Kaspersky Industrial Cybersecurity Conference 2023

Kaspersky SD-WAN

Промышленные сценарии использования

Максим Каминский
BDM Kaspersky SD-WAN/SASE

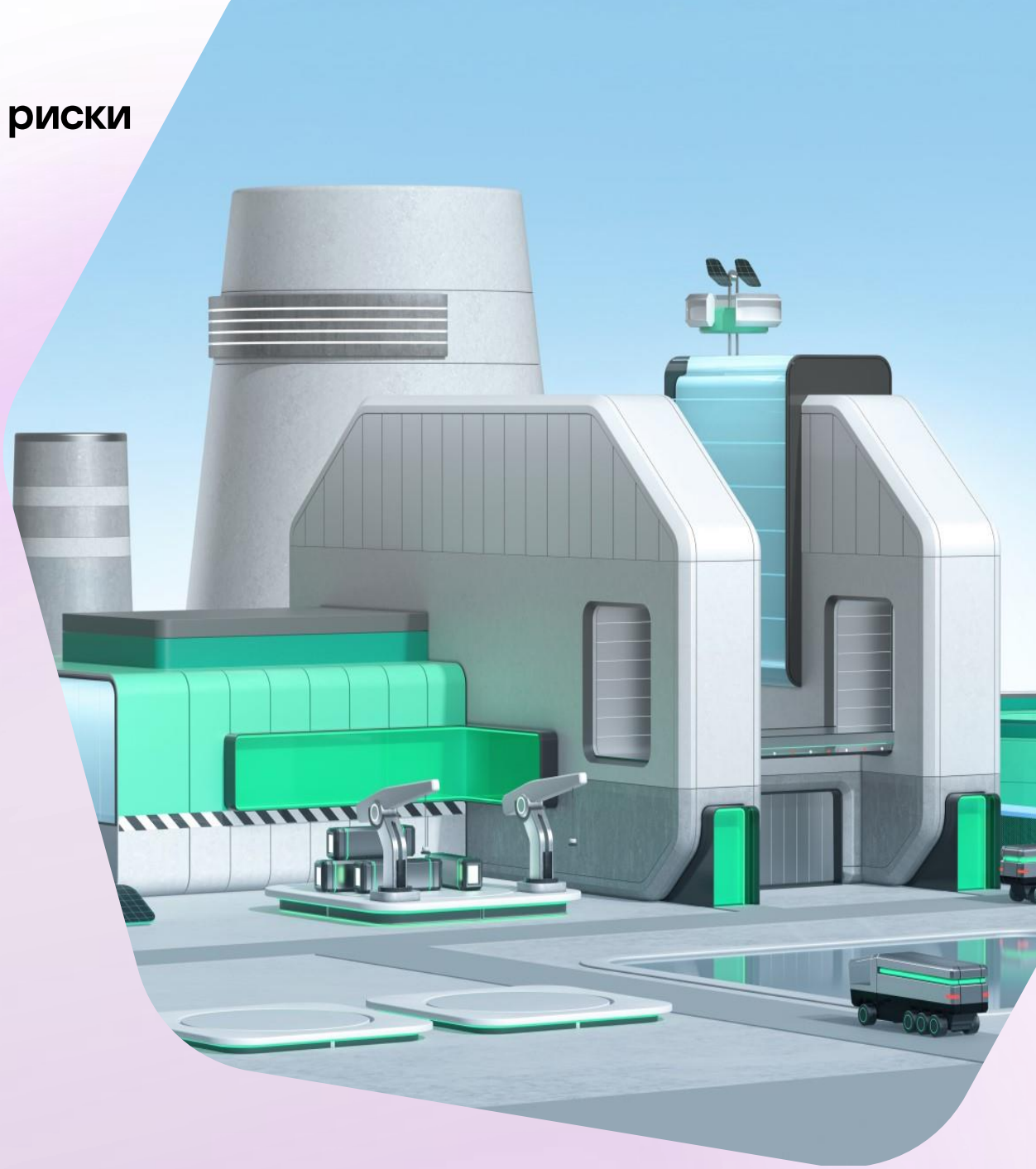
kaspersky

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 сети – это всегда более высокие риски и дополнительные требования.



> As digital business blurs the digital and physical worlds, digital breaches result in physical damage.

