Аутсорсинг ИБ.

Подход оператора связи

На базе управляемых сервисов
кибербезопасности Solar MSS

Ростелеком
Солар

Содержание

I. Различие подходов – традиционный и сервисный

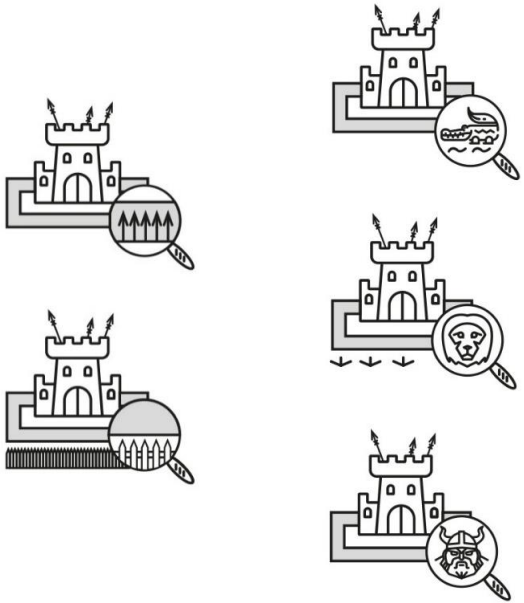
II. Сервисы Solar MSS

III. Сервис UTM – аутсорсинг межсетевых экранов

Подходы к защите. Наглядная иллюстрация

Традиционный подход

Каждый защищается сам как умеет

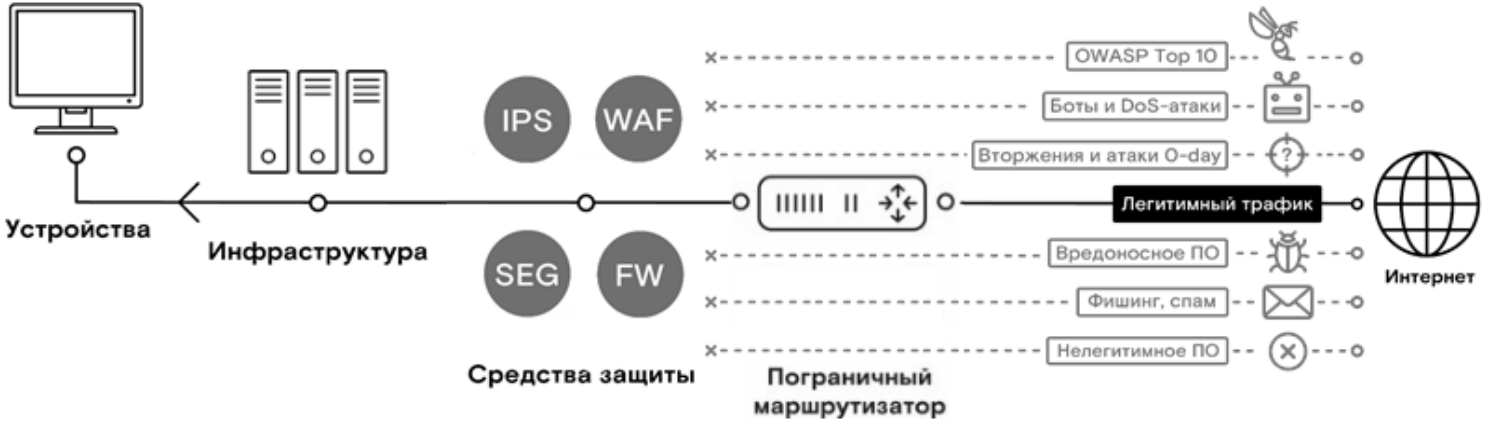


Сервисная модель

Нанимаем современные технологии

Ростелеком
Солар

Традиционный подход к ИБ. Своими силами

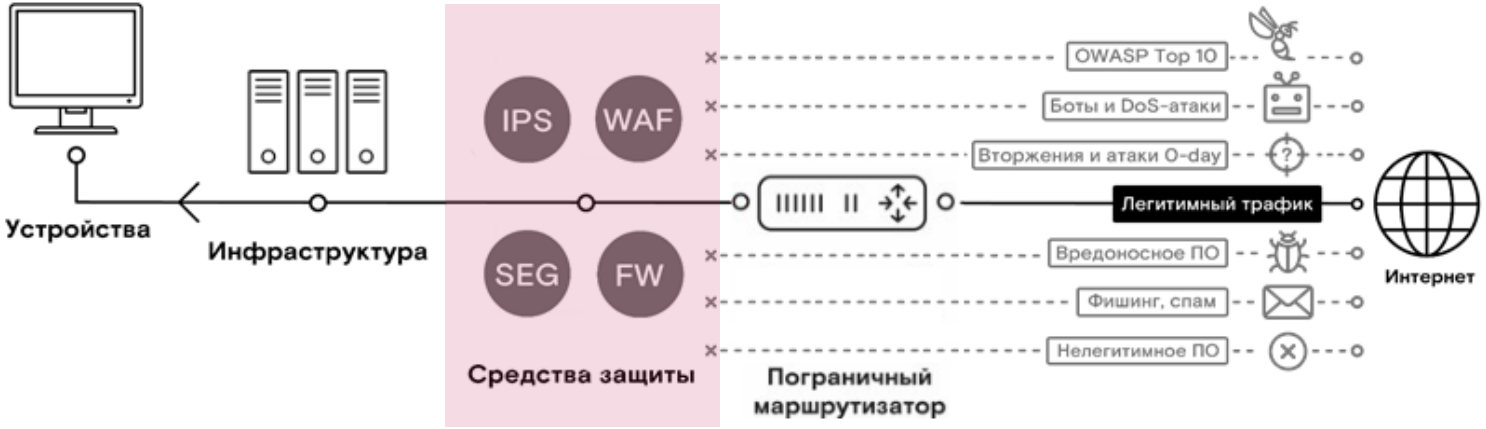


Сегмент ИС клиента | Сеть провайдера | Интернет

Ростелеком
Солар

Традиционный подход к ИБ. Привлечение партнера

Аутсорсинговый партнер:
Поставляет, внедряет, обслуживает,
управляет, заменяет

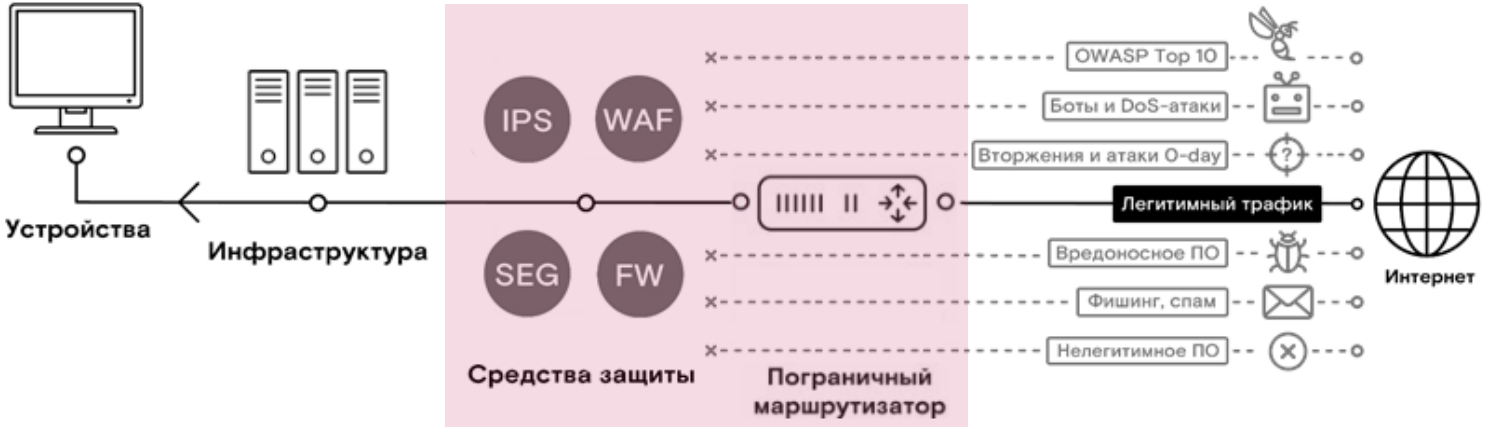


Сегмент ИС клиента	Сеть провайдера	Интернет

Ростелеком
Солар

Традиционный подход к ИБ. Привлечение партнера

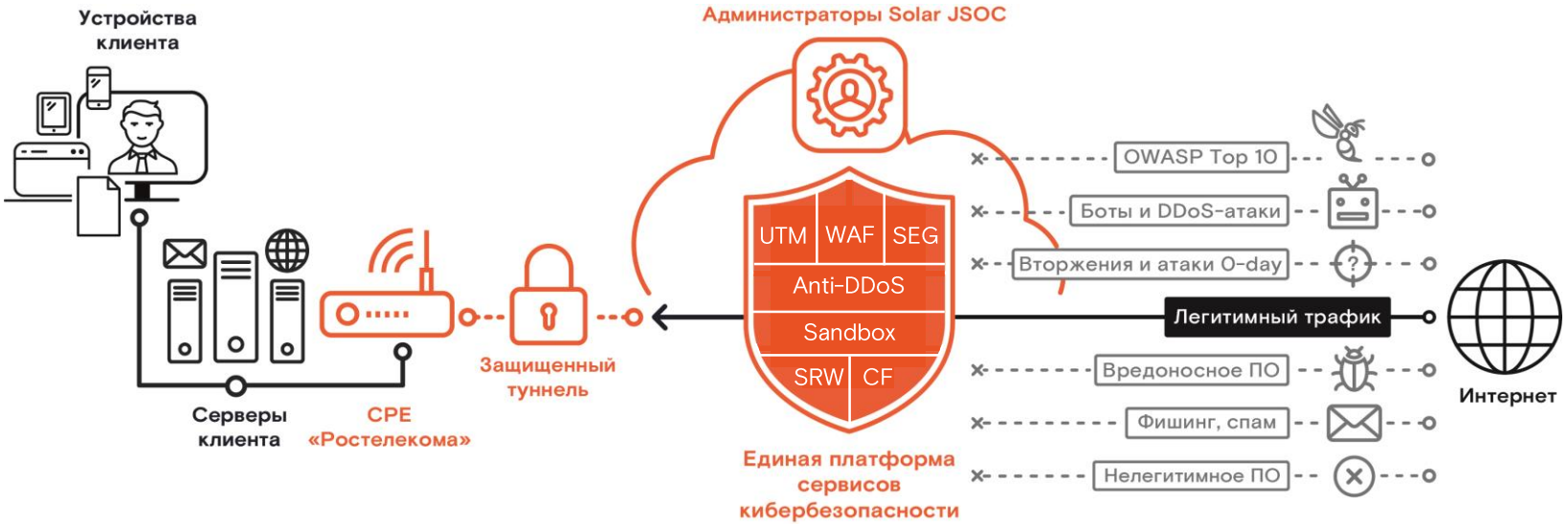
Аутсорсинговый партнер:
Поставляет, внедряет, обслуживает, управляет, заменяет.
Не только ИБ



