kaspersky

Kaspersky OT CyberSecurity

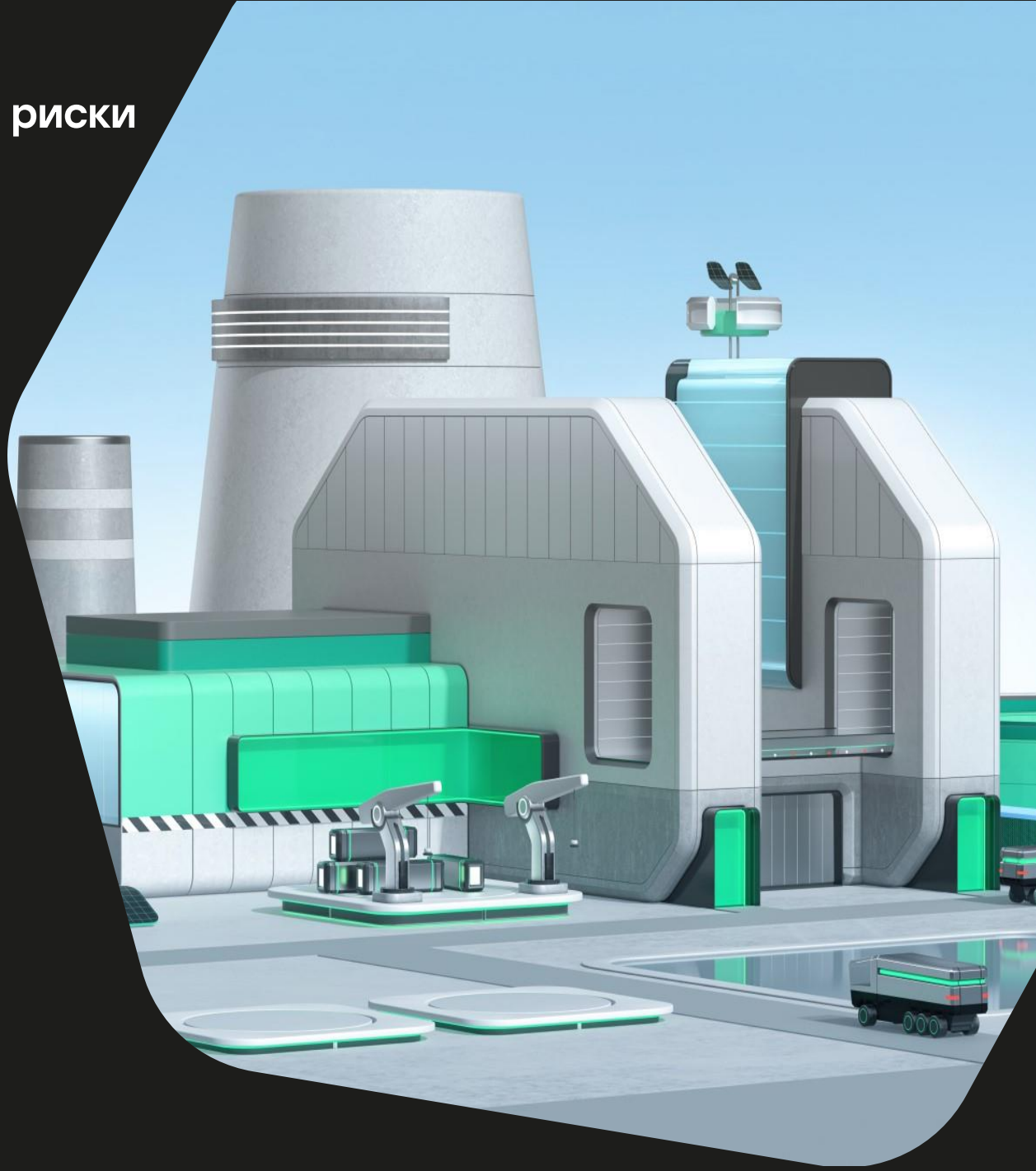
Экосистема промышленной безопасности

Промышленные предприятия – цифровизация и риски

Сегодня процесс цифровизации – синоним конкурентоспособности и эффективности в том числе и для промышленных предприятий.

