИЗАТОР

- предоставление сервисов NAT, Firewall
- маршрутизация
- организация защищенных сетевых туннелей для объединения офисов компаний (IPsec VPN)
- организация удаленного доступа к локальным ресурсам в сетях предприятий L2TP, PPTP, OpenVPN
- фильтрация сетевых данных по различным критериям
- AAA (user accounting and policy)
- ограничение скорости (Shaper)
- ограничение трафика и времени (Limiter)
- HTTP редиректор

ПЕРЕЧЕНЬ ОБОРУДОВАНИЯ

- ESR-10
- ESR-100
- ESR-200
- ESR-1000
- ESR-1200
- ESR-1700
- ESR-12V
- ESR-12F

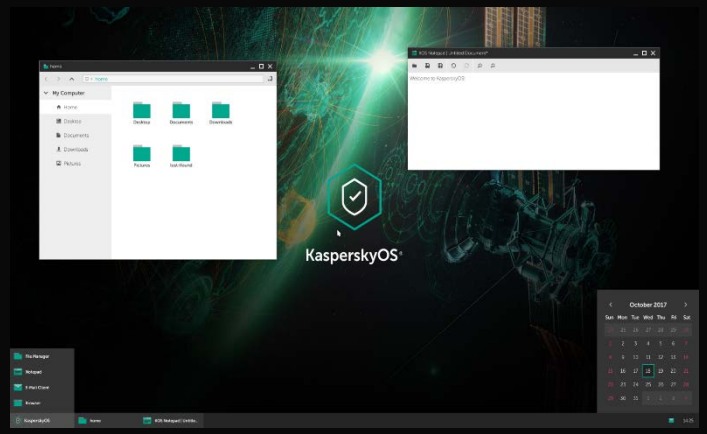


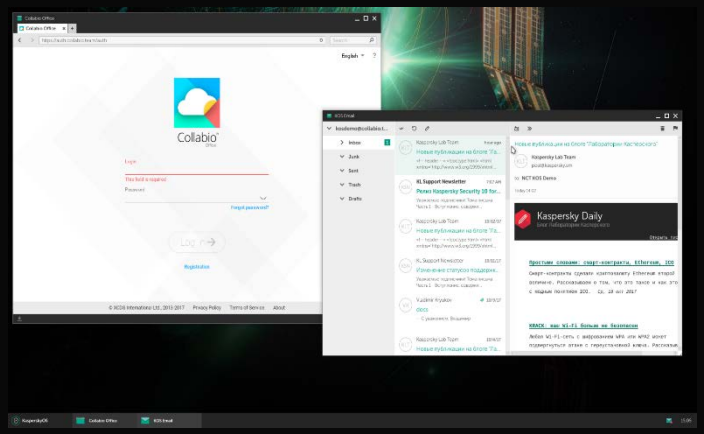
МАРШРУТИЗИРУЮЩИЙ КОММУТАТОР L3

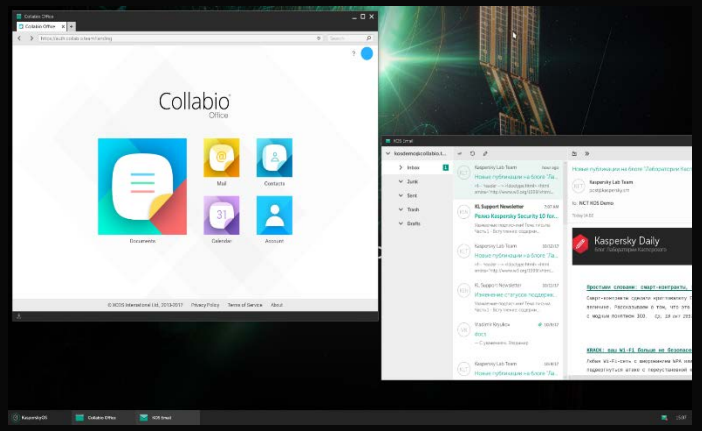
Коммутирующая матрица	Модуль коммутирующей матрицы на основе процессора Marvell 98DX4122, 32-разрядный, 800 МГц, архитектура ARM, 128MB оперативной памяти
Коммутируемые порты	Под 1Gigabit: 24 порта SFP; Под 10Gigabit: 2 порта SFP+
Порты управления	1 порт RJ-45 10/100/1000 Base-T; 1 порт SFP 1000 Base-LX; 1 порт RS-232
Интерфейсы	1 порт, USB 2.0; 1 порт VGA (D-SUB15)
Индикация	Индикатор состояния системы; индикаторы активности коммуникационных портов; индикаторы скорости соединения коммуникационных портов
Размер таблицы MAC адресов	До 128 000 записей, аппаратно поддерживается 16 000 записей
Виртуальные локальные сети	До 4096 сетей VLAN
Протоколы маршрутизации	IGMP v1, v2, v3; RIP v2; OSPFv2; BGPv4; VRRP v3; ECMP
Протоколы управления	SNMP v1, v2C, v3; Telnet, SSH, CLI
Методы аутентификации	RADIUS, TACACS+, DACL, Secure Shell (SSH)
Поддерживаемые стандарты	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1s, IEEE 802.1ad