Сегмент ИС клиента	Сеть провайдера	Интернет

Ростелеком
Солар

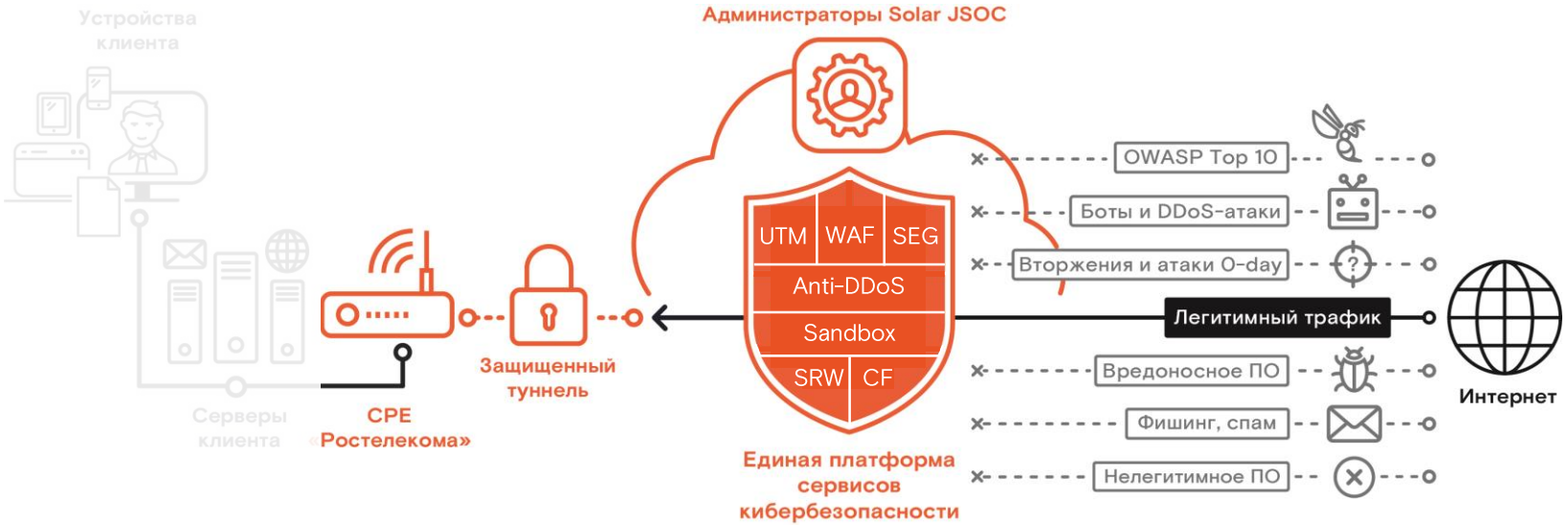
Сервисная модель от оператора связи



Сегмент ИС клиента	Облако «Ростелеком-Солар»	Интернет

Ростелеком
Солар

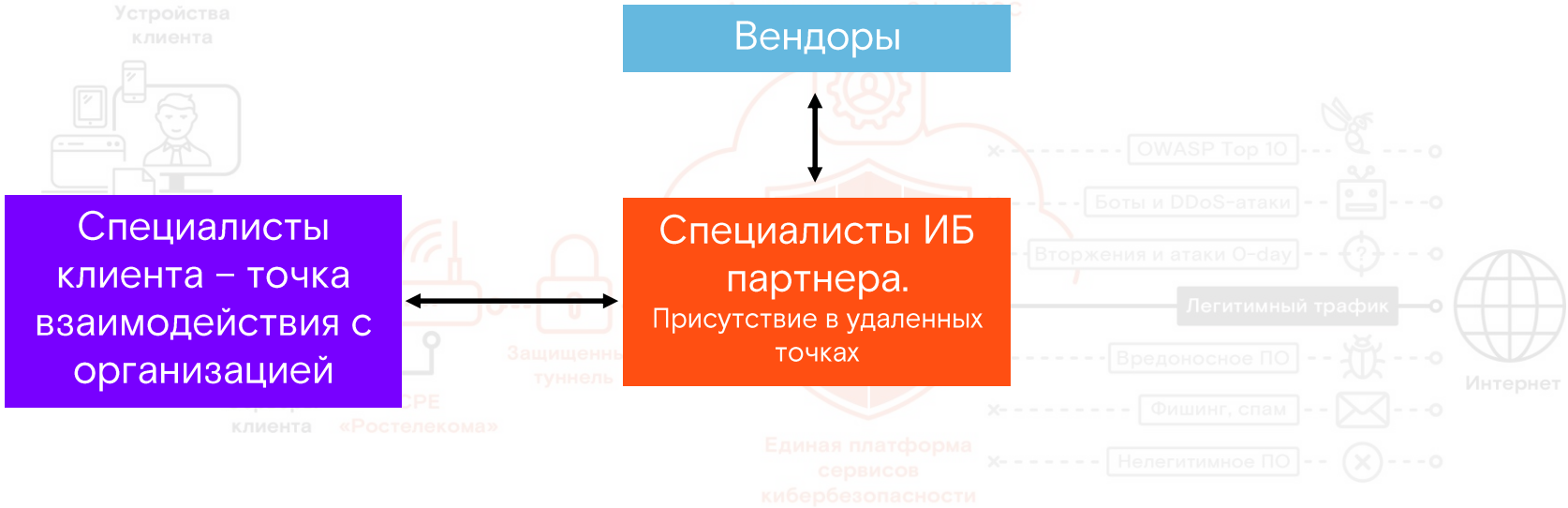
Сервисы – не просто поставить железки в ЦОДе и обслуживать



Сегмент ИС клиента	Облако «Ростелеком-Солар»	Интернет

Ростелеком
Солар

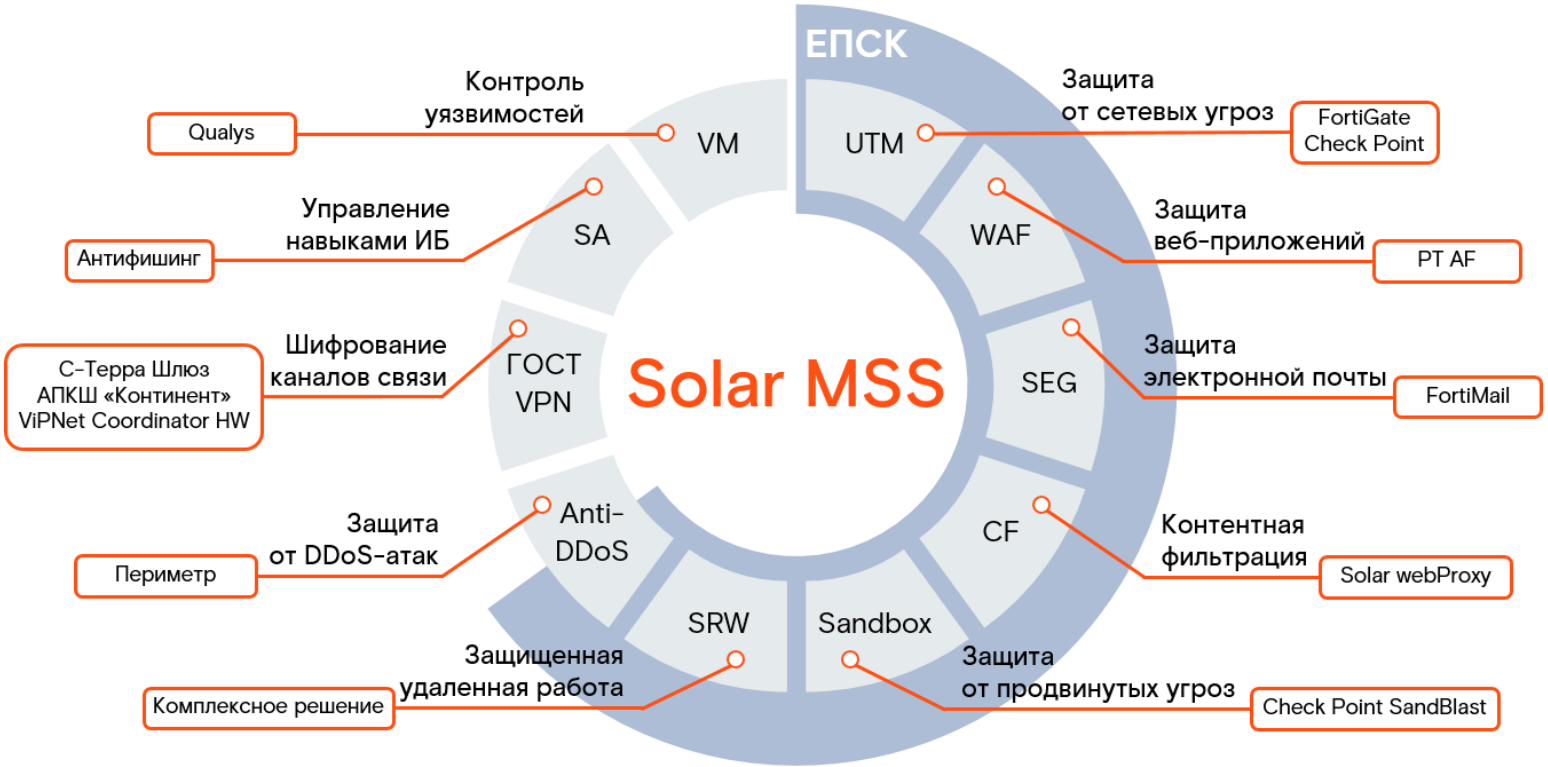
Традиционное взаимодействие между клиентом, партнером и вендором



Сегмент ИС клиента	Облако «Ростелеком-Солар»	Интернет

Ростелеком
Солар

Сервисы Solar MSS



Ростелеком
Солар

Solar MSS – управляемые сервисы кибербезопасности

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защищенная удаленная работа (SRW)
- Регистрация и анализ событий (ERA)
- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Контентная фильтрация (CF)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)

В основе сервисов – технологии ведущих компаний в области кибербезопасности:

POSITIVE TECHNOLOGIES NOKIA FORTINET Check Point SOFTWARE TECHNOLOGIES LTD. КОД БЕЗОПАСНОСТИ

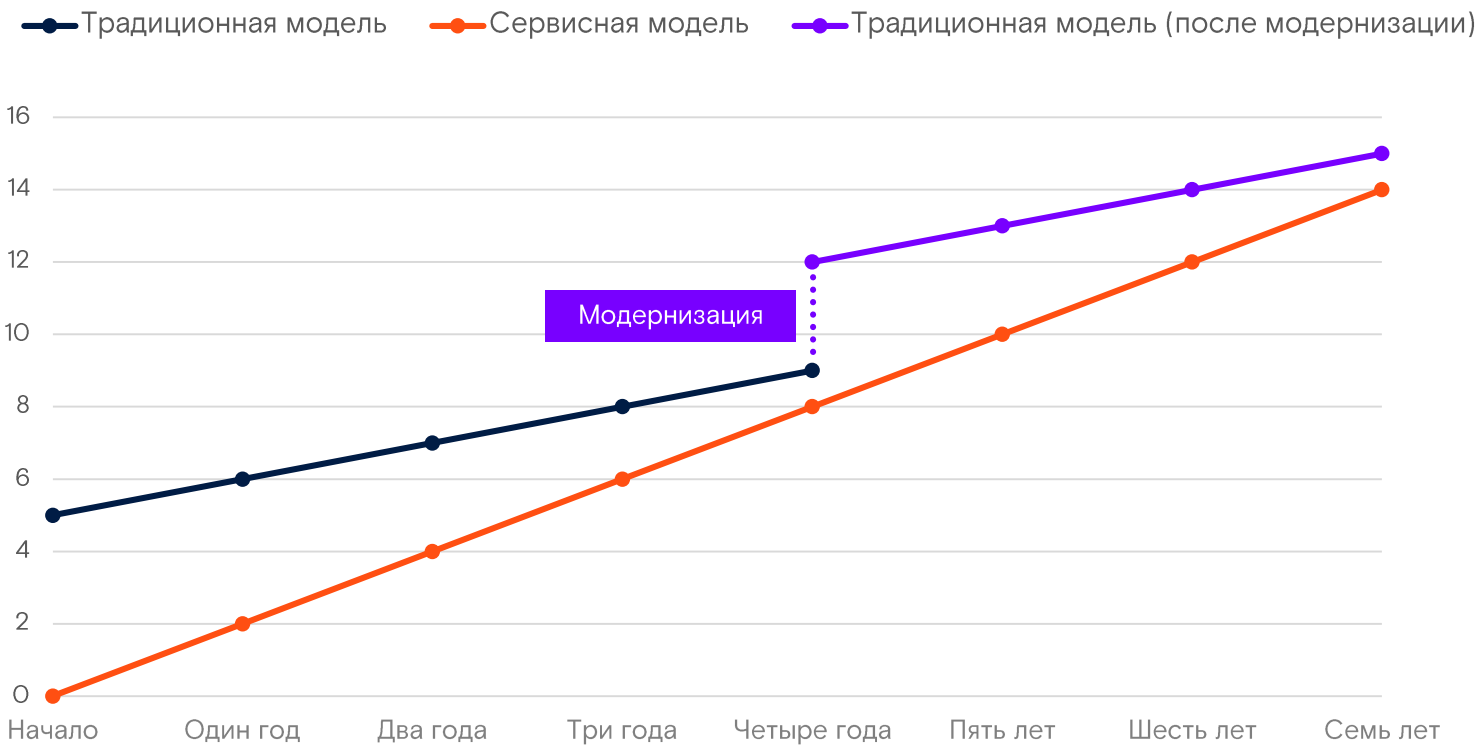
Qualys. infotecs Ростелеком Солар ГАРДА ТЕХНОЛОГИИ s•terra Антифишинг