Обеспечение стабильности соединений в промышленных сетях, повышение их надежности и оптимизация операционных затрат – важные задачи.

Однако, промышленные системы и сети – это всегда более высокие риски и дополнительные требования.



Современные ИБ-реалии

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 ухода ИБ-вендоров, изменение целей киберпреступников и связанных с этим тактик и техник

Началась активная фаза импортонезависимости

АСУ в 2023

Рост интереса хактивистов к системам автоматизации

Увеличение числа APT-угроз в промышленном сегменте

31,9%* компьютеров АСУ в России были атакованы ВПО в H1 2023 года

Атаки для сбора всевозможного рода информации, например, связанных с развитием промышленных секторов экономики

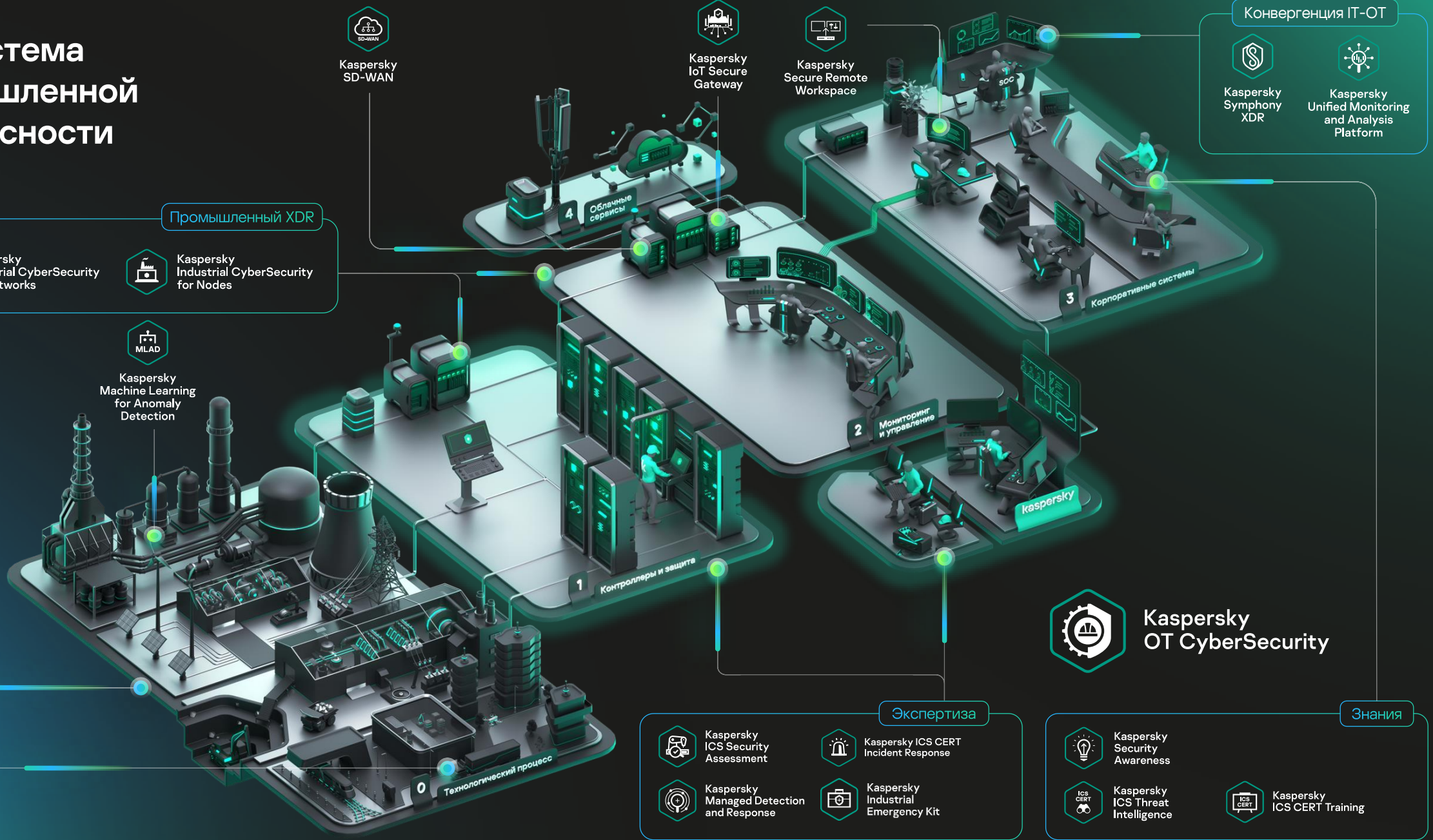
Атаки с целью закрепиться на «черный день», а также с целью нанесения прямого ущерба

