Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

KasperskyOS как платформа для обеспечения комплексной безопасности вертикально-интегрированной АСУ ТП

Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Безопасность АСУ ТП

Современные АСУ ТП – это очень сложные системы

- Распределенная архитектура
- Интеграция с ERP системами и IT инфраструктурой
- IIoT
- Удаленный доступ
- Industry 4.0

Информационная безопасность АСУ ТП – комплексный вопрос

- Управление предприятием
- Технологический аспект
- Человеческий фактор
- Поддержка и обслуживание
- Внешнее окружение

И множество других аспектов

Вопросы информационной безопасности часто недооцениваются

- Экономическая составляющая играет очень важную роль

Наша цель – разработка технологических решений для обеспечения безопасности, удовлетворяющих всем потребностям пользователей

Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

KasperskyOS – операционная система для безопасных решений

Микроядерная архитектура, ядро разделения

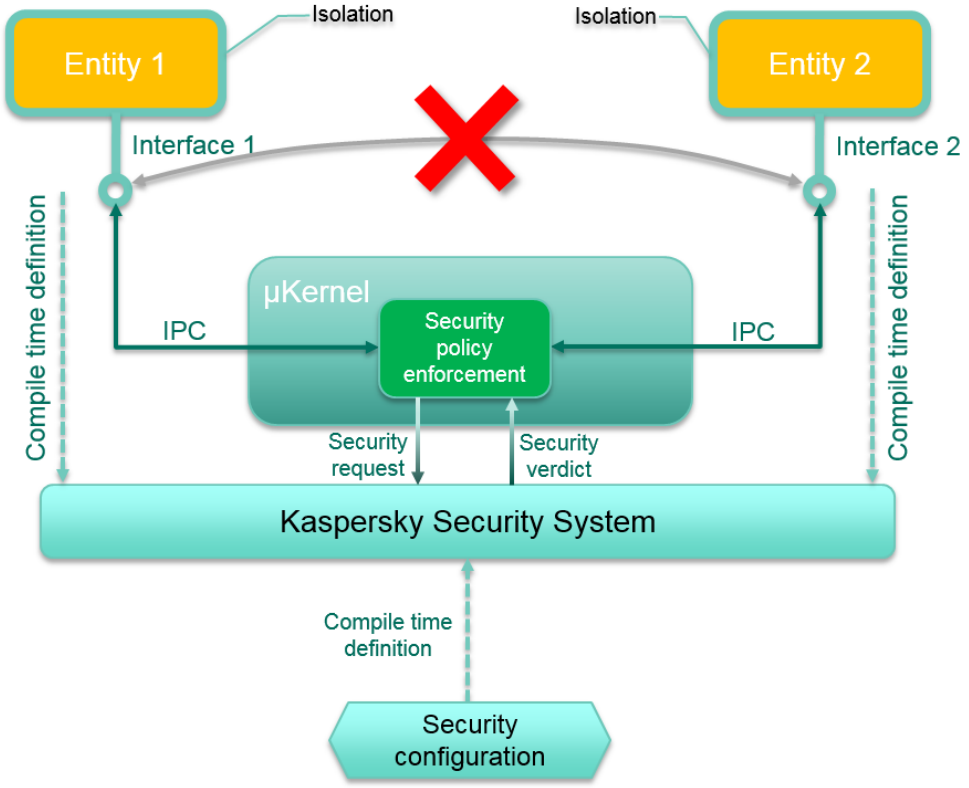
- Чрезвычайно малая поверхность атаки (3 системных вызова)
- Единственный механизм IPC, контролируемый микроядром
- Типизированные взаимодействия, предоставляют удобные механизмы контроля
- Подсистема безопасности **Kaspersky Security System**
- Единственная точка применения вердиктов безопасности

Kaspersky Security System, вычисление вердиктов безопасности

- Поддержка большого количества формальных моделей безопасности одновременно
- Исключительная гибкость при описании свойств безопасности решения
- Исполняемый код политик безопасности генерируется на основе высокоуровневого описания заданного в терминах формальных моделей безопасности

Поддержка **POSIX**

- Легкость переносимости готового ПО



В совокупности это дает:

- Возможность построения решений с заданными свойствами безопасности
- Позволяет минимизировать объем доверенной кодовой базы

Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Kaspersky Secure Hypervisor – виртуализация в KasperskyOS