Ростелеком Солар

TCO сервисной модели

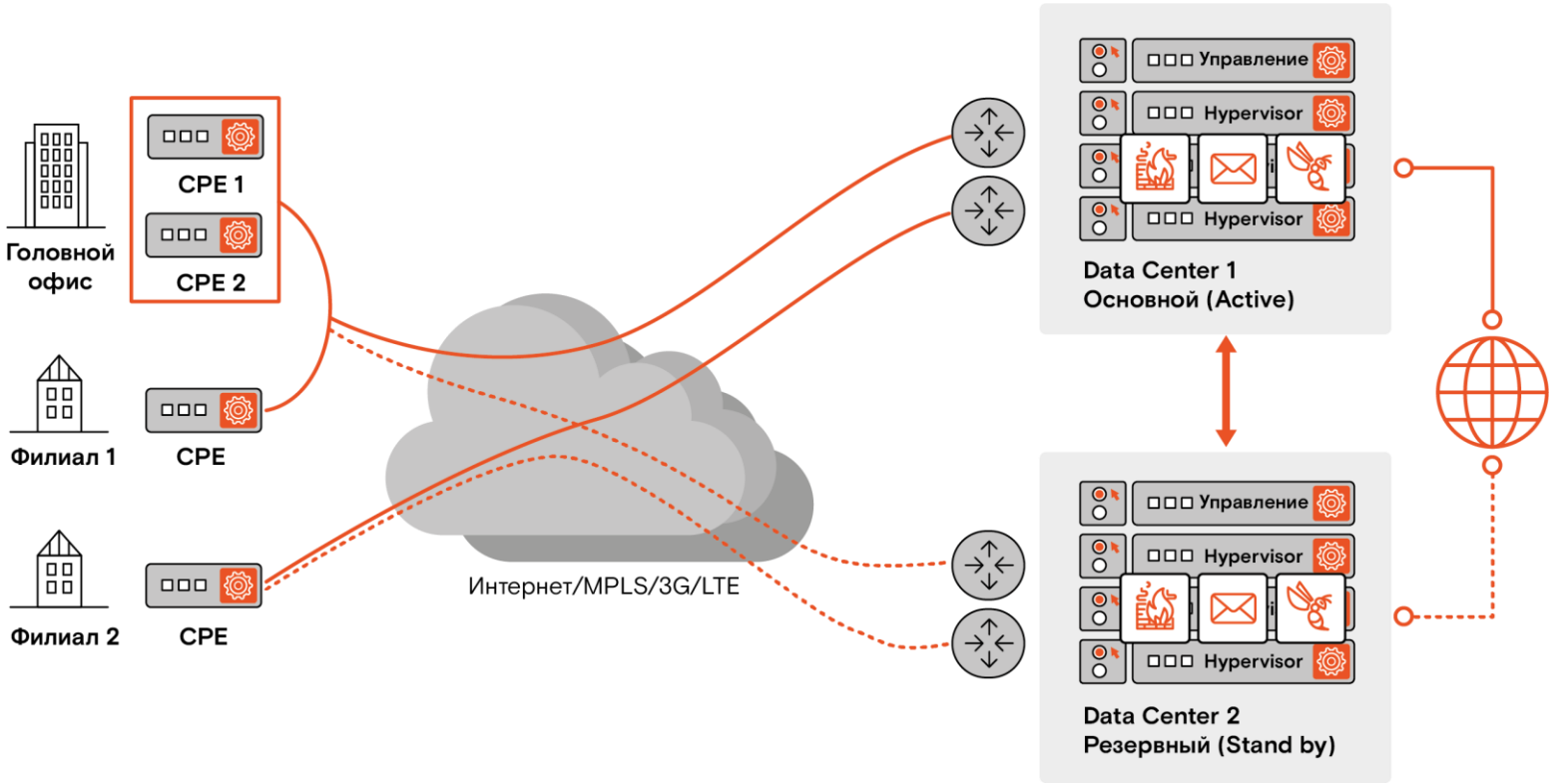
Ростелеком
Солар

TCO сервисной модели



Ростелеком
Солар

Высокоуровневая архитектура подключения

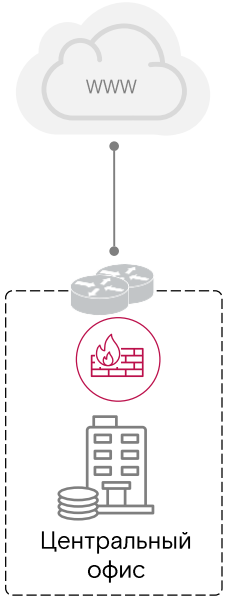


Ростелеком
Солар

Аутсорсинг межсетевых экранов

Ростелеком
Солар

Защита сети межсетевыми экранами

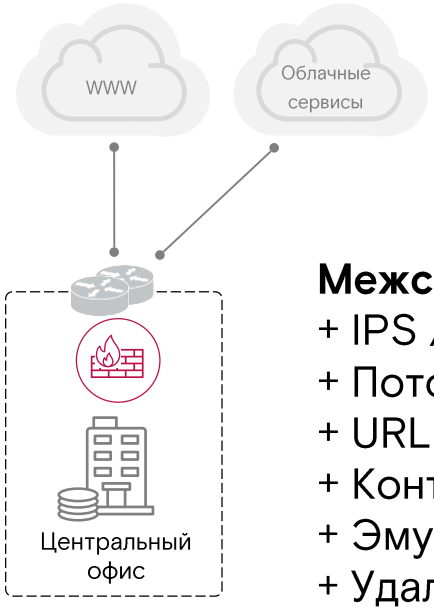


Межсетевой экран

Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами

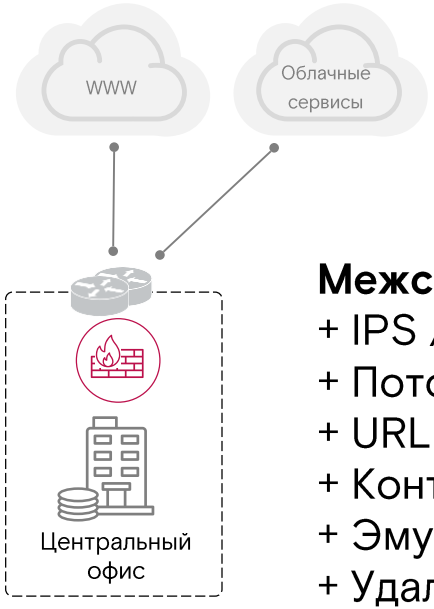


Межсетевой экран
+ IPS / IDS
+ Потоковый антивирус
+ URL фильтрация
+ Контроль приложений
+ Эмуляция файлов
+ Удаленные сотрудники

Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами



Межсетевой экран
+ IPS / IDS
+ Потоковый антивирус
+ URL фильтрация
+ Контроль приложений
+ Эмуляция файлов
+ Удаленные сотрудники

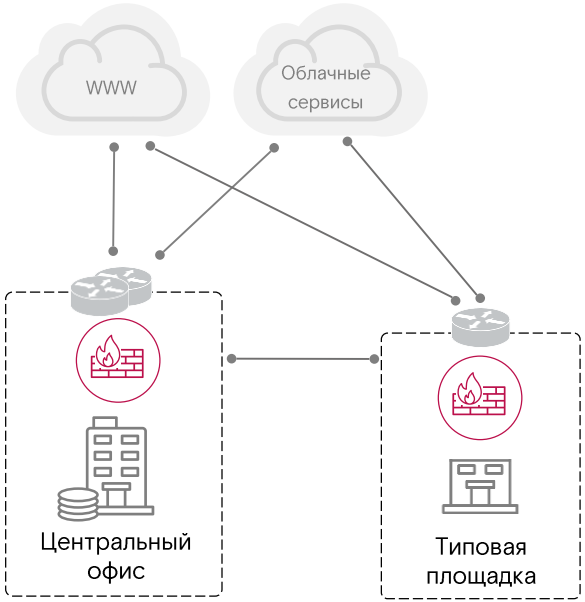
↑$

1. Требует обслуживания
2. Продление подписки
3. Техподдержка вендора

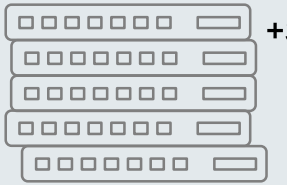
Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами



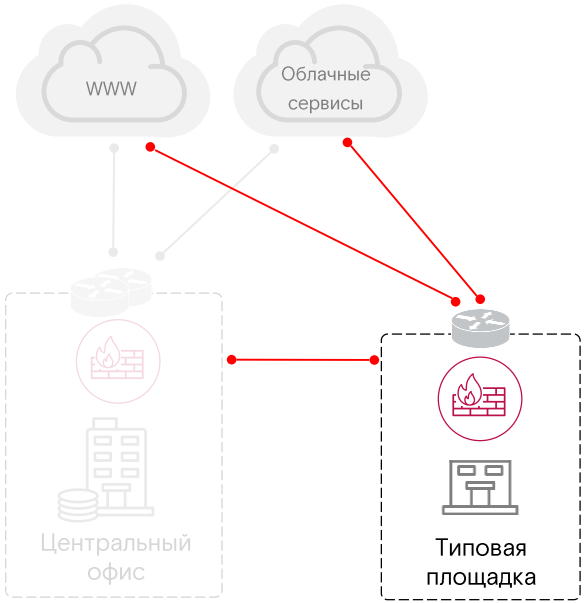
Дополнительный филиал или офис продаж



Обслуживаемое оборудование

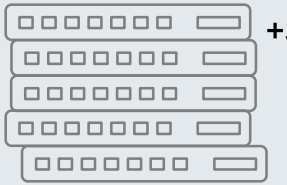
Ростелеком
Солар

Защита сети межсетевыми экранами



Дополнительный филиал или офис продаж

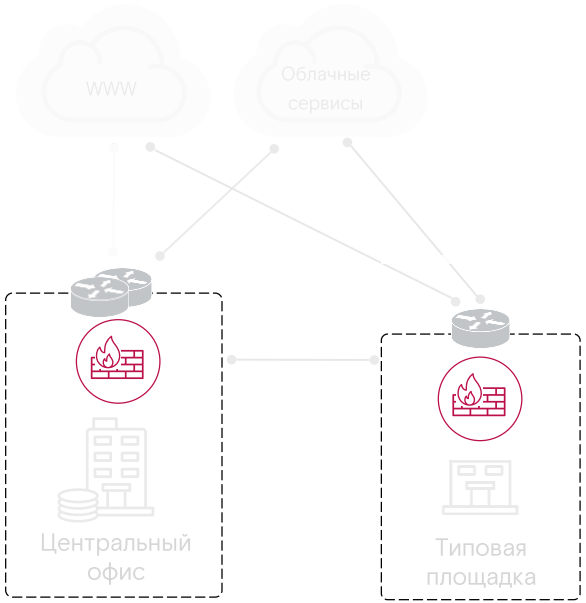
— требуется контроль всех подключений



Обслуживаемое оборудование

Ростелеком
Солар

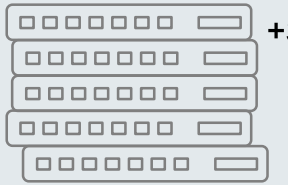
Защита сети межсетевыми экранами



Дополнительный филиал или офис продаж

— требуется контроль всех подключений

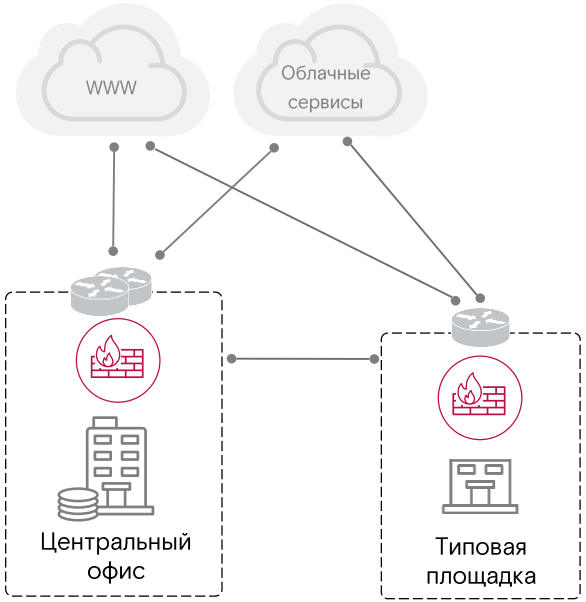
— обслуживание и поддержка оборудования на каждой площадке



Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами

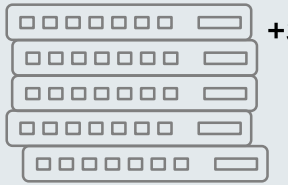


Дополнительный филиал или офис продаж

— требуется контроль всех подключений

— обслуживание и поддержка оборудования на каждой площадке

— поддержка только в рабочее время 8x5

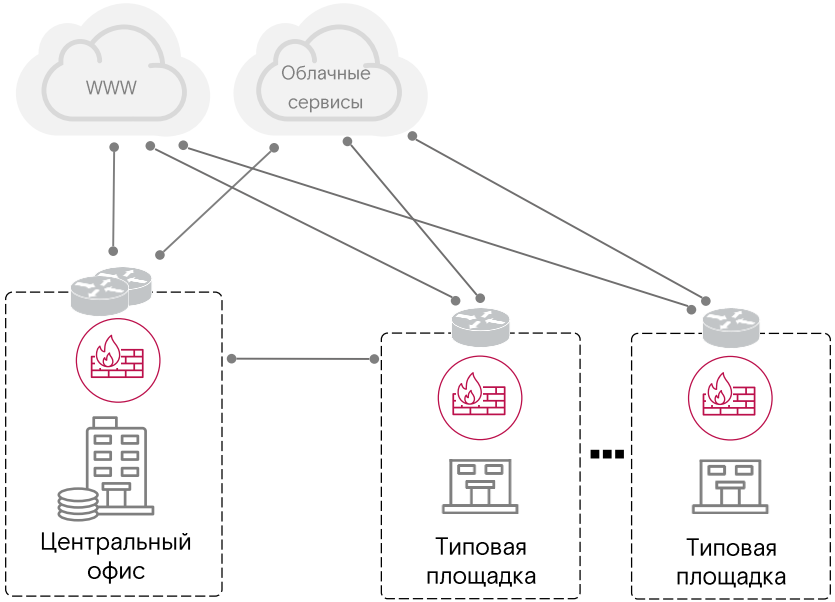


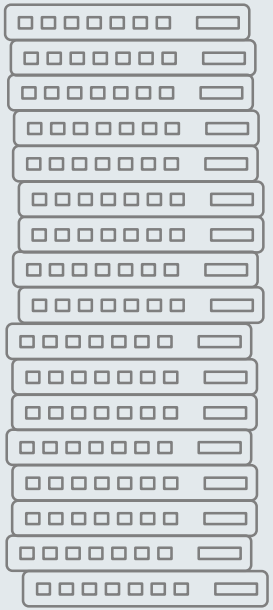
Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами

Масштабирование

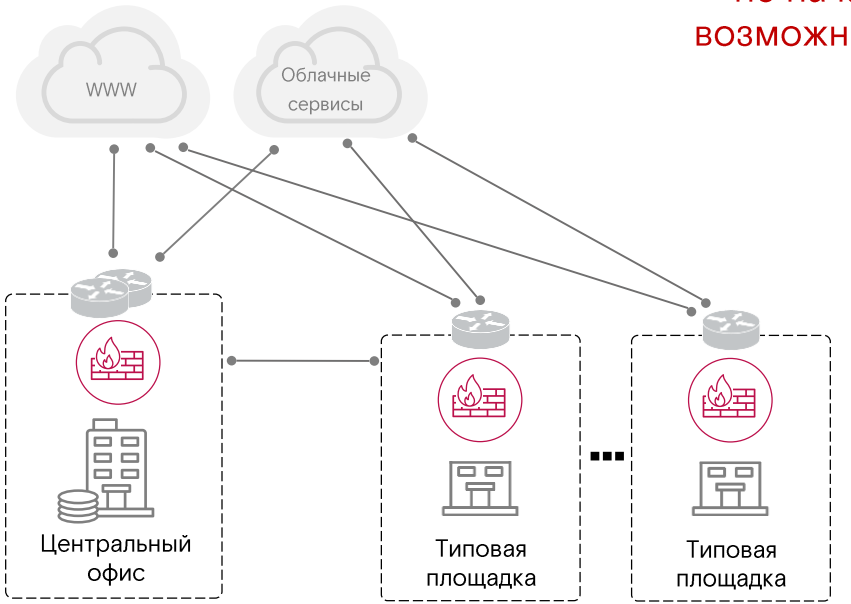




Обслуживаемое оборудование

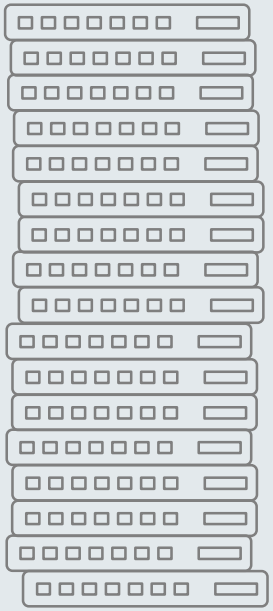
Ростелеком
Солар

Защита сети межсетевыми экранами



Масштабирование

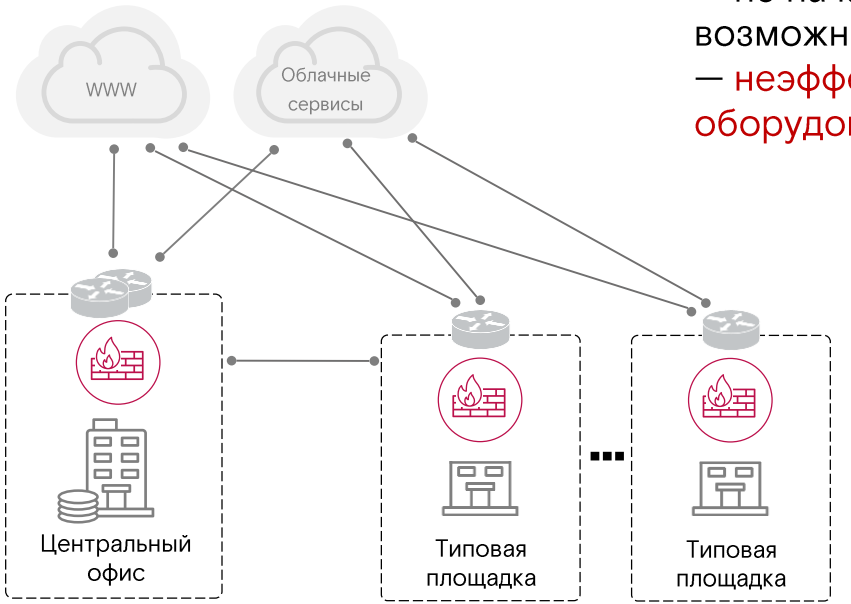
— не на каждой площадке есть возможность выделенного канала связи



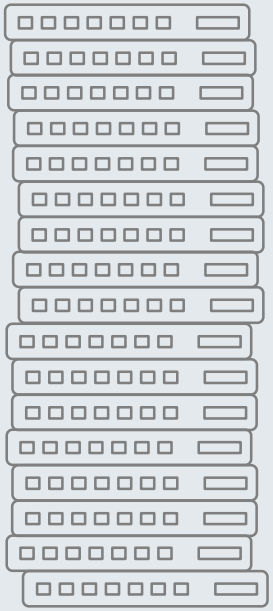
Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами



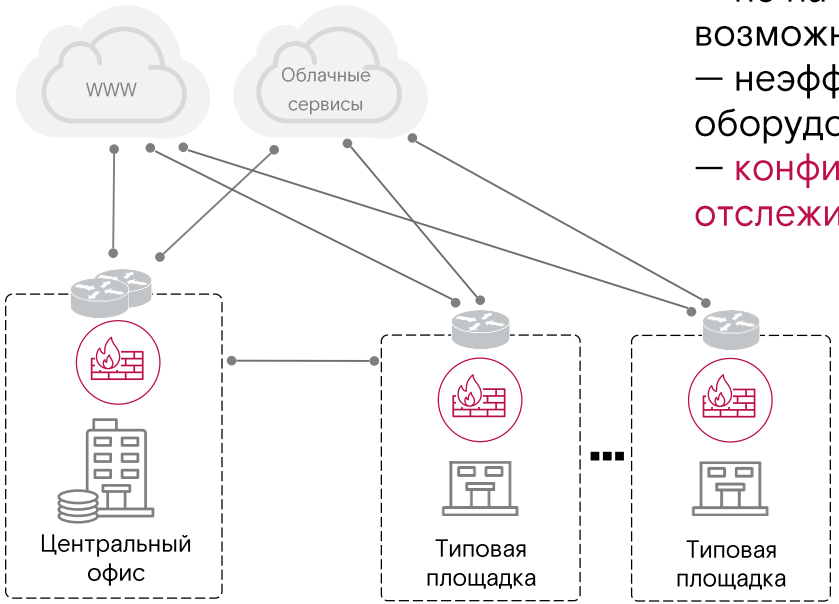
Масштабирование
— не на каждой площадке есть возможность выделенного канала связи
— неэффективное использования оборудования



Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами

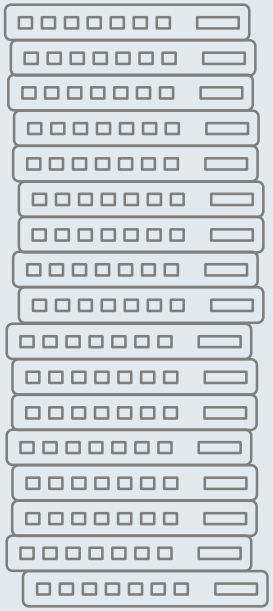


Масштабирование

— не на каждой площадке есть возможность выделенного канала связи

— неэффективное использования оборудования

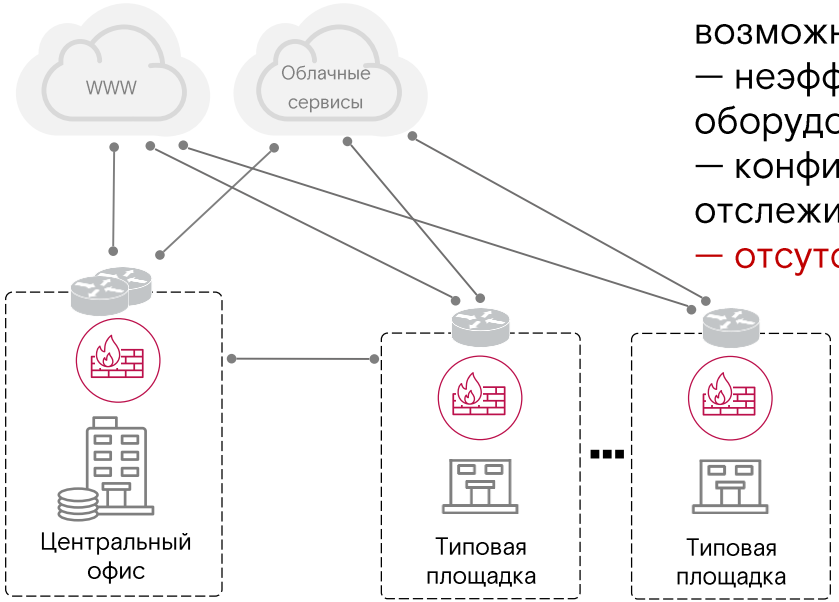
— конфигурации требует времени и отслеживания



Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами



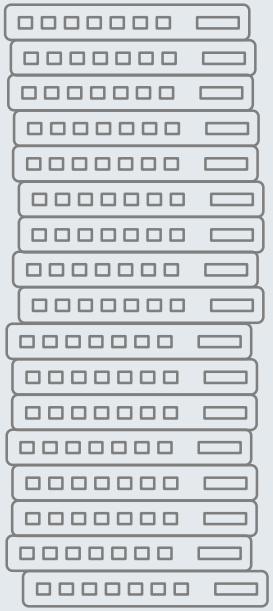
Масштабирование

— не на каждой площадке есть возможность выделенного канала связи

— неэффективное использования оборудования

— конфигурации требует времени и отслеживания

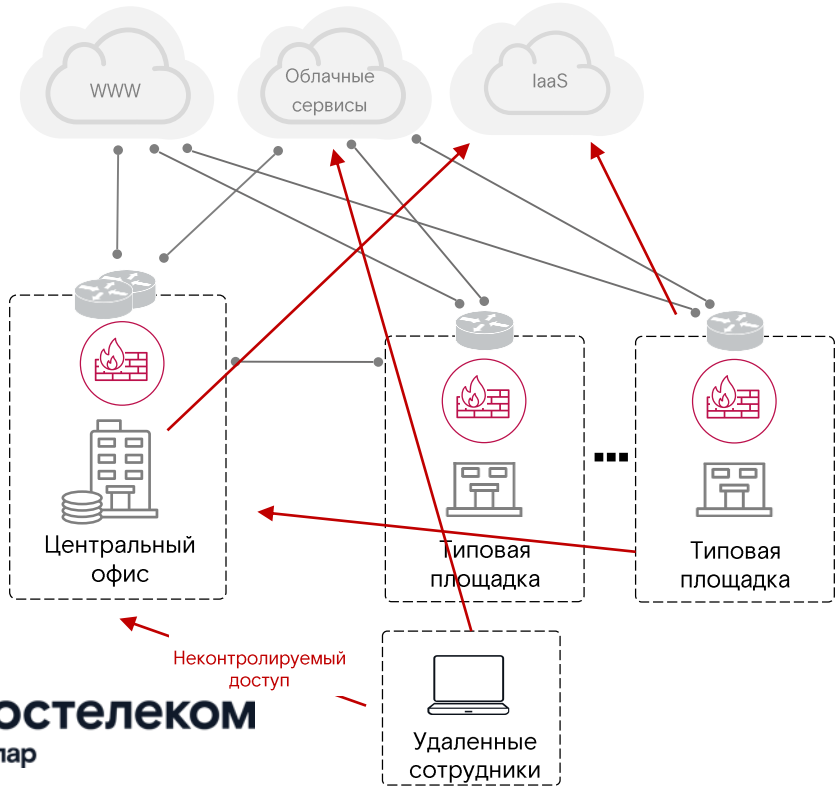
— отсутствие специалистов на местах

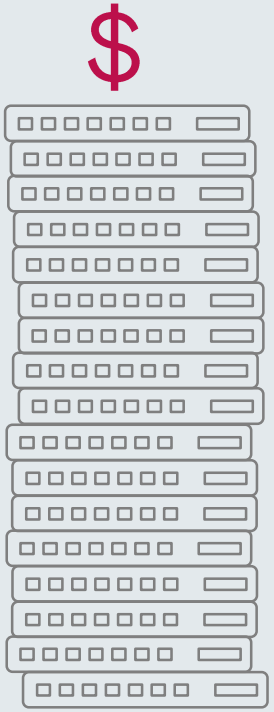


Обслуживаемое оборудование

Ростелеком
Солар

Защита сети межсетевыми экранами



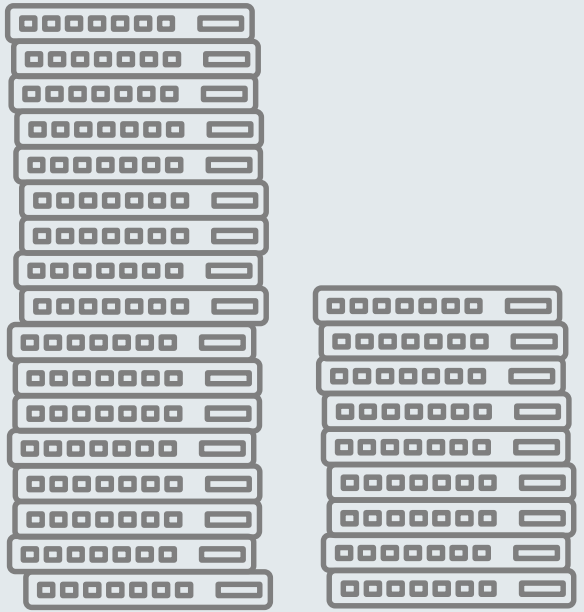


Обслуживаемое оборудование

Ростелеком Солар

Аутсорсинг ИБ и часть ИТ

Жизненный цикл «железного» решения



Обслуживание, хранение, замена, поддержка, склад, учет, устаревание...