Главные факторы активности атакующих — геополитическая напряженность

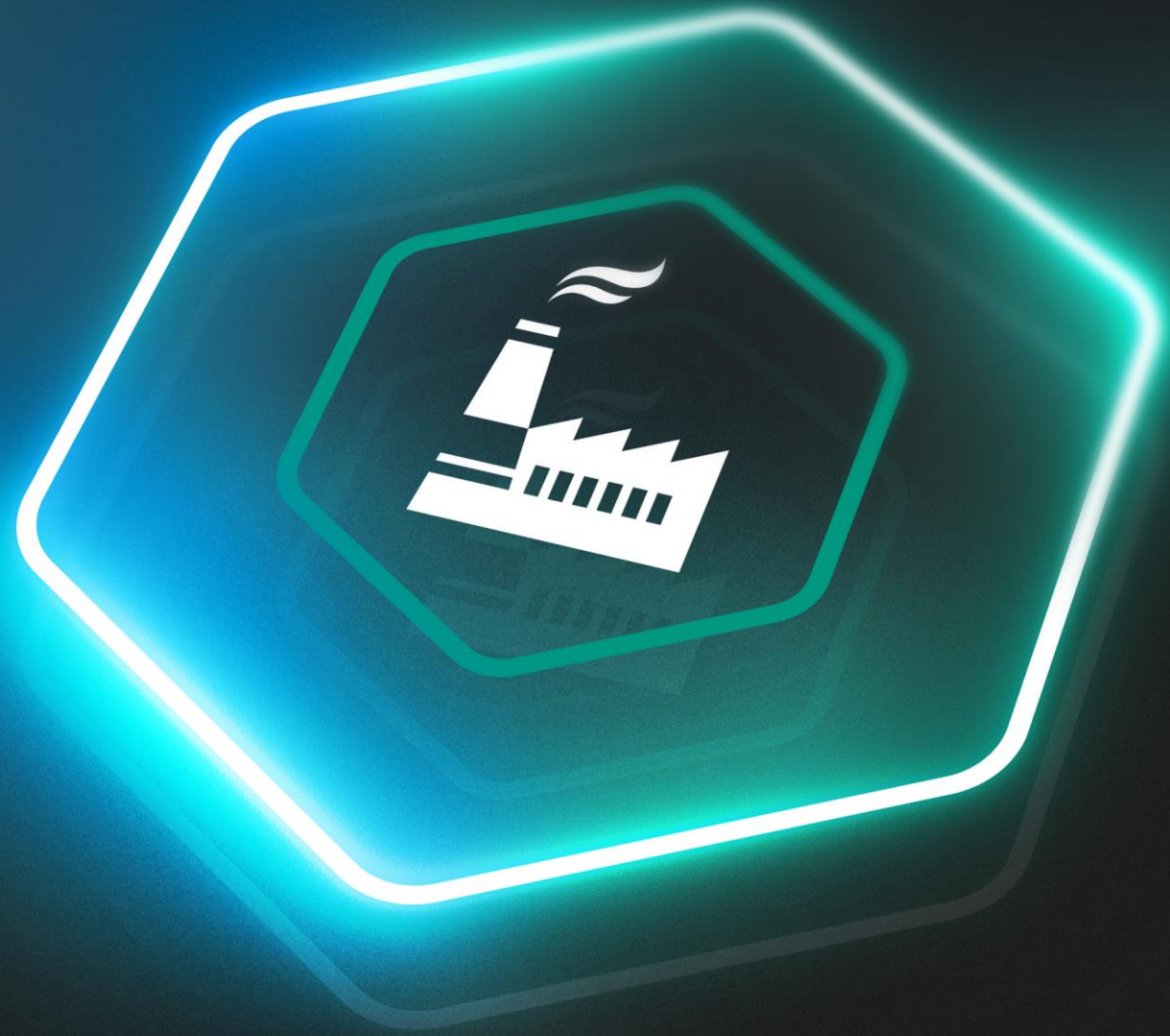
Необходимость соответствовать требованиям регулирующих органов побуждают организации к внедрению специализированных средств киберзащиты промышленных инфраструктур.