Gartner

Какие бывают промышленные объекты

Какие бывают промышленные объекты

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

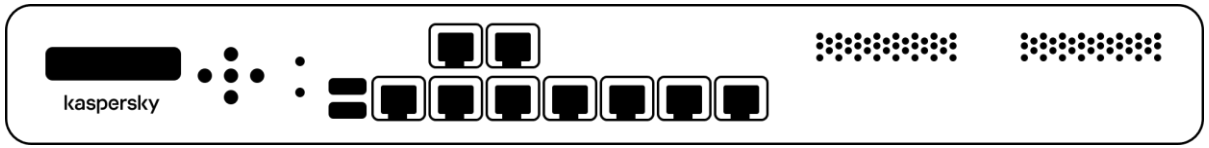
Высокие требования к отказоустойчивости систем

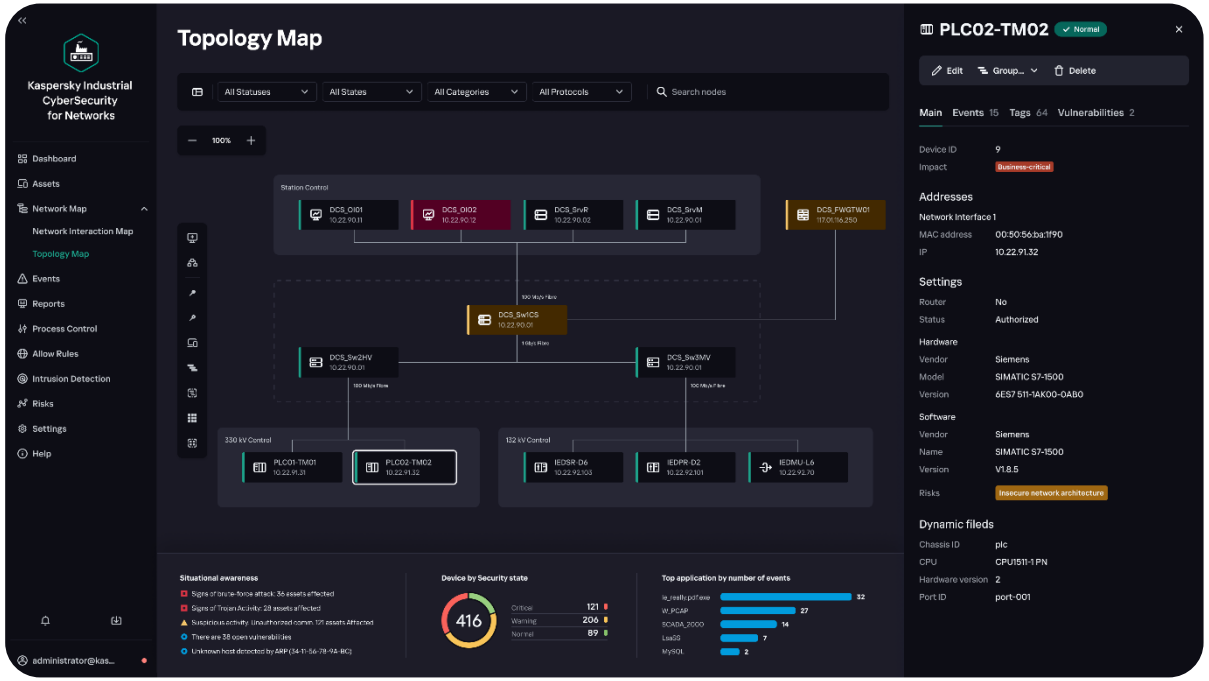
Промышленные системы управления (ICS) и сбора данных (SCADA) нуждаются в стабильных каналах связи с высоким качеством обслуживания

Сеть: развертывание и интерфейсы

Kaspersky ICS for Networks

Сервер Kaspersky ICS for Networks:
ПО или виртуализированное оборудование





Анализ сетевого трафика, обнаружение и реагирование

Телеметрия с конечных точек
и сетевой трафик

Опционально:
активный опрос (Active Polling)

Kaspersky ICS for Nodes

APM оператора

Сервер

Свитч

Программируемый логический контроллер (PLC)

Промышленное устройство

Пассивное подключение
к промышленной сети

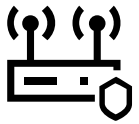
Автоматизация

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

Надежность

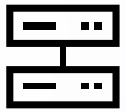
Механизмы программно-определяемых сетей помогают повысить надежность сетевой инфраструктуры и обеспечить ее безопасность