Ростелеком
Солар

Сетевой периметр – цель киберпреступников

+40%

выросло количество атак, направленных на получение контроля над инфраструктурой

58%

доля внешних кибератак, т.е. атаки «снаружи»

+11%

рост атак с использованием вирусного ПО

40%

Уязвимых серверов, принадлежат крупным коммерческим и государственным компаниям

Данные: Solar JSOC, 2019

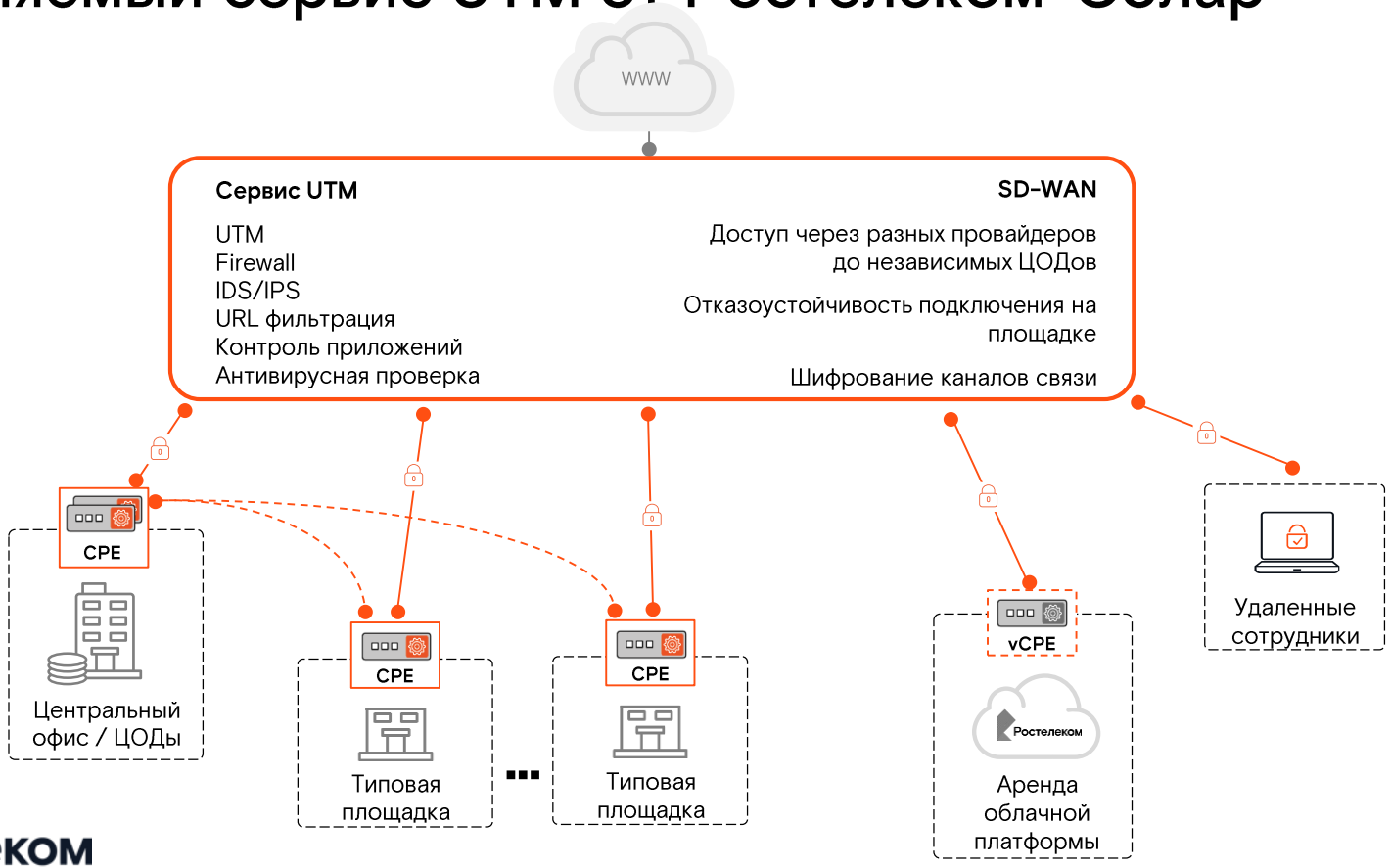
Рост bruteforce-атак на RDP – один из основных каналов входа в периметр организации с марта 2020

Ростелеком
Солар

Сервисный подход к межсетевым экранам

Ростелеком
Солар

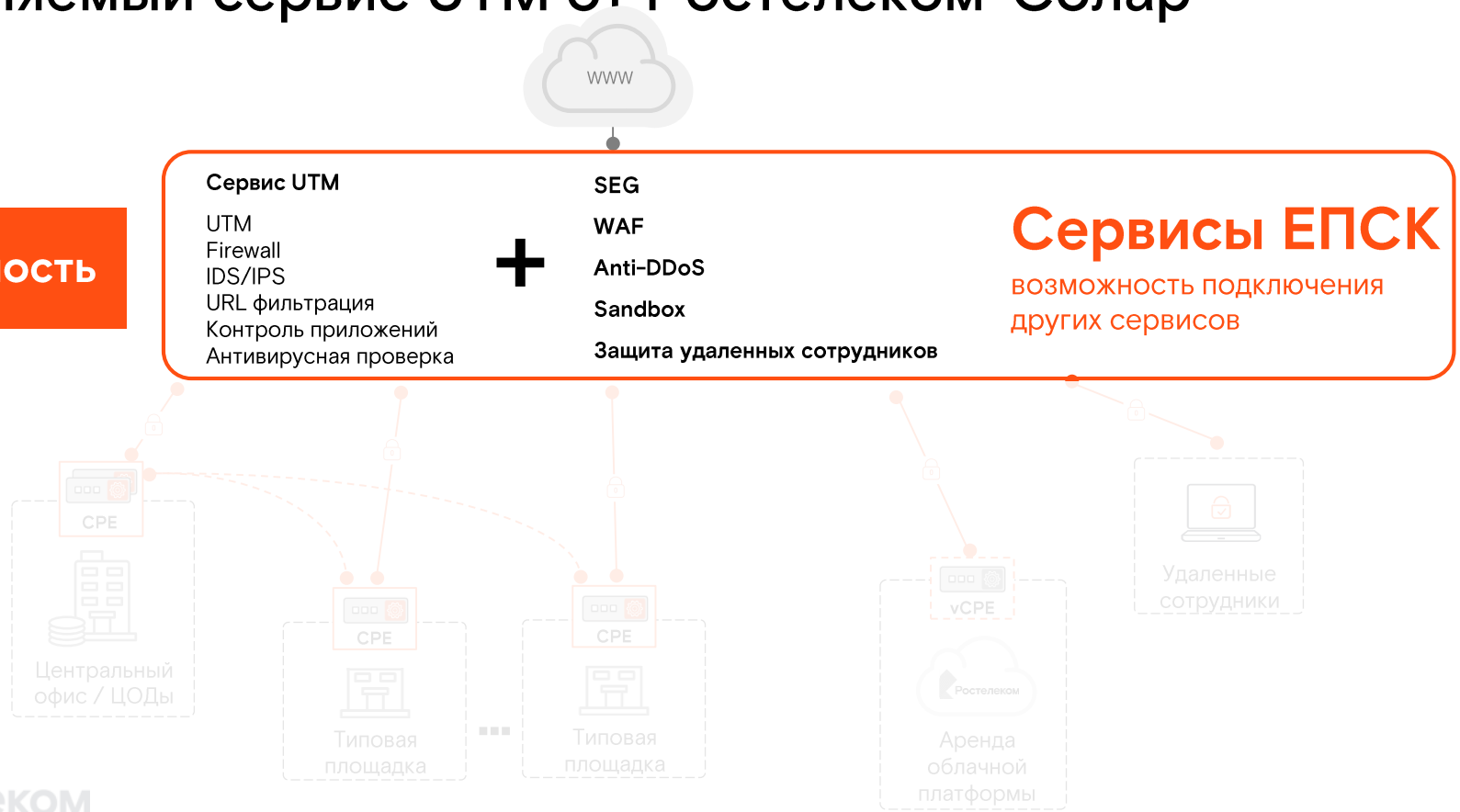
Управляемый сервис UTM от Ростелеком-Солар



Ростелеком
Солар

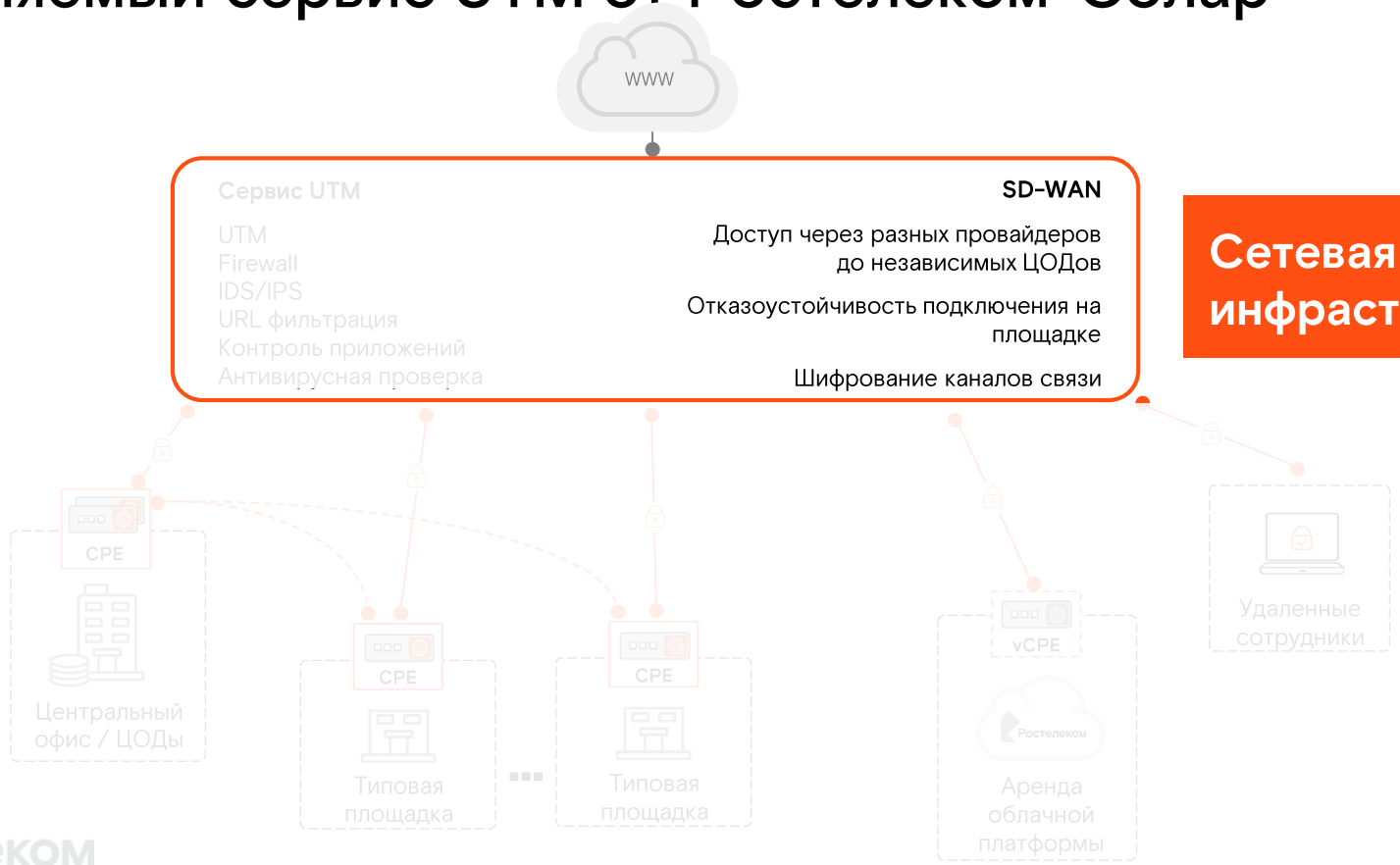
Управляемый сервис UTM от Ростелеком-Солар

Безопасность



Ростелеком Солар

Управляемый сервис UTM от Ростелеком-Солар



Ростелеком
Солар

Управляемый сервис UTM от Ростелеком-Солар

FORTINET

Check Point SOFTWARE TECHNOLOGIES LTD.