Kaspersky ICS CERT, сентябрь 2023 г.

Экосистема промышленной безопасности



XDR платформа Kaspersky Industrial CyberSecurity



Kaspersky
Industrial
CyberSecurity

Специализированное решение
для мониторинга сети АСУ ТП и защиты
конечных узлов промышленной среды.
Представляет собой специализированную
промышленную платформу класса XDR.

Ключевые преимущества

Признание

Более 10 лет активного
присутствия в сфере. Признана
компанией года на рынке
промышленной кибер-
безопасности.
Frost and Sullivan – 2020.

Совместимость

Более 100 сертификатов
совместимости с
решениями ведущих
мировых и отечественных
вендоров АСУ ТП

Сертификация

Продукты разработаны
с учетом соответствия
требованиям 187-ФЗ о защите
КИИ и сертифицированы
ФСТЭК и ФСБ России

Специализированная защита

Продукты не влияют
на технологический
процесс
и работают в
распределенных
и изолированных сетях

XDR платформа нативного типа для защиты промышленных систем автоматизации

Сеть: детектирование и реагирование

Анализ и разбор трафика от Endpoint сенсоров и сетевых проб. Обнаружение аномалий тех. процесса, сетевых угроз, корреляция с EDR телеметрией и интеграция с сетевым оборудованием для реагирования.

Управление активами, рисками и аудит

Пассивный и активный опрос активов, аудит безопасности с технологией OVAL, выявление уязвимостей и рисков. Ситуационная осведомленность и отчетность.

Узлы: детектирование и реагирование

Защита конечных точек, контроль устройств и приложений. Граф расследования угроз и реагирование с EDR. До 16 модулей безопасности и широчайшее покрытие промышленной инфраструктуры.

Архитектура нативной OT XDR-платформ

Kaspersky Industrial CyberSecurity for Nodes

Инструменты класса
EPP и EDR, аудит

- Сервер
- Рабочая станция
- Портативные сканеры

Kaspersky Industrial CyberSecurity

- Единая консоль
- Нативная интеграция
- Кросс-продуктовые сценарии
- Общий kill-chain

Управление рисками и активами

- Пассивное обнаружение компонентов и уязвимостей OT
- Дополнительный активный опрос, ориентированная на риск ситуационная осведомленность и отчетность

Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика
(ICS DPI, IDS)