Основные характеристики **Kaspersky Secure Hypervisor**

- Гипервизор второго типа для **x86 32/64**
- Аппаратная поддержка виртуализации
- Поддержка **KasperskyOS IPC** внутри виртуальной машины
- Набор доступных **«из коробки»** сервисов и паттернов безопасности
- Возможность взаимодействия с **Kaspersky Security System**
- Поддержка наиболее популярных гостевых ОС **(Windows, Linux, KasperskyOS)** без паравиртуализации
- Большой набор эмулируемых устройств **(Storage, HID, Network, Video)**
- Возможность **«**проброса**»** оборудования
- Компонентная архитектура, включая возможность кастомизации **backend** для эмулируемых устройств
- Статическая конфигурация виртуальной машины

Использование **Kaspersky Secure Hypervisor** позволяет

- Запускать компоненты АСУ ТП в их стандартном рабочем окружении **(**под управлением гостевой ОС**)**
- Реализовать новый дополнительный независимый уровень безопасности для гостевой операционной системы

Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Защита PLC на примере CODESYS runtime

CODESYS runtime – популярная среда исполнения для **PLC**

- **CODESYS runtime** реализует большое количество функций, включая сетевые коммуникации и управление устройствами
- Путем эксплуатации сетевого стека появляется возможность нарушить правильную работу системы

При использовании **KasperskyOS** появляется возможность существенного повышения безопасности системы

- Требуется изолировать коммуникационные компоненты от логики управлением оборудования
- В соответствии с моделью угроз требуется задать набор политик, обеспечивающих безопасное функционирование устройства

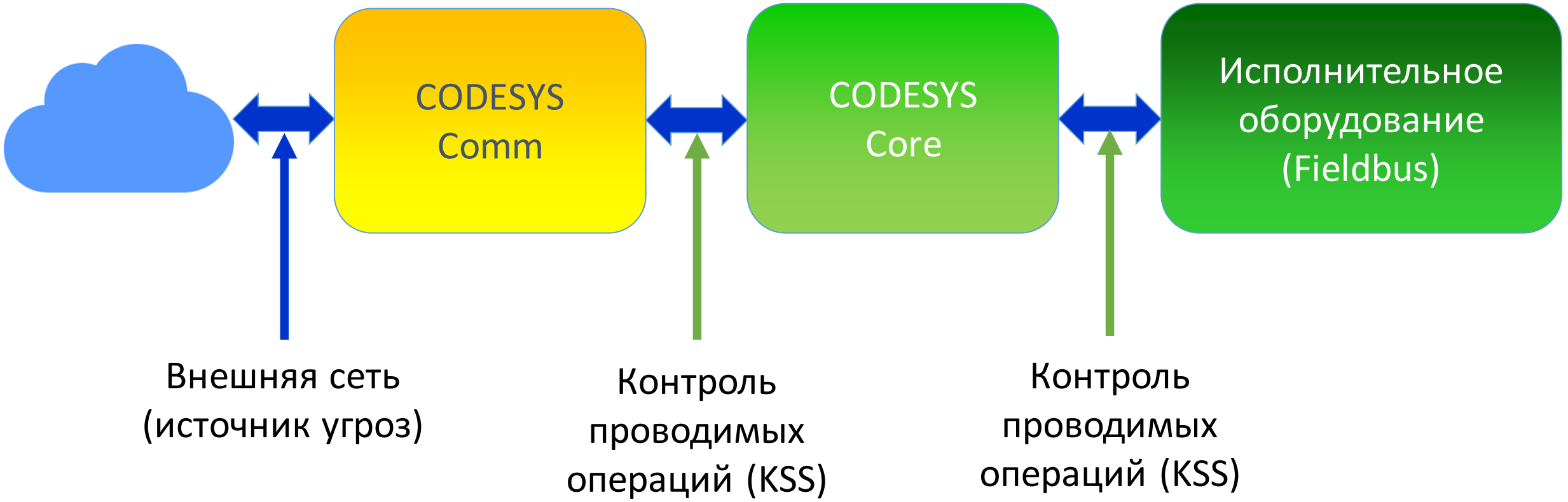
Лаборатория Касперского, совместно к компанией **BE.services** адаптировала **CODESYS runtime** для работы под управлением **KasperskyOS**

Функциональность **CODESYS runtime** была разделена на **2** части

- **CODESYS Comm:** отвечает за взаимодействия по внешним каналам связи
- **CODESYS Core:** реализует бизнес-логику прошивки

Взаимодействие между компонентами производится с использованием интерфейса, определенного таким образом, чтобы имелась возможность контроля управляющих воздействий на компонент **CODESYS Core** со стороны компонента **CODESYS Comm**

Защита PLC на примере CODESYS runtime



Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Защита SCADA на примере PcVue Secure