UserGate

Сервис UTM

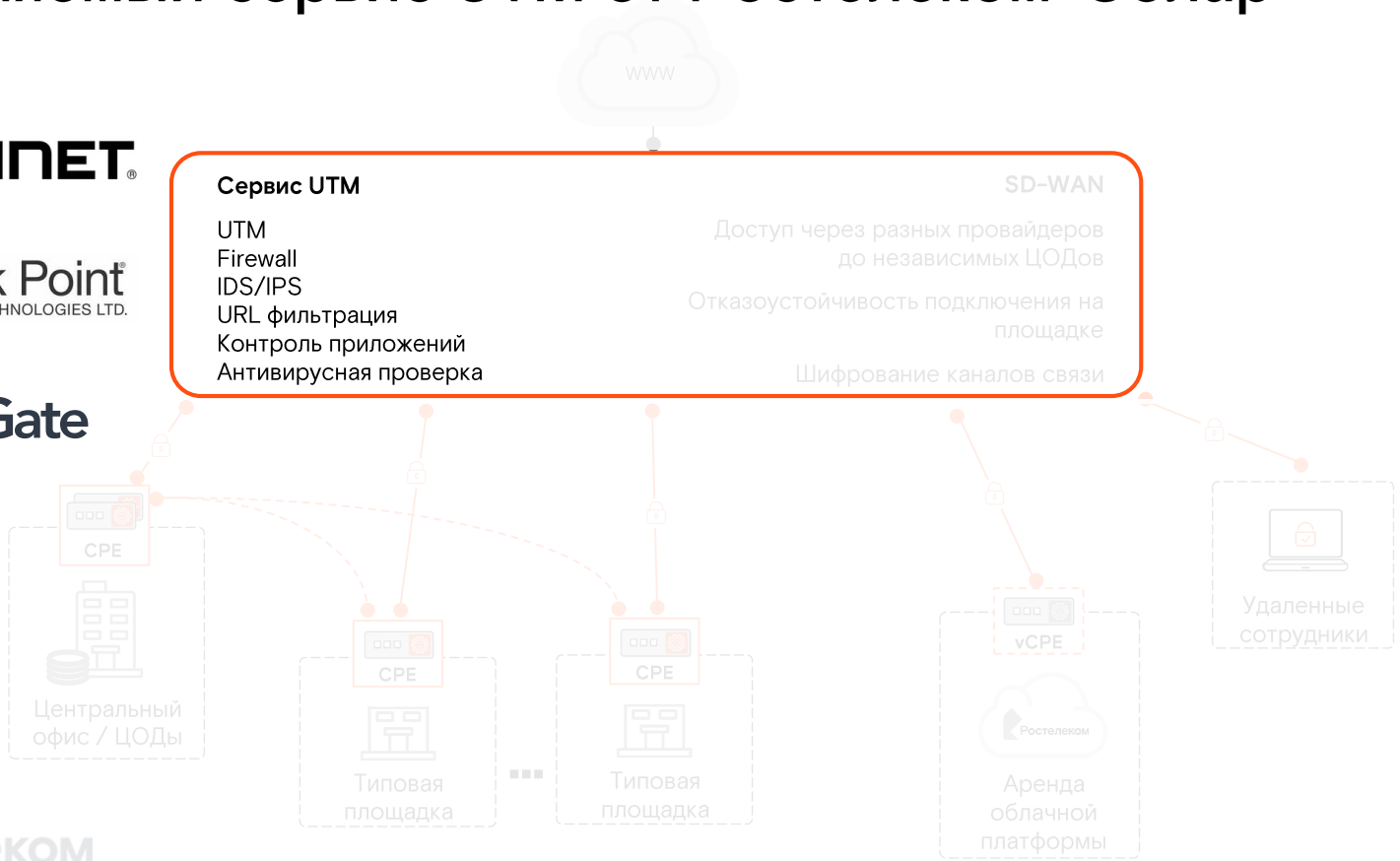
UTM
Firewall
IDS/IPS
URL фильтрация
Контроль приложений
Антивирусная проверка

SD-WAN

Доступ через разных провайдеров до независимых ЦОДов

Отказоустойчивость подключения на площадке

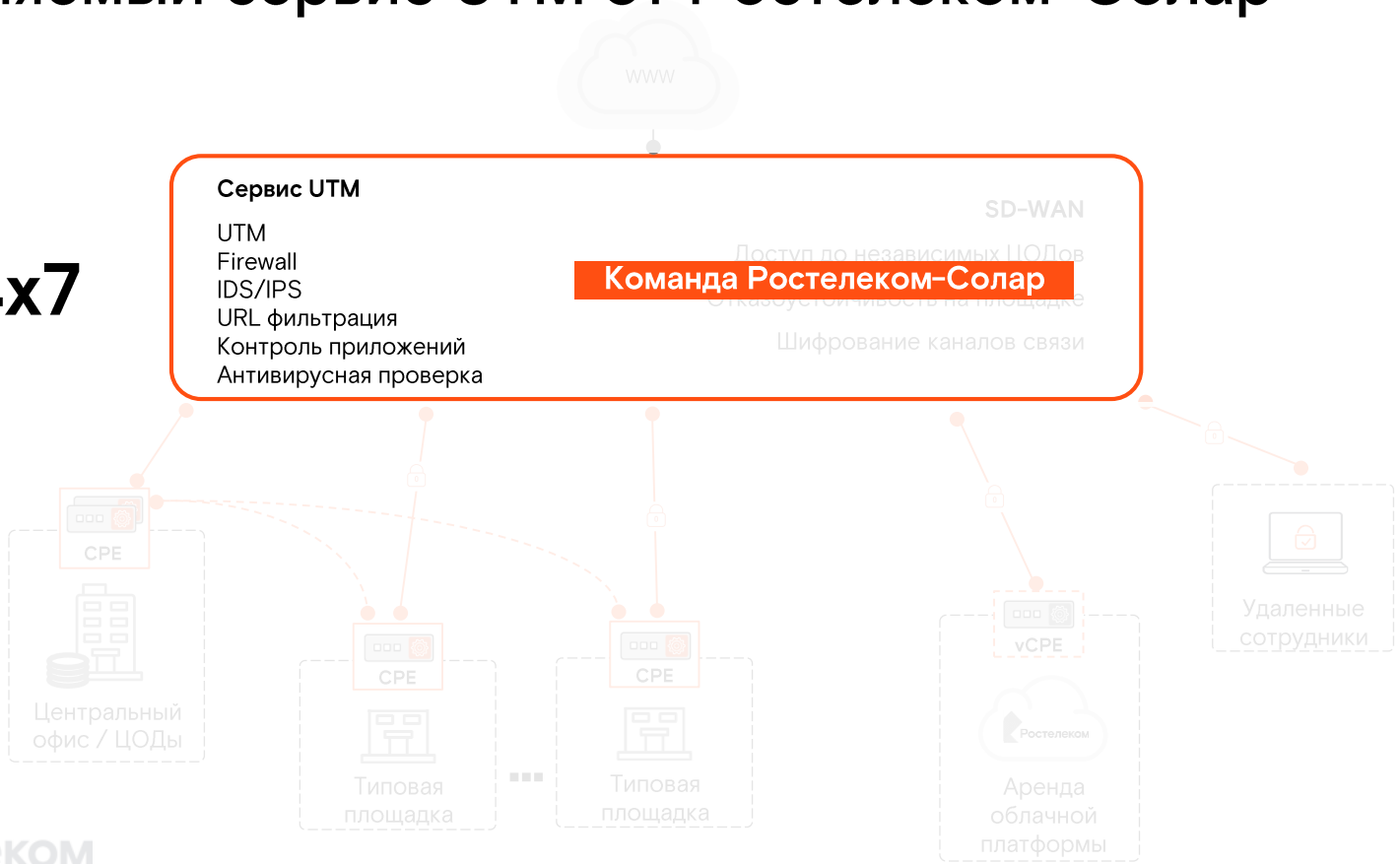
Шифрование каналов связи



Ростелеком Солар

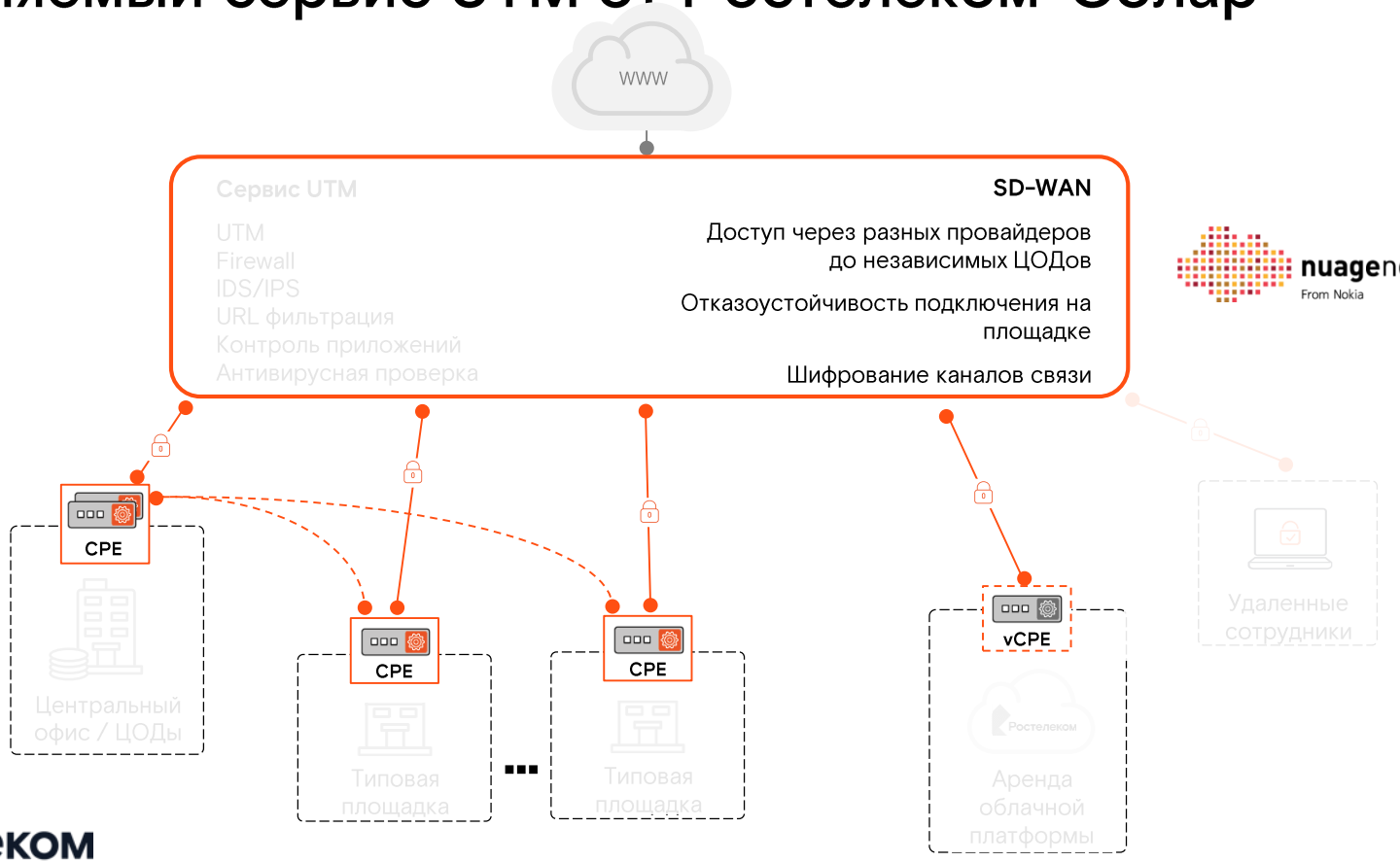
Управляемый сервис UTM от Ростелеком-Солар