- Сервер
- Сенсор

Статус защиты

Аудит безопасности

Сетевые коммуникации

Передача телеметрии хоста

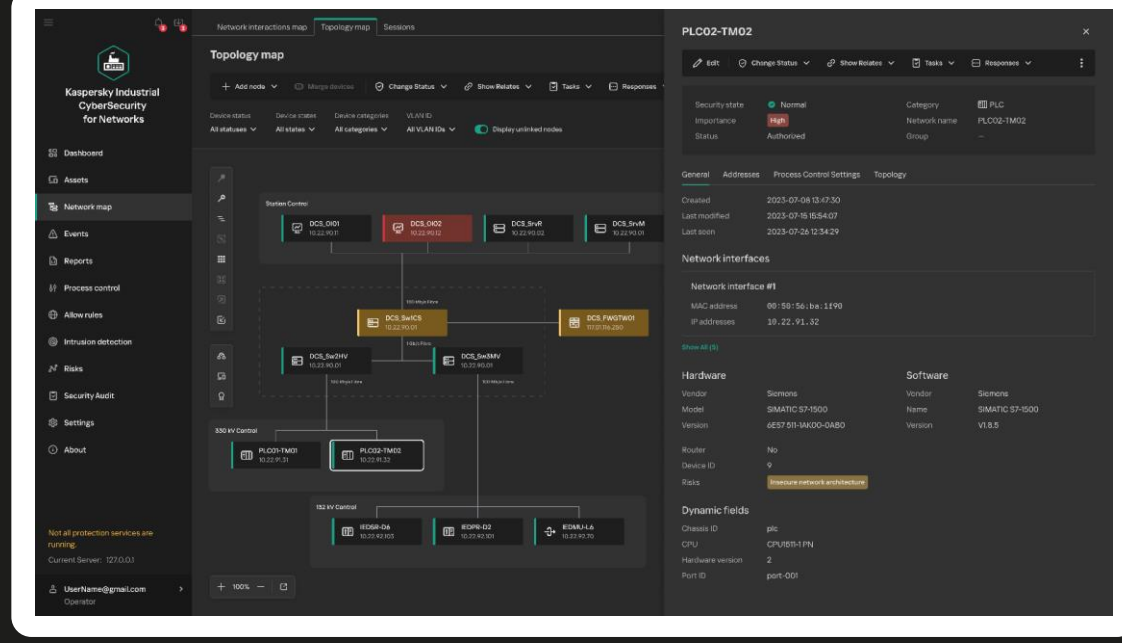
Контроль оборудования

Реагирование на инциденты

KICS for Networks базовая архитектура внедрения

Программная или виртуальная поставка

Kaspersky Industrial CyberSecurity for Networks



Анализ сетевого трафика, обнаружение угроз и реагирование

Пассивный мониторинг промышленной сети

kaspersky

Kaspersky SD-WAN. Kaspersky Industrial CyberSecurity

Надежность и безопасность распределенных промышленных сетей

Сетевые особенности промышленных предприятий

Требования к форм-фактору устройств

Специфика промышленных сетей зачастую требует, чтобы устройства были исполнены в компактном форм-факторе и комбинировали в себе несколько сетевых функций

Серьезные риски безопасности и катастроф

Вывод из строя промышленных объектов – это серьезный риск, поэтому сетевые решения должны быть защищены с самого начала, т.е. с момента их развертывания

Удаленность объектов и отсутствие персонала

Объекты малой автоматизации зачастую не имеют технических специалистов на местах, поэтому развертывание сети, управление ею и мониторинг должны осуществляться удаленно

Высокие требования к отказоустойчивости систем

Промышленные системы управления (ICS) и сбора данных (SCADA) нуждаются в стабильных каналах связи с высоким качеством обслуживания

Автоматизация

Программно-определяемые технологии позволяют автоматизировать развертывание сети и упростить управление ею

Надежность

Механизмы программно-определяемых сетей помогают повысить надежность сетевой инфраструктуры и обеспечить ее безопасность

Единое решение для надежности промышленных сетей

Kaspersky SD-WAN

Позволяет построить на предприятиях отказоустойчивую территориально распределенную сеть с централизованным управлением, а также обеспечить непрерывность производственных процессов

Kaspersky Industrial CyberSecurity for Networks

Поддерживает использование инфраструктуры SD-WAN, что позволяет организовать систему централизованного мониторинга и защиты для большого количества распределенных промышленных объектов

Kaspersky SD-WAN

SD-WAN – это решение для построения распределенных сетей, которое состоит из:

специальных маршрутизаторов (SD-WAN CPE)

Устанавливаются на объектах компании

интеллектуальной системы управления

Устанавливается в ЦОД или головном офисе

SD-WAN обеспечивает

Быстрое подключение новых объектов

Надежность сетевых подключений

Упрощенную миграцию в облако

Упрощенное управление сетью

Поддержку различных каналов связи и их комбинаций

Централизацию политик безопасности и сетевых настроек

Безопасную работу распределенных команд

Что Kaspersky SD-WAN предлагает промышленным предприятиям?

Быстрое подключение промышленных объектов с использованием существующих каналов связи

Управление и мониторинг всей сети через единый веб-интерфейс

Простая интеграция решений сетевой безопасности

Обеспечение гарантированного качества передачи данных приложений

Контроль используемых приложений в сети и централизованная политика безопасности

Использование отечественных аппаратных платформ, входящих в реестр ТОРП Минпромторга России

Что такое Kaspersky SD-WAN для промышленных сетей

Единое компактное решение

Архитектура решения и унифицированное телекоммуникационное оборудование (CPE) позволяют комбинировать различные сетевые функции в рамках одного компактного устройства

Интеграция средств защиты

Kaspersky SD-WAN позволяет легко интегрировать средства защиты «Лаборатории Касперского» и других производителей
в виде виртуальных сетевых функций (VNF)

Централизованный менеджмент

Технология Zero Touch Provisioning обеспечивает простое и быстрое подключение новых точек без предварительной настройки устройства (CPE), а управление и мониторинг осуществляются из единого веб-интерфейса

Надежность сетевых соединений

Использование любых доступных каналов связи, а также интеллектуальное управление трафиком обеспечивают высокое качество сетевого обслуживания и позволяют приоритизировать трафик ICS / SCADA

Мониторинг 100% инфраструктуры

Использование беспроводных каналов связи и компактных CPE для установки на отдаленные объекты и в труднодоступные места инфраструктуры увеличивает поверхность мониторинга промышленной сети

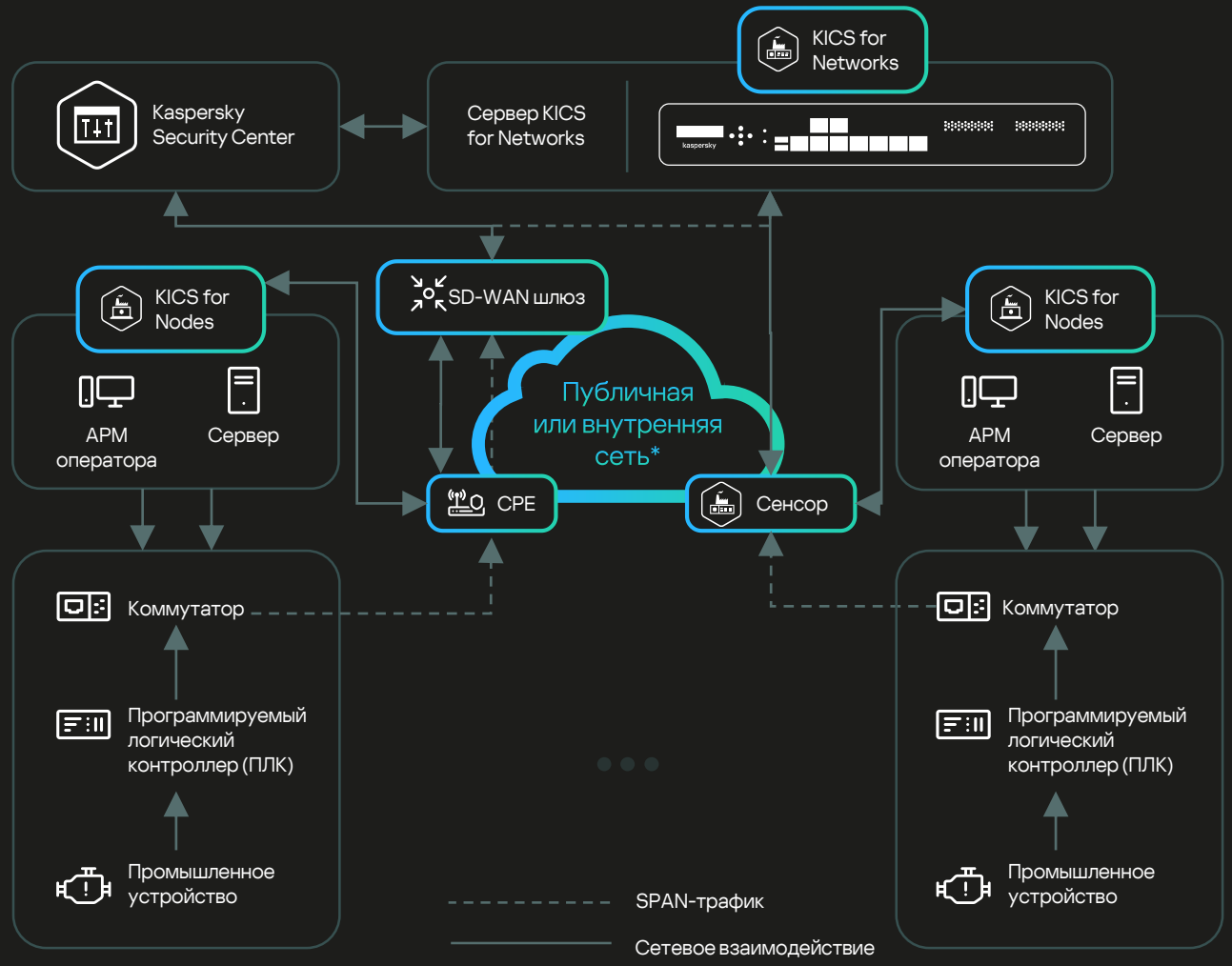
Единое решение для надежности промышленных сетей

Гибкость в создании распределённой инфраструктуры ИБ

Портативное устройство (CPE) для установки на объекты, которое совмещает различные задачи

Разделение каналов внутри сети SD-WAN и поддержка различных сценариев, которые не влияют друг на друга

Резервирование с помощью нескольких каналов связи



*Реализация сценария возможна в рамках одной АСУ ТП либо для связи с удаленным объектом по каналам связи LTE

Пример решения задач промышленных компаний с помощью Kaspersky SD-WAN

Энергетическая компания

Задачи / проблемы

Требуется обеспечить защиту всех подстанций и объектов по распределению электроэнергии

Большое количество объектов и высокая стоимость средств защиты для них

Необходима единая система управления сетью, контроля и защиты передаваемого между объектами трафика

Решение должно соответствовать требованиям регуляторов

Необходимо оптимизировать бюджет на построение системы защиты без ущерба для безопасности объектов

Решение

Использование KICS for Networks инфраструктуры SD-WAN позволяет с помощью CPE передавать трафик большого количества защищаемых объектов на средства защиты, которые развернуты на центральных объектах

Такая архитектура существенно сокращает затраты на средства защиты и реализует централизованный подход к построению инфраструктуры

Технологии решения Kaspersky SD-WAN позволяют изолировать различные типы трафика

Управление всеми устройствами CPE осуществляется из единой консоли

Решение Kaspersky SD-WAN и платформа Kaspersky Industrial CyberSecurity обладают необходимыми государственными сертификатами, а CPE (устройства KESR) входят в реестр РЭП Минпромторга России

Результат

Создана единая отказоустойчивая сеть передачи трафика и защиты объектов по распределению электроэнергии

Затраты на построение системы защиты благодаря использованию решения Kaspersky SD-WAN оптимизированы на 75%

Построенная система защиты объектов полностью соответствует требованиям регуляторов

Активируй будущее!

kaspersky