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

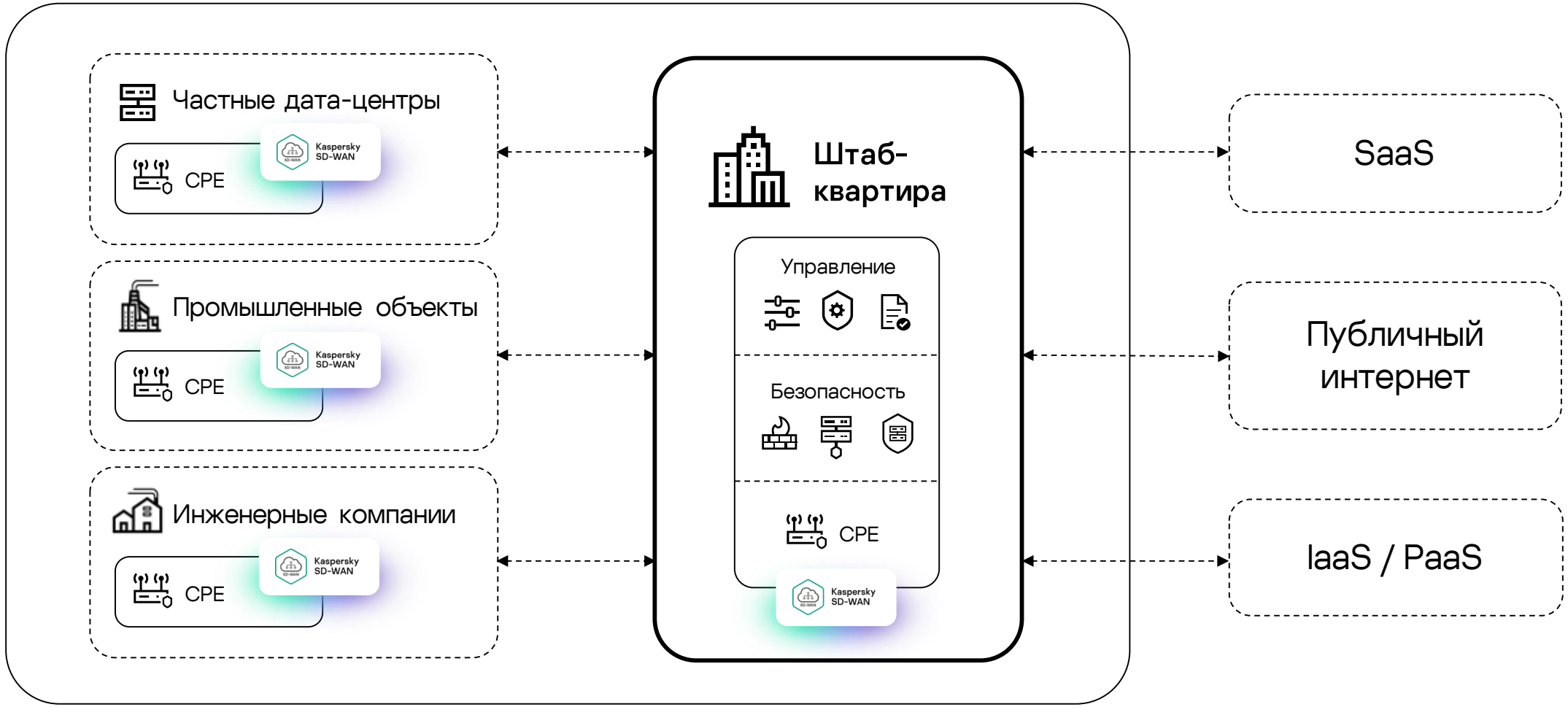
Поддержку различных каналов связи и их комбинаций

Централизацию политик безопасности и сетевых настроек

Безопасную работу распределенных команд

Просто о SD-WAN

Пример внедрения Kaspersky SD-WAN



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

Бескомпромиссная безопасность

Интегрированные сервисы защиты, мониторинг в реальном времени компонентов решения и централизованное развертывание политик обеспечивают безопасность сети и устройств с самого начала