24x7



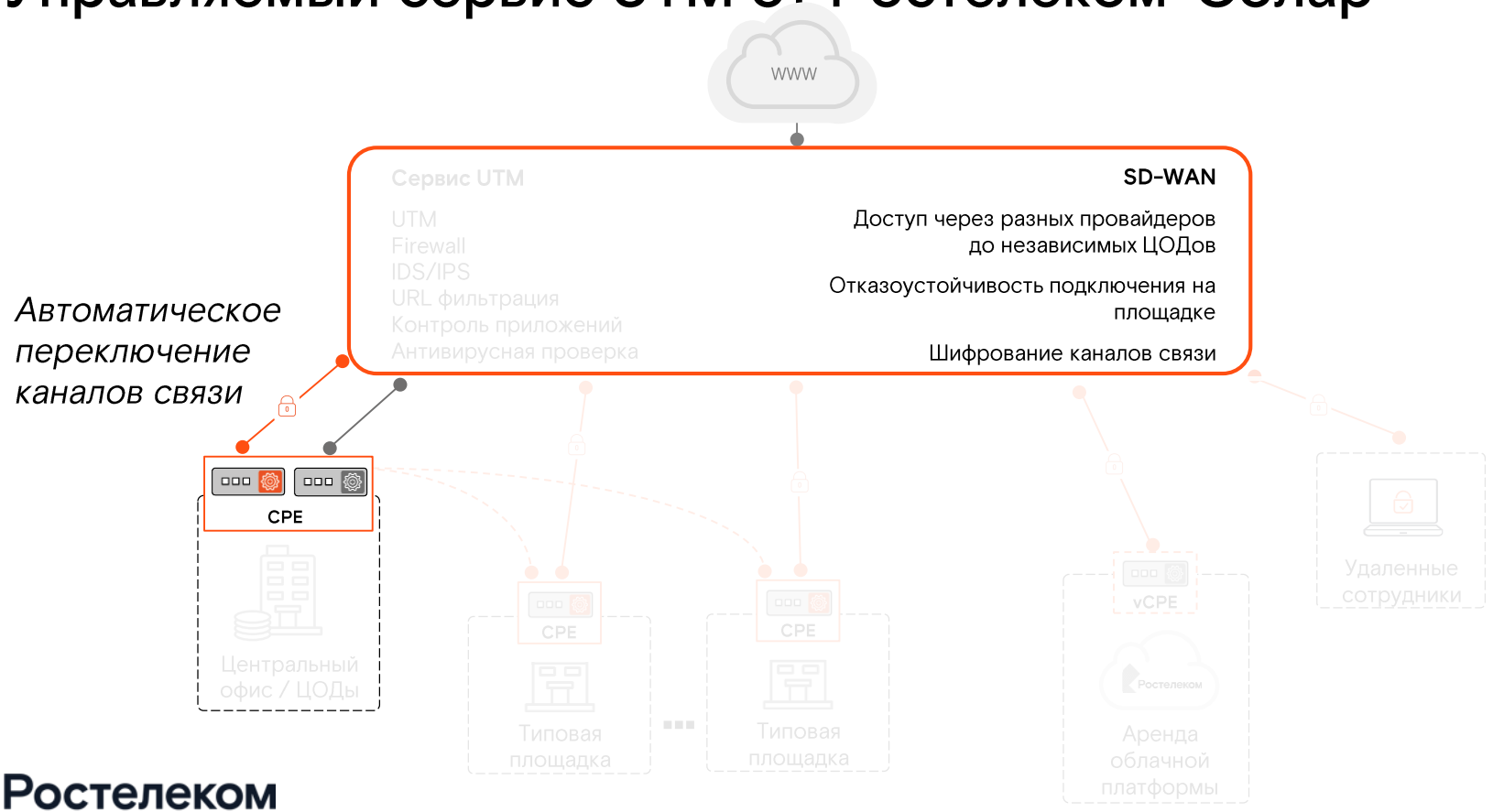
Ростелеком Солар

Управляемый сервис UTM от Ростелеком-Солар



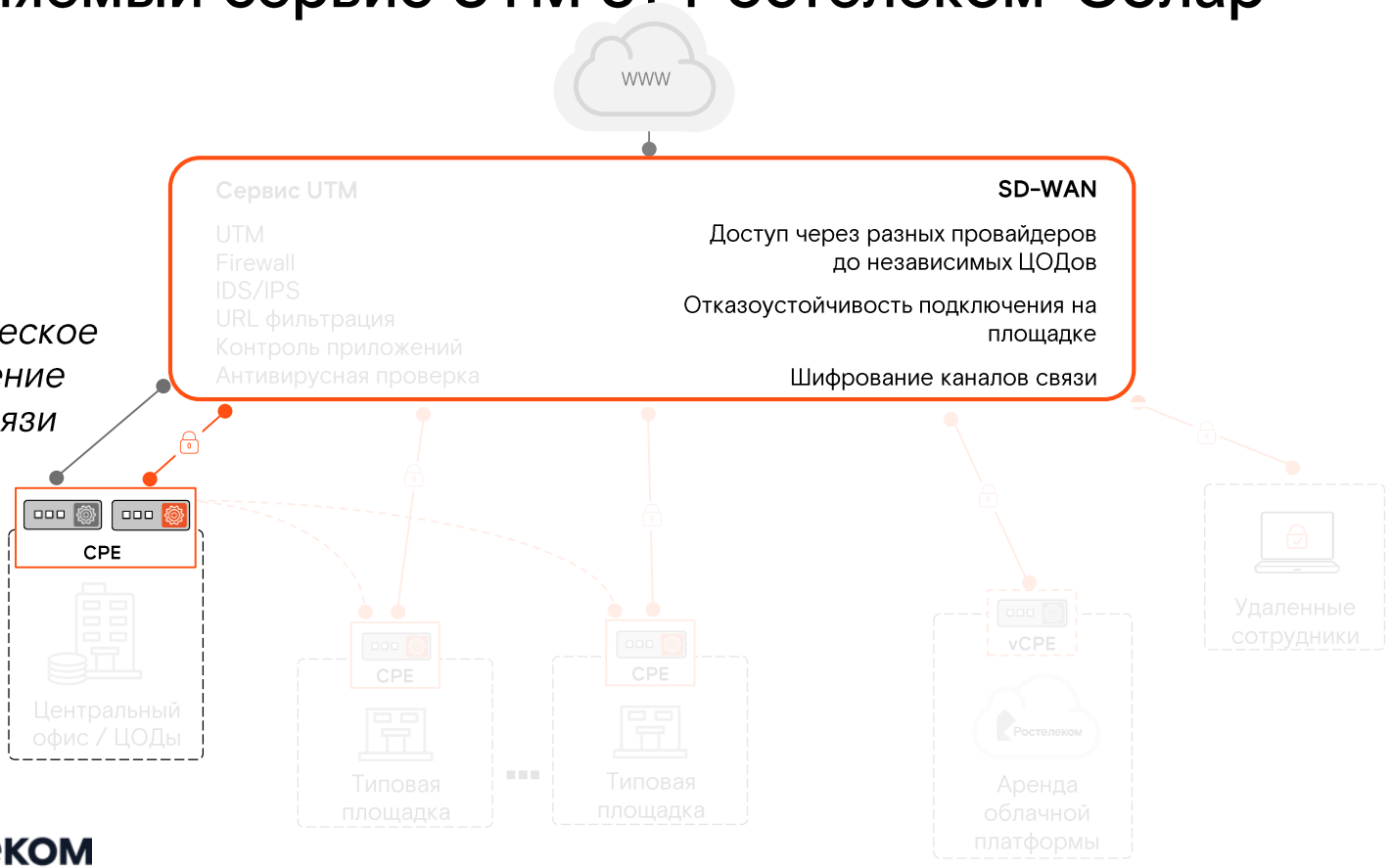
Ростелеком
Солар

Управляемый сервис UTM от Ростелеком-Солар



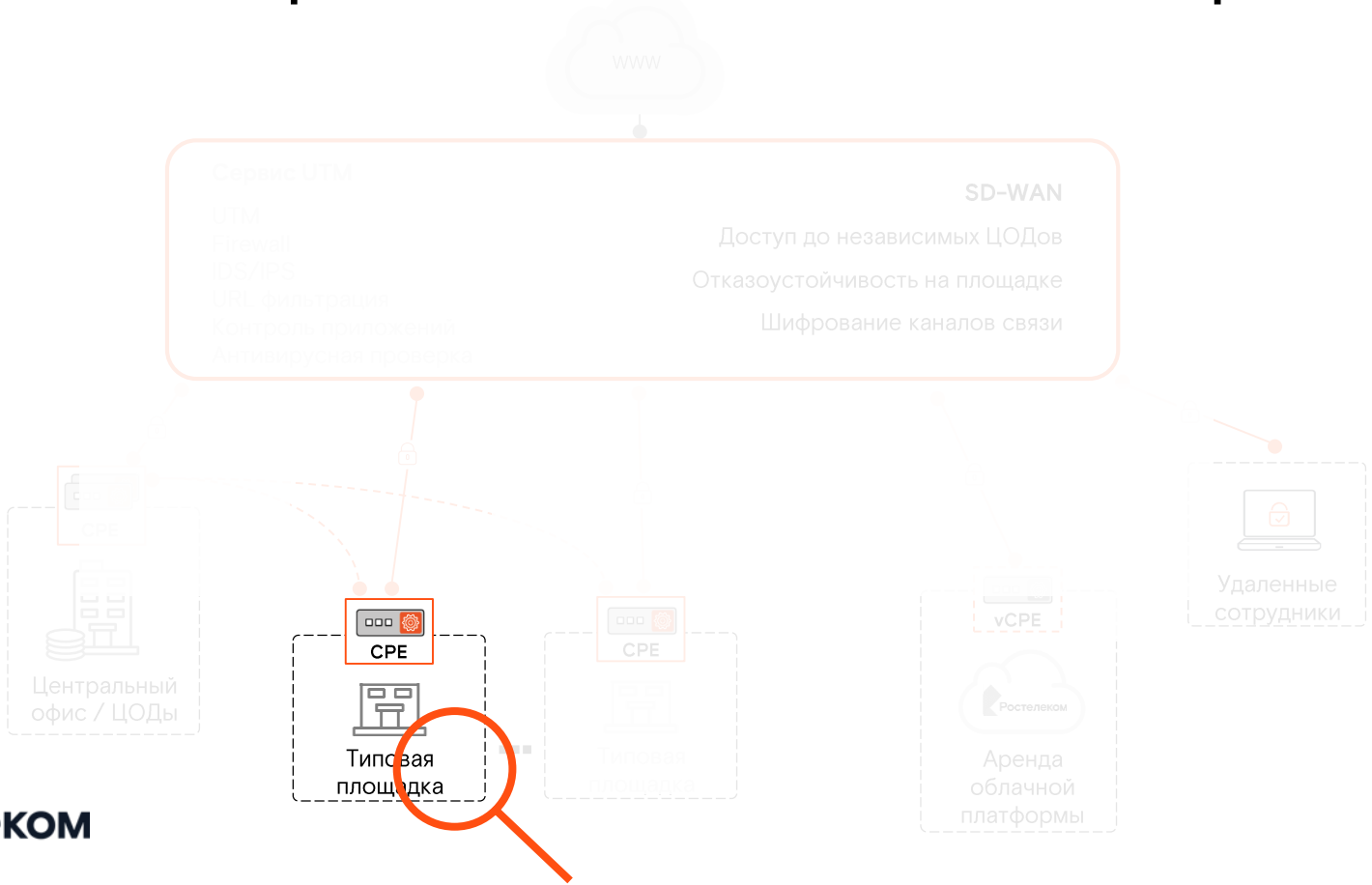
Ростелеком
Солар

Управляемый сервис UTM от Ростелеком-Солар



Ростелеком
Солар

Управляемый сервис UTM от Ростелеком-Солар



Ростелеком
Солар

Схема функционирования на отдельной площадке

Ростелеком
Солар

Схема функционирования на отдельной площадке

Схема функционирования на отдельной площадке

Customer Premises Equipment

- Подключение не требует сложных конфигураций
- Хранение запасного оборудование у Ростелекома
- Организация отказоустойчивого подключения

Варианты исполнения

до 70 Мбит/с

до 200 Мбит/с

от 1 000 Мбит/с

Ростелеком
Солар

Целесообразность сервиса UTM

Ростелеком
Солар

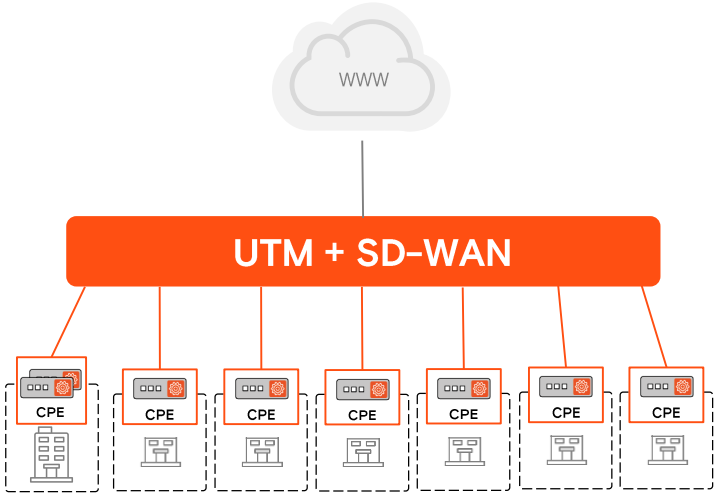
Кейс: UTM для учреждения здравоохранении

До

- 7 площадок, 200+ сотрудников
- Отсутствие ИБ и мало ИТ специалистов
- Нет контроля доступа к интернету в учреждениях