PcVue Secure – защищенная **SCADA** на основе **PcVue** и технологий **KasperskyOS**

- **KasperskyOS** обеспечивает безопасную среду исполнения программных компонентов
- **Kaspersky Secure Hypervisor** позволяет запустить **SCADA** в системе и включить ее в отдельный домен безопасности

Основная идея заключается в реализации дополнительного независимого уровня контроля за поведением системы

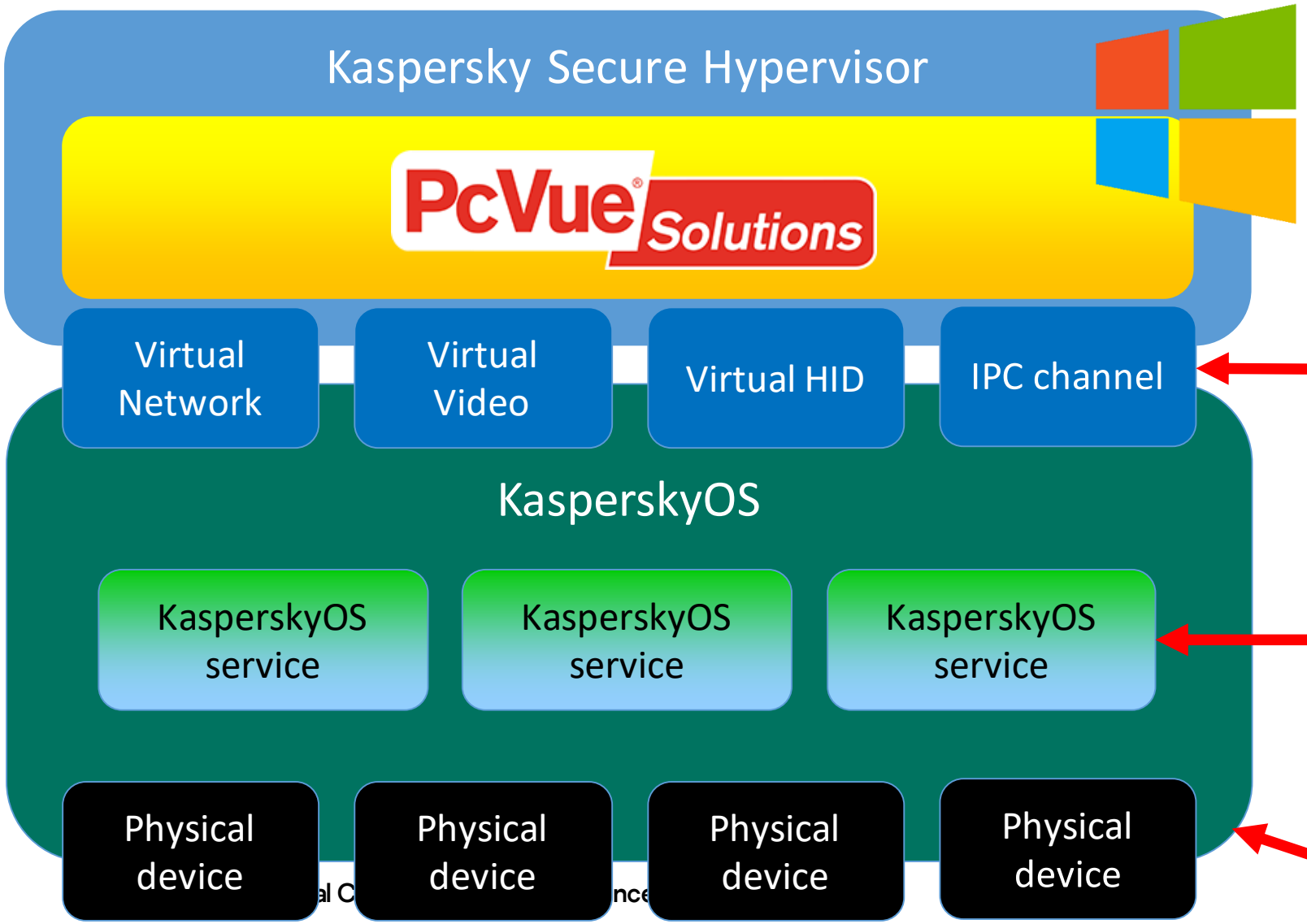
Критически важные сервисы безопасности (шифрование, управление доступом, принятие решений, мониторинг состояния системы, аудит) выносятся за пределы гостевой ОС и реализуются в доверенном окружении.