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

Интеграция средств защиты

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

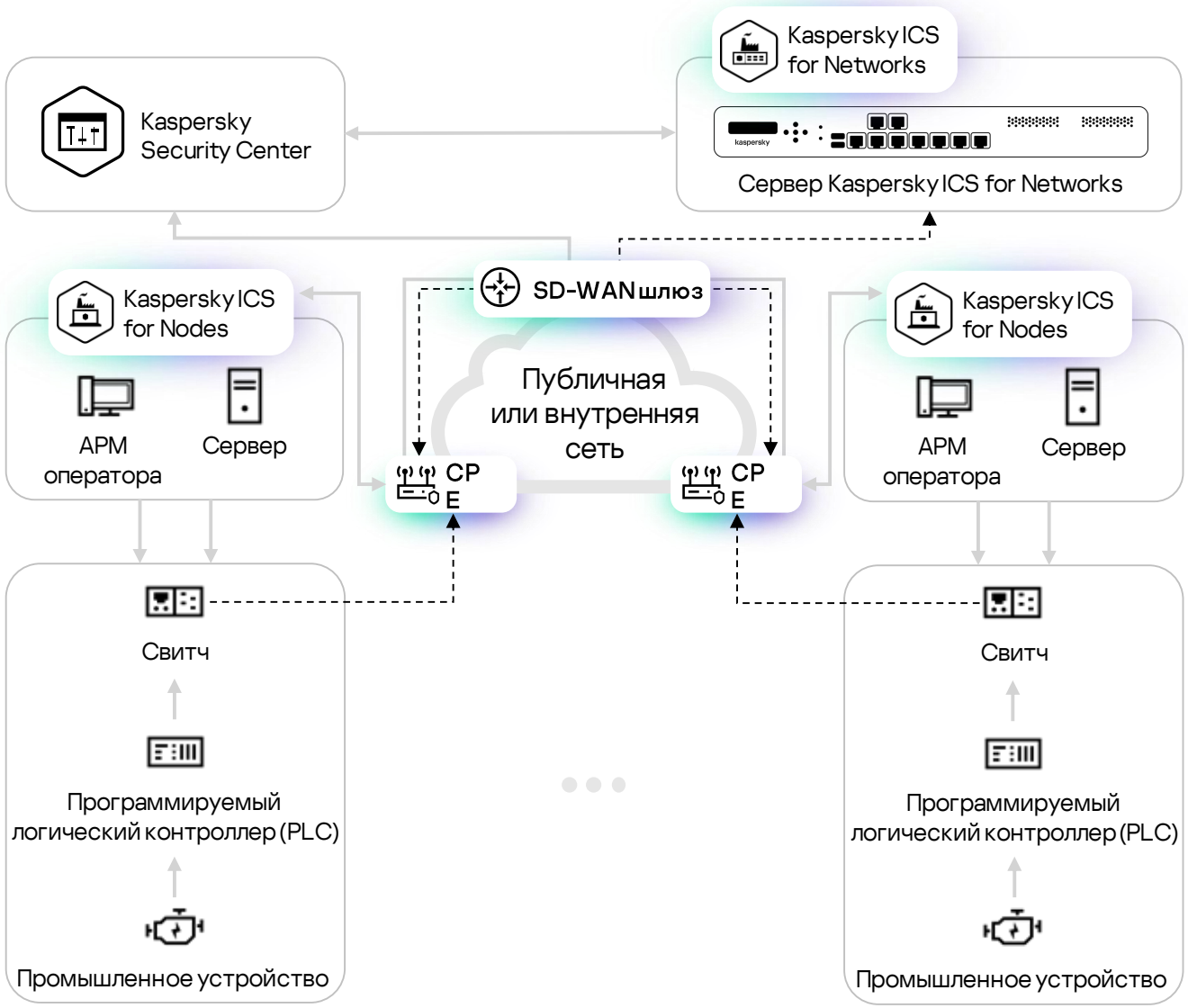
Единое решение для надежности промышленных сетей

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



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 Kaspersky ICS 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

Решения Kaspersky SD-WAN и Kaspersky ICS 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

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

Пример решения задач промышленных компаний с помощью Kaspersky SD-WAN

Сеть заправок

Задачи/проблемы

Требуется возможность быстро подключать новые заправочные станции, в том числе находящиеся на удалении от населенных пунктов

Необходима бесперебойная связь с сетью аппаратов для оплаты топлива и товаров из магазина

Требуется организовать разделение основного трафика и трафика гостевой сети Wi-Fi для посетителей заправок

Решение

Решение позволяет использовать любые доступные каналы связи и их комбинации, а технология Zero-Touch Provisioning обеспечивает быстрое подключение точек

При сбое CPE можно перезапустить удаленно из консоли или заменить силами работников заправки при наличии подменного фонда

Интеграция с Kaspersky ICS for Networks позволяет передавать копию трафика промышленной сети, чтобы организовать систему централизованного мониторинга и защиты

Ряд умных механизмов гарантирует бесперебойную связь даже в условиях нестабильных подключений

Механизмы решения помогают отделить трафик одного типа от другого и обеспечить безопасное разделение сети

Результат

Решение помогло подключить заправки на отдаленных от населенных пунктов шоссе и оптимизировать расходы на каналы связи на 21%

Заправочная сеть оснащена подменным фондом CPE, чтобы гарантировать работу приложений и терминалов оплаты даже в экстремальных ситуациях

Построена единая система мониторинга и защиты

Сеть сегментирована, внутренний трафик безопасно изолирован, трафик Wi-Fi сетей контролируется в том числе с помощью технологии DPI

Широкие возможности интеграции с продуктами и сервисами «Лаборатории Касперского»

Kaspersky Managed Detection and Response

Kaspersky Threat Intelligence

Интеграция с KUMA SIEM и передача телеметрии

Возможность реагирования на инциденты силами наших экспертов

Всегда актуальная информация о последних угрозах

Широкие возможности интеграции с продуктами и сервисами «Лаборатории Касперского»

Скоро

Возможность создания продвинутой XDR-платформы для реагирования на киберинциденты

Единая консоль управления всеми решениями

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 РЭП Минпромторга России

Kaspersky SD-WAN как часть экосистемы промышленной безопасности

Спасибо!

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

Максим Каминский
BDM Kaspersky SD-WAN/SASE

kaspersky