После

- Сервис оказывается **в круглосуточном режиме**
- Нет затрат на оборудование, новых специалистов, обучение
- **Начальные затраты на 95% ниже, чем в проектной модели**



Ростелеком
Солар

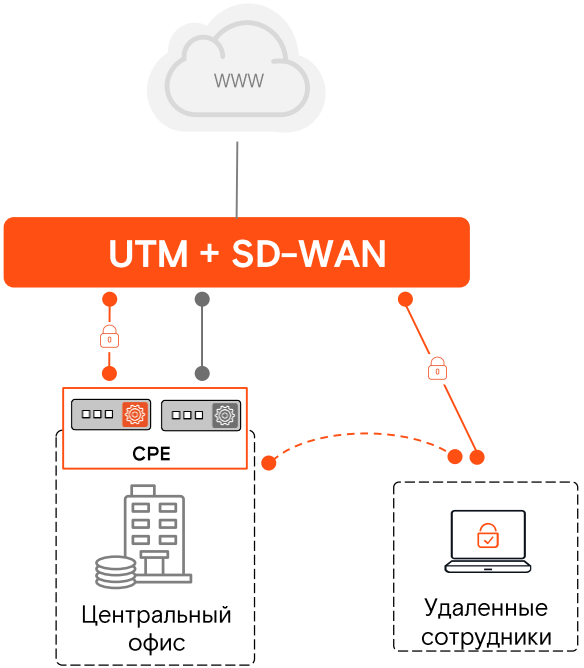
Кейс: UTM для нефтегазовой компании

До

- Размер: 1000+ сотрудников
- Хотели обновить межсетевой экран
- Нет ИБ специалистов

После

- Сервис оказывается в круглосуточном режиме
- Скорость фильтрации трафика – 500 Мбит/с
- **Отказоустойчивость** подключения к интернету
- После пилотного внедрения

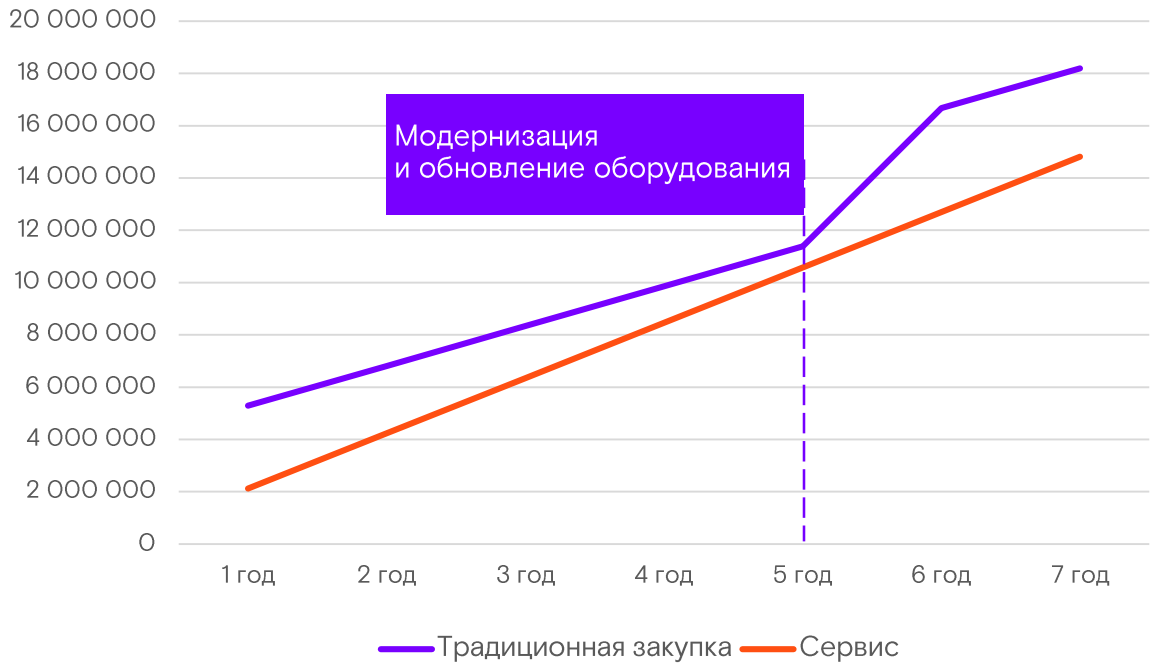


Ростелеком
Солар

Сравнение стоимости владения. Вариант 1

Количество офисов:

1 главный офис
+
20 филиалов



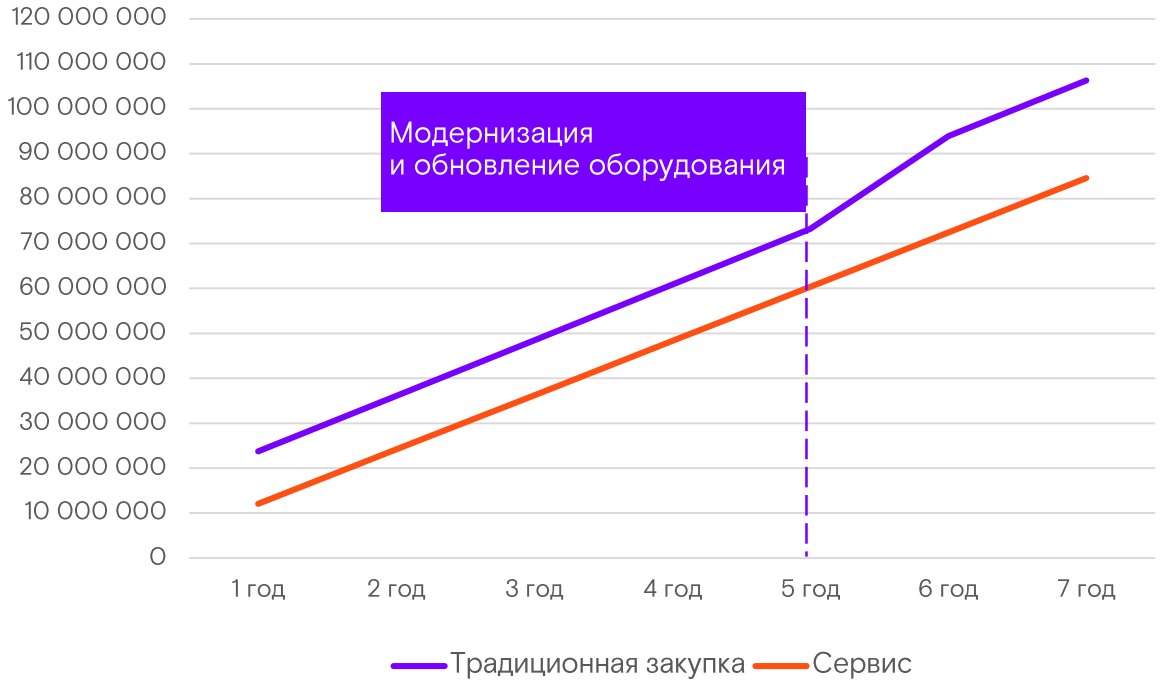
Ростелеком
Солар

Статья на Anti-Malware про экономику сервисного решения

Сравнение стоимости владения. Вариант 2

Количество офисов:

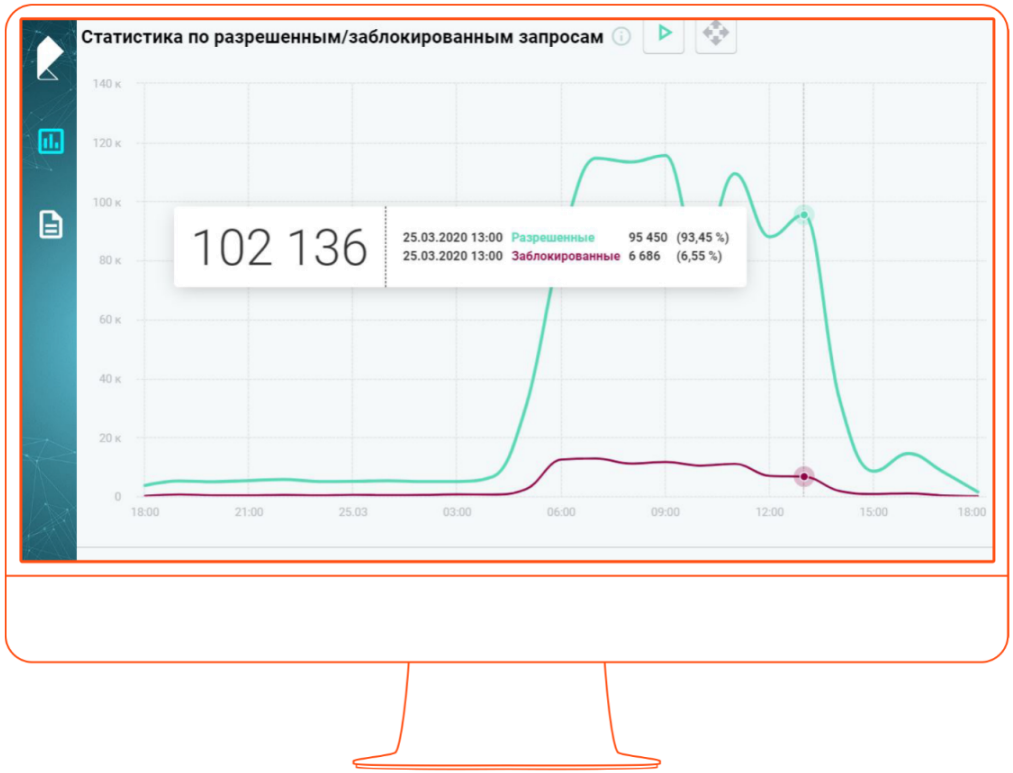
10 офисов
+
200 филиалов



Ростелеком
Солар

[Статья на Anti-Malware про экономику сервисного решения]

Личный кабинет Solar MSS – единое окно



- Связь с личным менеджером и технической поддержкой
- Подключение новых сервисов в один клик
- Гибко настраиваемые виджеты
- Детализированная статистика по атакам и угрозам
- Информация о статусах подписок на сервисы
- Понятные отчеты для представления руководству

Ростелеком
Солар

Тезисно

Функциональность лидеров рынка МЭ

Централизация доступа в сеть для филиалов

Единые политики безопасности и отчетность

Поддержка и мониторинг в режиме 24×7×365

Solar JSOC – экспертные сервисы кибербезопасности

Solar JSOC – крупнейший коммерческий SOC в России*,
защищающий как своих клиентов, так и другие корпоративные SOC

Решаемые задачи

- Мониторинг и реагирование на инциденты ИБ
- Проверка устойчивости к кибератакам
- Техническое расследование инцидентов ИБ
- Разведка на основе открытых источников (OSINT)
- Мониторинг АСУ ТП и субъектов КИИ (SOC OT)
- Создание SOC и Центров ГосСОПКА
- Эксплуатация SOC по гибридной модели

Ключевые преимущества

- 200+ сотрудников в 5 филиалах
- Работа в режиме 24/7/365
- Крупнейшая база IoC от лидеров отрасли
- Отработанные процессы, 100+ клиентов
- SLA – 99,5%, персональный менеджер
- Сотрудничество с ФинЦЕРТ ЦБ РФ, ФСТЭК России и НКЦКИ ФСБ России

*Anti-Malware. Сравнение услуг коммерческих SOC (Security Operations Center). Часть 1. 2019

Филиалы Solar JSOC и ПАО «Ростелеком»

Ростелеком
Солар

ПАО «Ростелеком»

Филиалы Solar JSOC

Продуктовый портфель «Ростелеком-Солар»

СЕРВИСЫ

SOLAR MSS
управляемые сервисы кибербезопасности

- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Защищенная удаленная работа (SRW)
- Контентная фильтрация (CF)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)
- Регистрация и анализ событий (ERA)

Технологической основой Solar MSS является ЕПСК* – уникального для России проекта на основе технологий SD-WAN, NFV и ZTP

SOLAR JSOC
экспертные сервисы кибербезопасности

- Мониторинг, реагирование и анализ инцидентов ИБ
- Комплексный контроль защищенности
- Техническое расследование инцидентов
- Эксплуатация систем ИБ и реагирование на атаки
- Построение SOC и его частных процессов
- Мониторинг АСУ ТП и субъектов КИИ (SOC OT)
- Сервисы ГосСОПКА

Первый и крупнейший коммерческий центр по мониторингу и реагированию на инциденты кибербезопасности (SOC) в России

* Единая платформа сервисов кибербезопасности

УСЛУГИ

- **Интеграционные услуги (8)**
- **Сервисная поддержка (6)**
- **Соответствие требованиям (6)**
- **Кибербезопасность АСУ ТП (7)**

ТЕХНОЛОГИИ

- **Solar Dozor** (DLP)
- **Solar appScreener** (SAST)
- **Solar inRights** (IdM/IGA)
- **Solar webProxy** (SWG)

Ростелеком Солар

Заказать бесплатный пилот сервисов

presale@rt-solar.ru

Ростелеком
Солар