Используя этот подход можно реализовать множество функций, позволяющих существенно повысить безопасность решения, включая:

- Безопасное хранение данных журнала событий
- Расширенную аутентификация
- Ролевой доступ к системе
- Безопасную загрузка и безопасное обновление
- Централизованное администрирование
- Безопасный удаленный доступ (для пользователей и для администратора)
- Безопасную работу с оборудованием
- **IDS** и **IPS**

PcVue Secure

Защита **SCADA** на примере **PcVue Secure**



SCADA решение работает в стандартном окружении в «песочнице»

Доступ к оборудованию находится под контролем

Сервисы, обеспечивающие безопасность работают в контролируемом окружении

- СКЗИ
- Аудит
- Дополнительные возможности

Контроль осуществляется при помощи KSS

Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

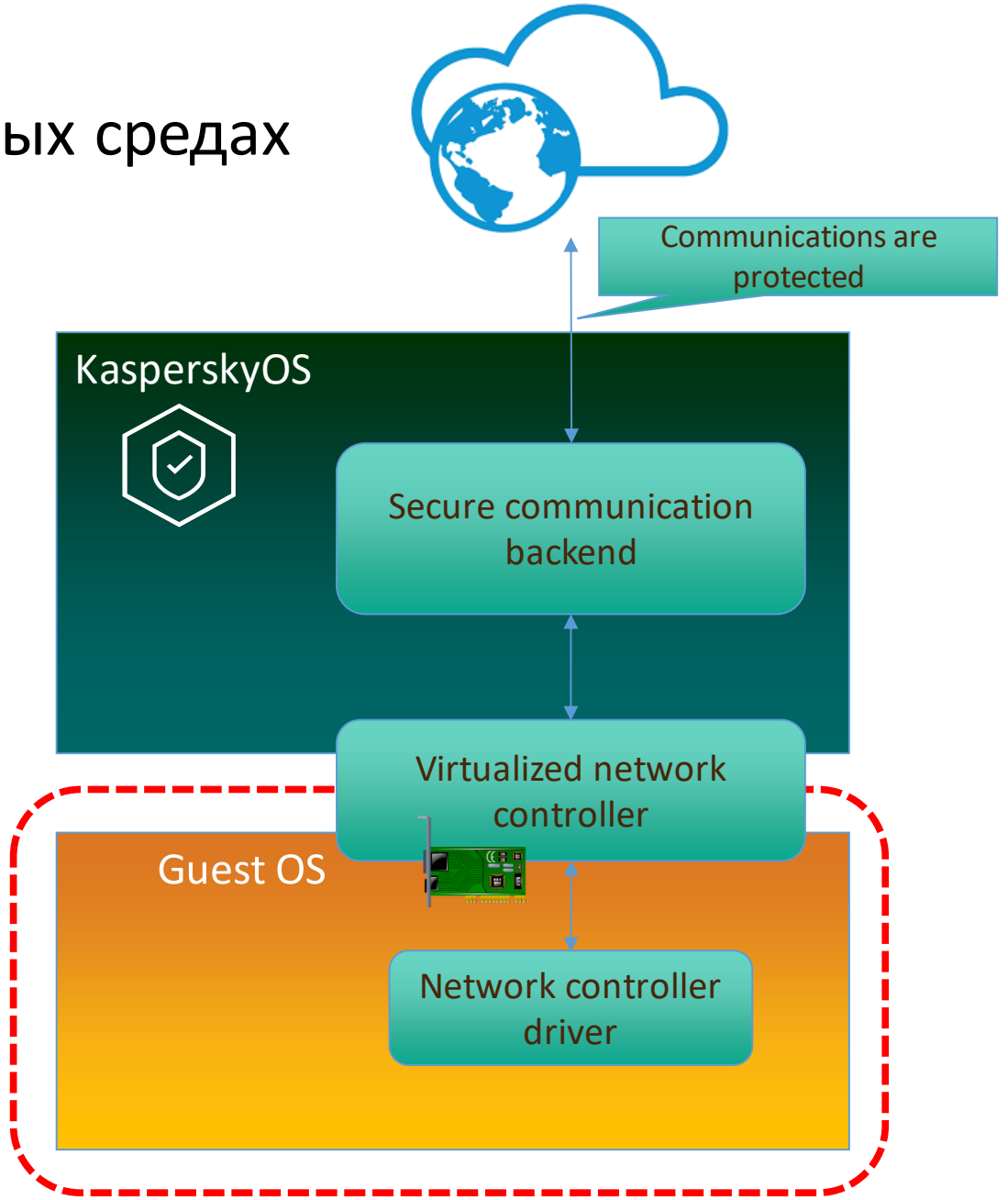
Защита коммуникаций в распределенных средах

Организация частной виртуальной сети

- Использование средств виртуализации позволяет реализовать независимый от гостевой ОС слой шифрования данных, что позволяет реализовать виртуальные частные сети с высоким уровнем защищенности
- Решается проблема совместной работы сервисов с высокими требованиями к информационной безопасности и прочих сервисов в рамках единой ИТ инфраструктуры

Сетевое оборудование на базе **KasperskyOS**

- Лаборатория Касперского совместно с партнерами **(Kraftway, Eltex)** разрабатывает сетевое оборудование для задач, требующих повышенного уровня защищенности



Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

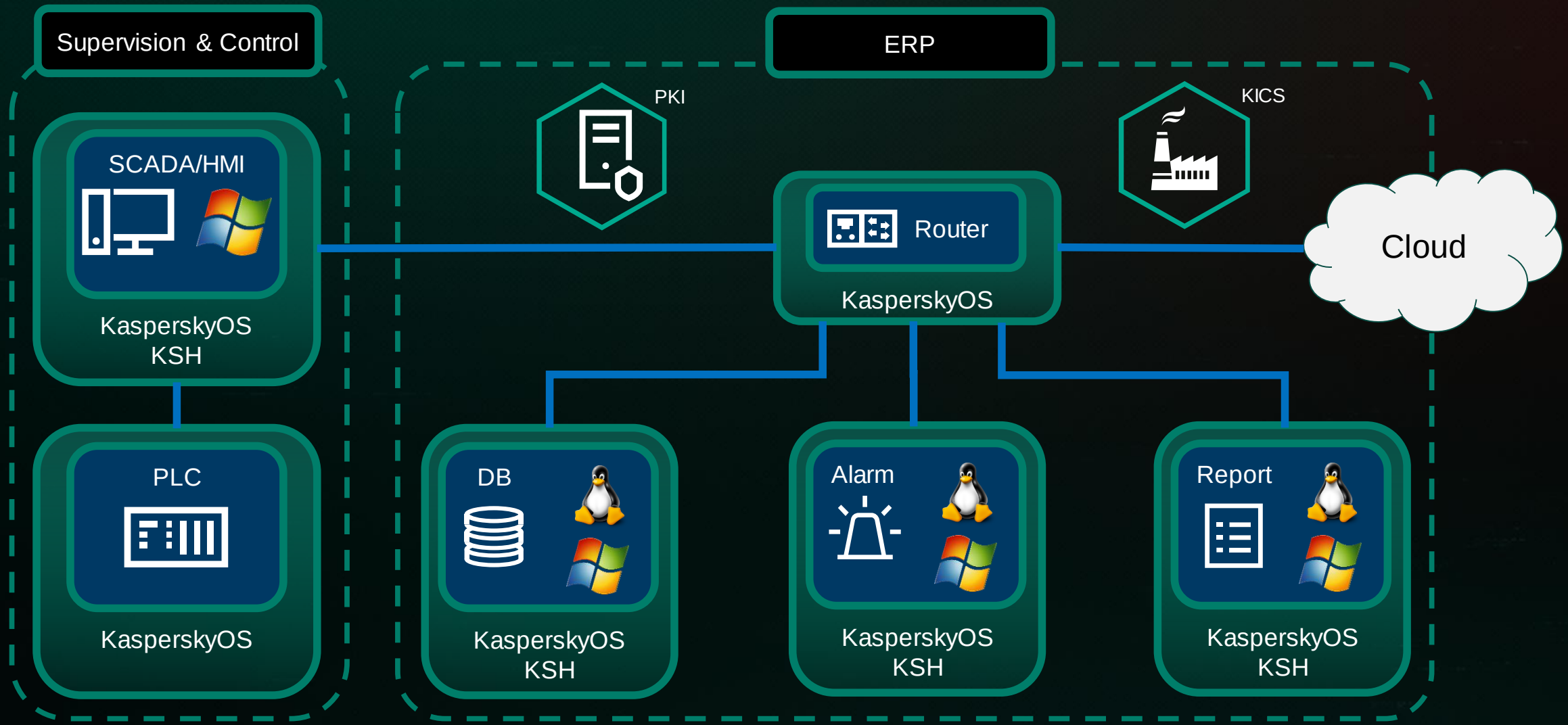
Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Обзор технологий KasperskyOS для АСУ ТП



Agenda

Безопасность АСУ ТП

Что такое KasperskyOS?

Kaspersky Secure Hypervisor

Защита PLC

Защита SCADA

Защита инфраструктуры

Обзор технологий

Вопросы

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

kaspersky.com