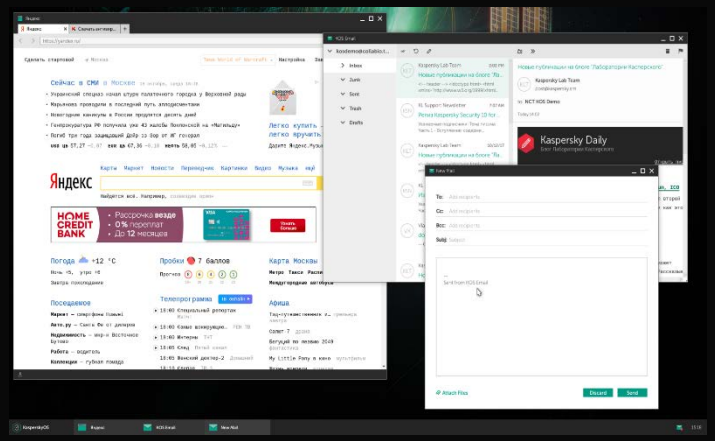
ДЛЯ РАБОЧИХ СТАНЦИЙ И ТОНКИХ КЛИЕНТОВ

- Защищенная/доверенная рабочая станция с использованием десктопоной версии KasperskyOS
- Примера использования:
  - Защищенный/доверенный документооборот с использованием приложений от МойОфис
  - Защищенный тонкий клиент для удаленного администрирования ИТ инфраструктуры
  - Защищенный тонкий клиент для VDI









PLC ДЛЯ SMART BUILDING

KASPERSKYOS

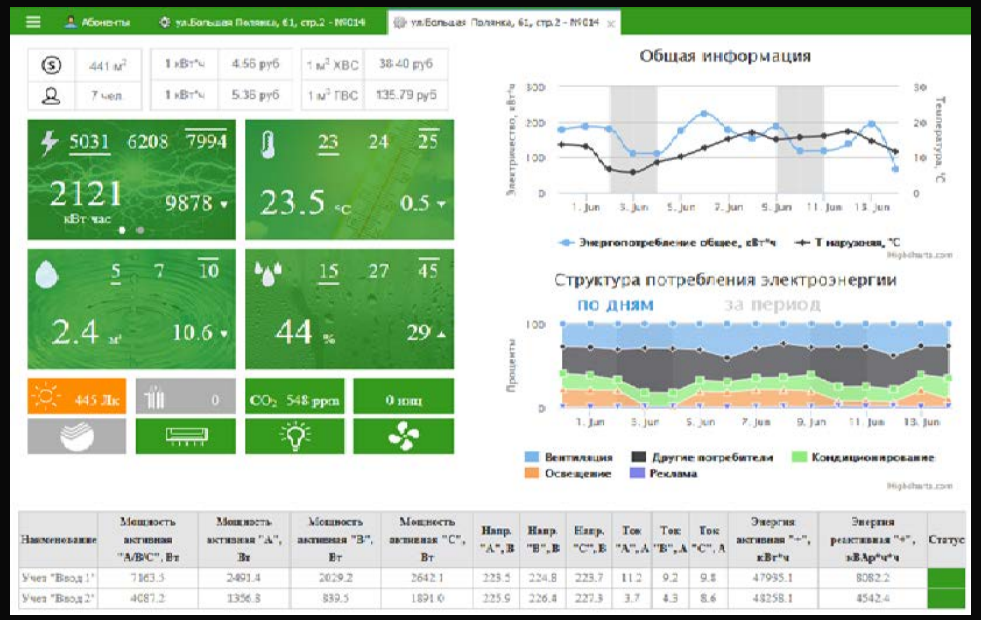
- Безопасность с нуля (единственный способ защитить IoT)
  - ✓ Изоляция всех доменов безопасности
  - ✓ Минимизация урона от уязвимостей
  - ✓ Защита важных данных (ключей шифрования)
  - ✓ Безопасная загрузка

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



LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab