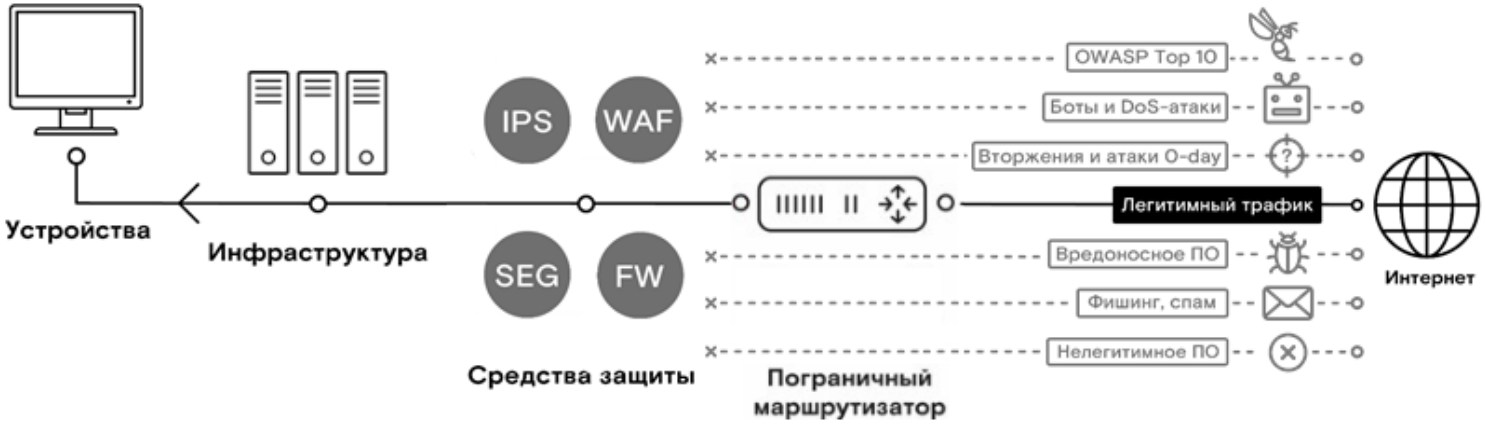
ИБ аутсорсинг

managed security services

Что можно и нужно отдавать на аутсорсинг

Ростелеком
Солар

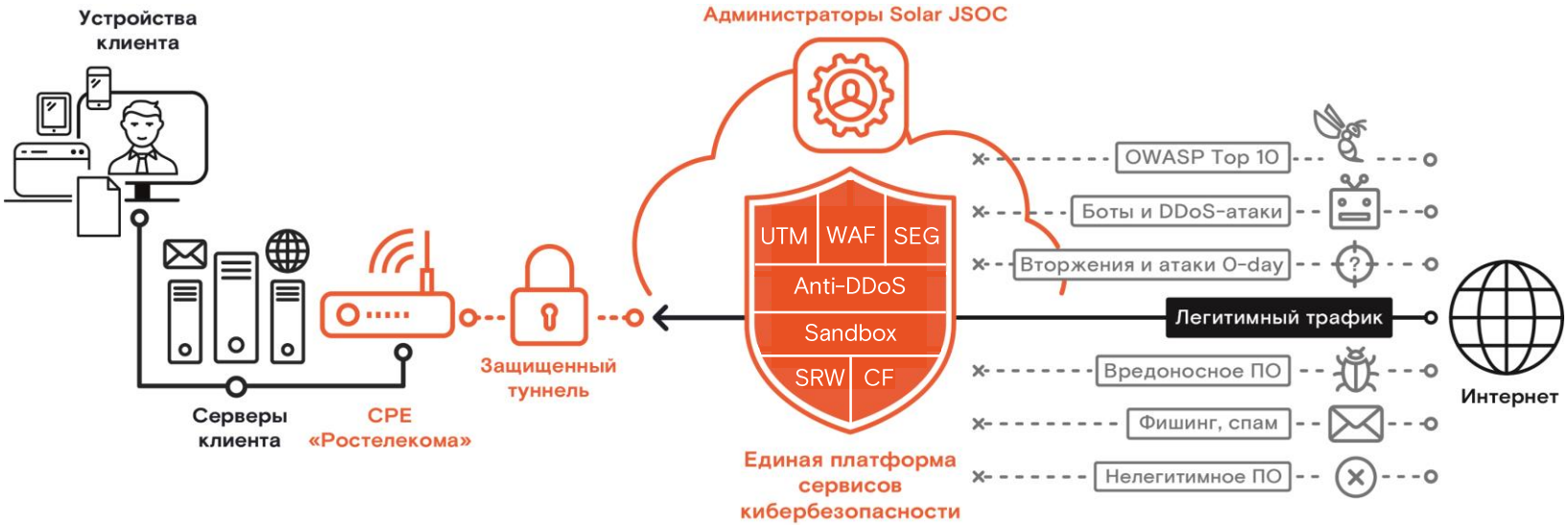
Традиционный подход к ИБ



Сегмент ИС клиента	Сеть провайдера	Интернет

Ростелеком
Солар

Сервисная модель



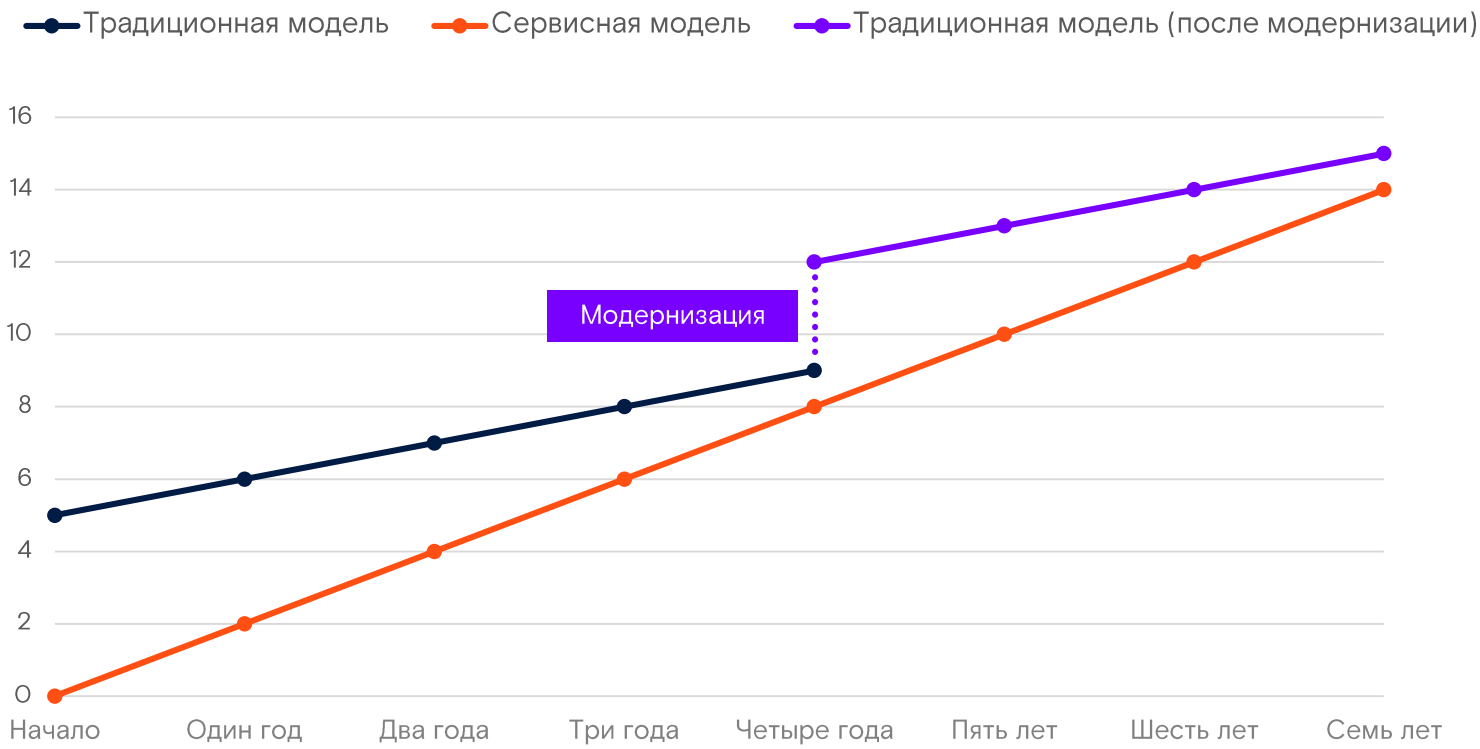
Сегмент ИС клиента	Облако «Ростелеком-Солар» в ЦОДах и Узлах Связи Ростелекома	Сеть Интернет

Ростелеком
Солар

TCO сервисной модели

Ростелеком
Солар

TCO сервисной модели



Ростелеком
Солар

ЕПСК – технологическая основа Solar MSS

Единая платформа сервисов кибербезопасности (ЕПСК) – уникальный для РФ проект на основе технологий программно-определяемых сетей (SD-WAN), виртуализации сетевых функций (NFV) и автоматической настройки оборудования (ZTP)

Сервисы на базе ЕПСК

- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Защита от продвинутых угроз (Sandbox)
- Защищенная удаленная работа (SRW)
- Контентная фильтрация (CF)

ЕПСК развернута в НОП на масштабируемых мощностях

Сервисы ЕПСК могут использоваться как одновременно, так и по отдельности

Для быстрого подключения к ЕПСК могут применяться CPE (Customer Premises Equipment)

Ростелеком
Солар

Customer Premises Equipment

Оконечное телекоммуникационное оборудование, использующее технологии Zero Touch Provisioning

С его помощью осуществляется:

- Подключение к локальной сети
- Перенаправление целевого трафика в ЦОДы ЕПСК
- Формирование шифрованного туннеля до ЕПСК
- Обеспечение сетевой связности между офисами по схеме Full Mesh
- Организация отказоустойчивого подключения

Варианты исполнения

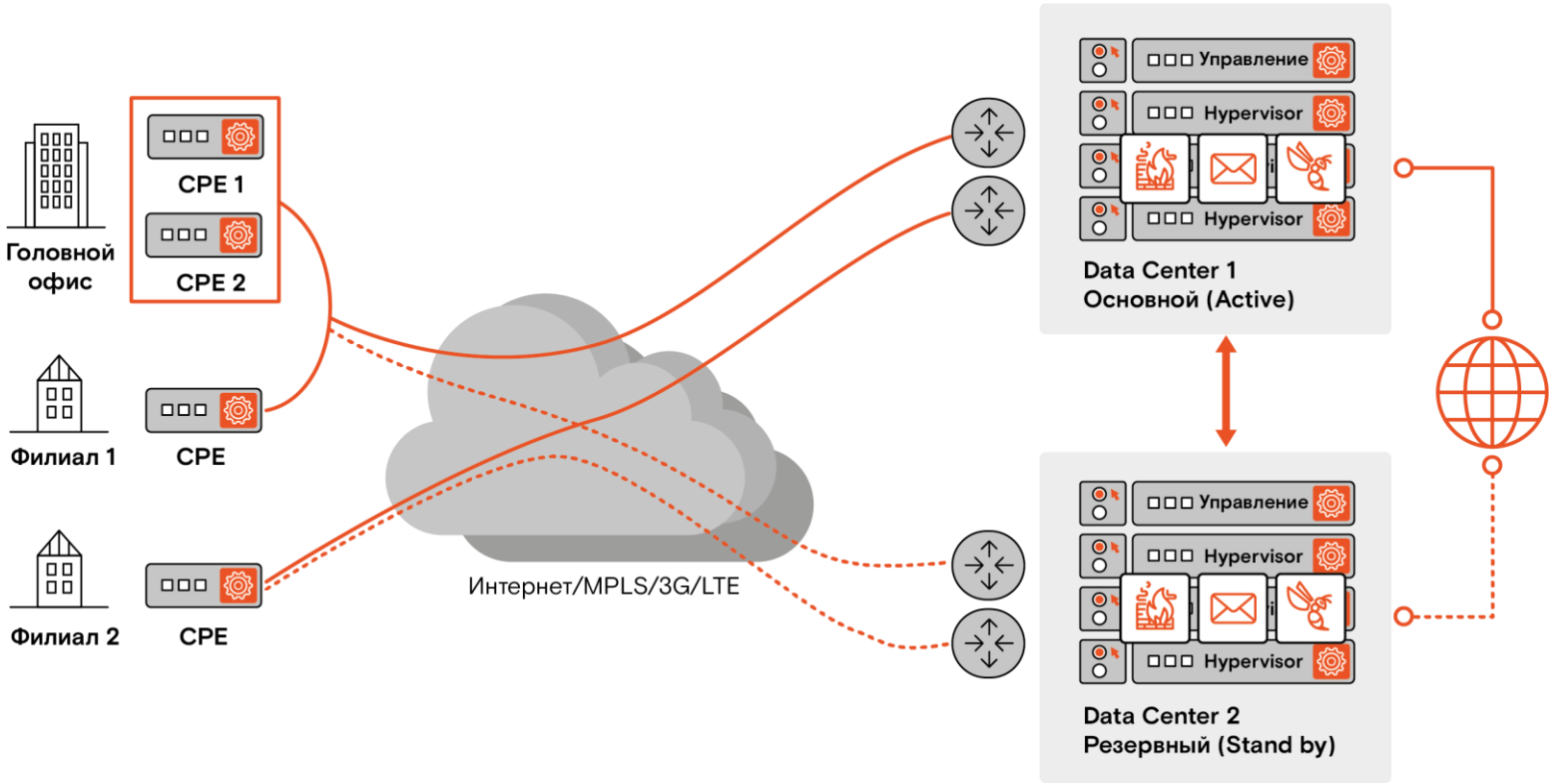
до 70 Мбит/с

до 200 Мбит/с

до 1 000 Мбит/с

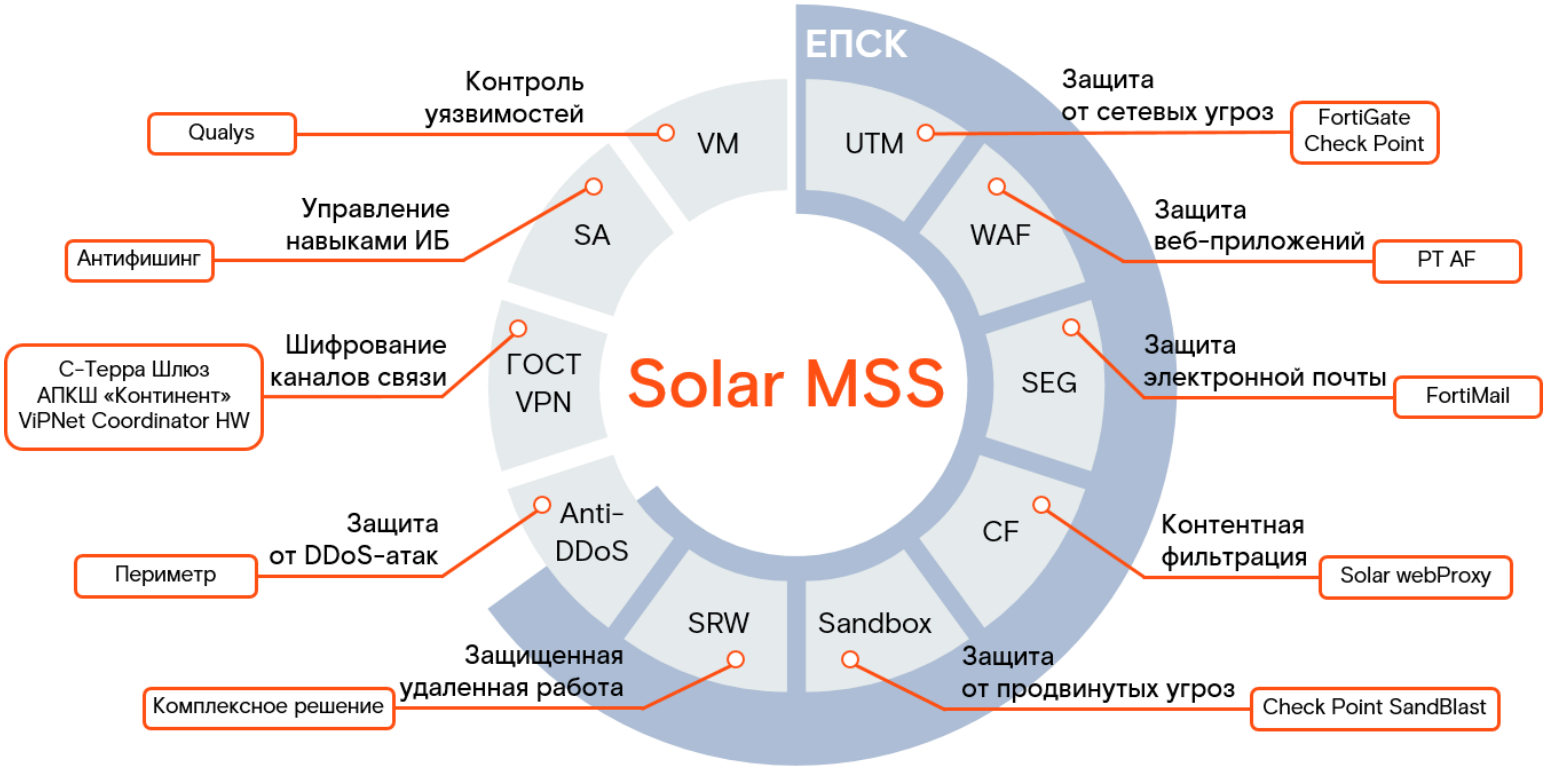
Ростелеком
Солар

Высокоуровневая архитектура подключения



Ростелеком
Солар

Экосистема Solar MSS



Ростелеком
Солар

Unified Threat Management

Сервис защиты от сетевых угроз

Ростелеком
Солар

Сервис защиты от сетевых угроз (UTM) ЕПСК

Обеспечивает комплексную защиту сетевого периметра при помощи нескольких взаимосвязанных средств защиты: межсетевого экрана, IPS, антивируса, веб- и спам-фильтров

Решаемые задачи

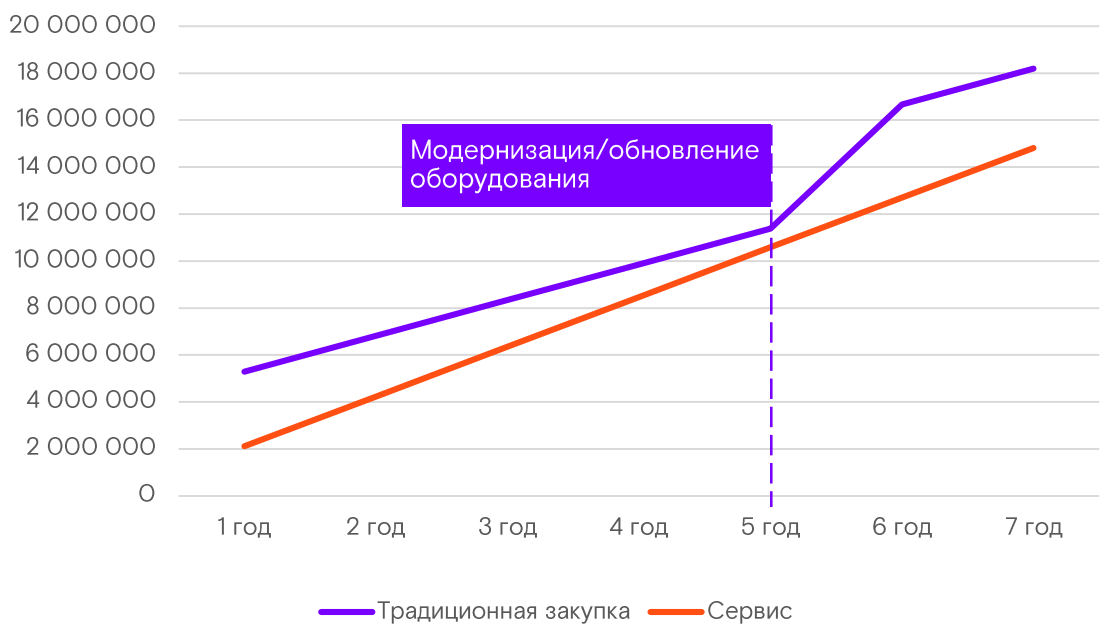
- Комплексная борьба с сетевыми угрозами
- Применение единых политик информационной безопасности во всей организации
- Централизация доступа в сеть для филиалов
- Круглосуточная защита от атак
- Фильтрация трафика и контроль использования веб-приложений

Ключевые преимущества

- Быстрое подключение новых точек
- Объединение разрозненных функций защиты сети
- Всегда актуальные настройки и сигнатуры
- Мгновенное применение единых ИБ-политик
- Единая система статистики по ИБ

Сравнение стоимости владения. Вариант 1

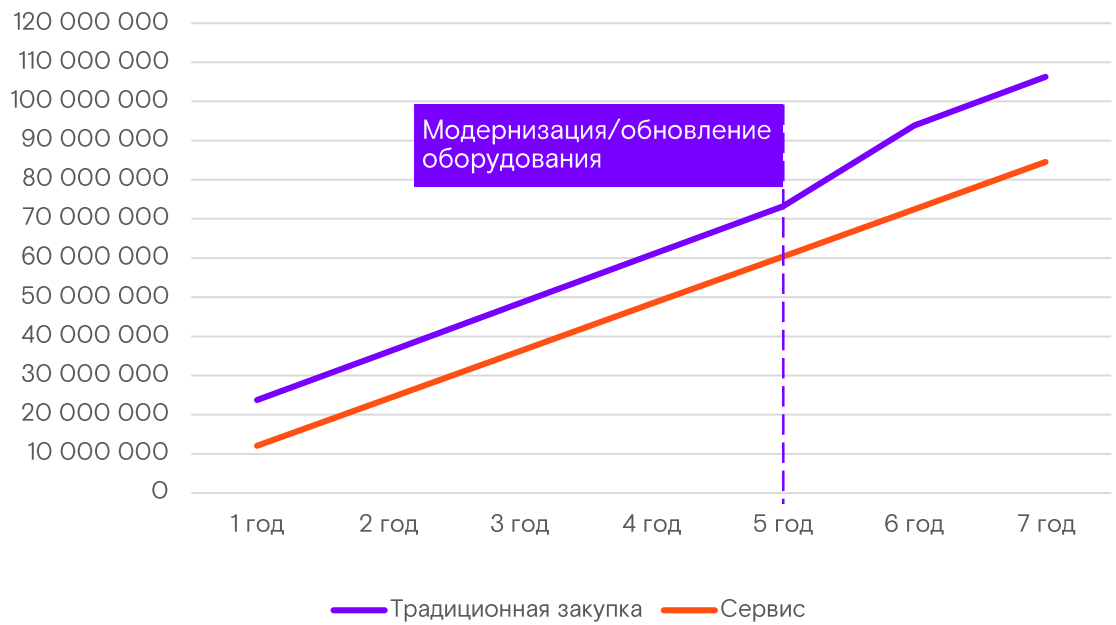
Средство защиты:	Аппаратный межсетевой экран/NGFW/UTM
Количество офисов:	1 главный офис + 20 филиалов
Пропускная способность с включенными функциями безопасности:	до 200 Мбит/сек



Ростелеком
Солар

Сравнение стоимости владения. Вариант 2

Средство защиты:	Аппаратный межсетевой экран/NGFW/UTM
Количество офисов:	10 офисов + 200 филиалов
Пропускная способность с включенными функциями безопасности:	до 1000 Мбит/сек



Ростелеком
Солар

Кейс: UTM для учреждения здравоохранении

О заказчике

- Сфера деятельности: здравоохранение
- Размер: 7 площадок, 200+ сотрудников

Задача

- Комплексная защита от сетевых атак
- Закрытие дефицита ИБ-специалистов
- Защита в режиме 24/7/365

Решение

- Подключение с помощью CPE (входят в стоимость)
- Сервис оказывается в круглосуточном режиме
- Нет затрат на оборудование, новых специалистов, обучение
- Актуальные настройки и мониторинг работоспособности обеспечивают специалисты «Ростелекома»

Результат

- Стоимость подписки – 80 000 рублей в месяц
- Начальные затраты на 95% ниже, чем в проектной модели
- Скорость фильтрации трафика – 100 Мбит/с

Ростелеком
Солар

Secure Email Gateway

Сервис защиты электронной почты

Ростелеком
Солар

Сервис защиты электронной почты (SEG) ЕПСК

Позволяет организовать многоуровневую проверку электронной почты до того, как она достигнет почтовых серверов организации и будет доставлена конечному пользователю

Решаемые задачи

- Защита почты от спама, фишинга и вредоносного ПО
- Фильтрация URL
- Поддержка черных и белых списков
- Email-аутентификация
- Снижение нагрузки на почтовые серверы

Ключевые преимущества

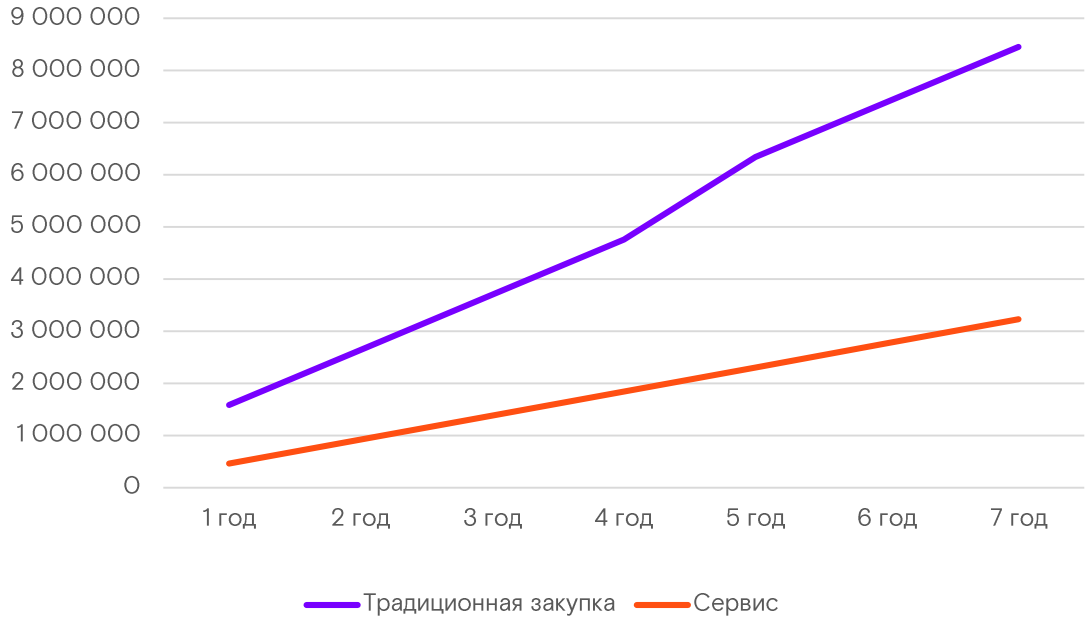
- Высокая производительность — до 1 000 000 писем в час
- Быстрое подключение новых точек
- Оперативное изменение параметров сервиса
- Мониторинг и реагирование в круглосуточном режиме

Сравнение стоимости владения. Вариант 1

Производитель: Fortinet

Количество почтовых ящиков: 300

Пропускная способность: 52 000 писем/час



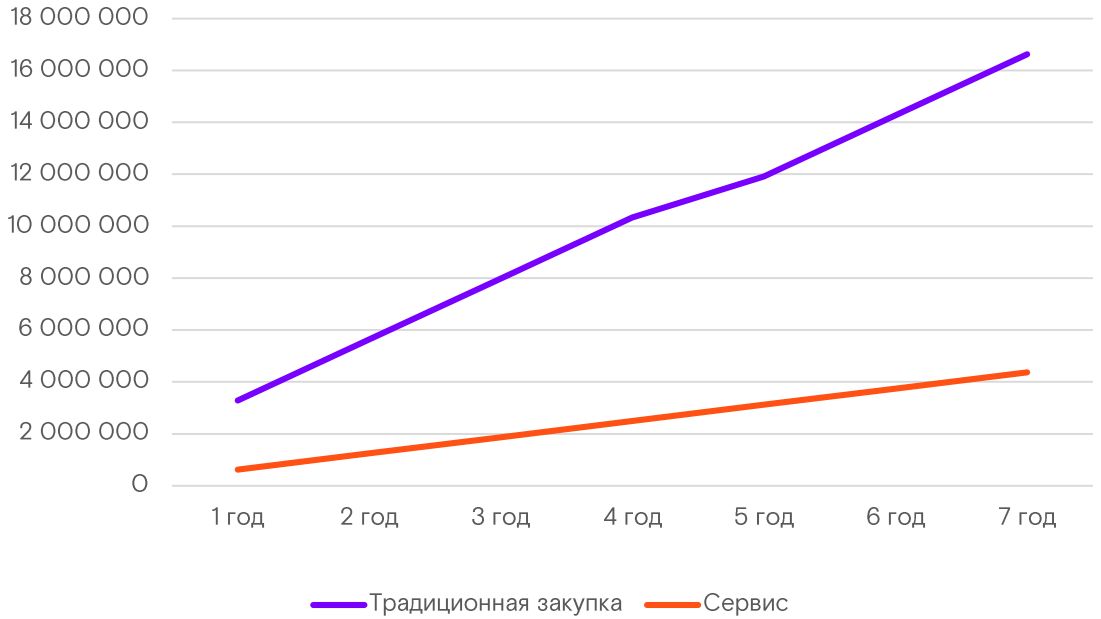
Ростелеком
Солар

Сравнение стоимости владения. Вариант 2

Производитель: Fortinet

Количество почтовых ящиков: 2000

Пропускная способность: 225 000 писем/час



Ростелеком
Солар

Кейс: SEG для производственной компании

О заказчике

- Сфера деятельности: производство (завод сыроварения)
- Размер: 400+ сотрудников

Задача

- Защита почтового трафика от спама, фишинга и вредоносного ПО
- Защита почтового сервера, находящего на стороннем хостинге
- Закрытие дефицита ИБ-специалистов

Решение

- SLA (Service Level Agreement) – 99,5%
- Нет затрат на оборудование, новых специалистов, обучение
- Актуальные настройки и мониторинг работоспособности обеспечивают специалисты Ростелекома

Результат

- Стоимость подписки на сервис – 20 000 рублей в месяц
- Начальные затраты на 85% ниже, чем в проектной модели
- У заказчика отсутствовал собственный DNS-хостинг, поэтому сервис подключили к стороннему DNS-хостингу
- Предоставлено комплексное решение, включающее сервис VPN и SEG

Ростелеком
Солар

Sandbox

Сервис защиты от продвинутых угроз

Ростелеком
Солар

Сервис защиты от продвинутых угроз (Sandbox) ЕПСК

Сервис обеспечивает комплексную защиту от продвинутых и ранее неизвестных угроз в реальном времени, функционируя как самостоятельно, так и в связке с сервисами UTM или SEG

Решаемые задачи

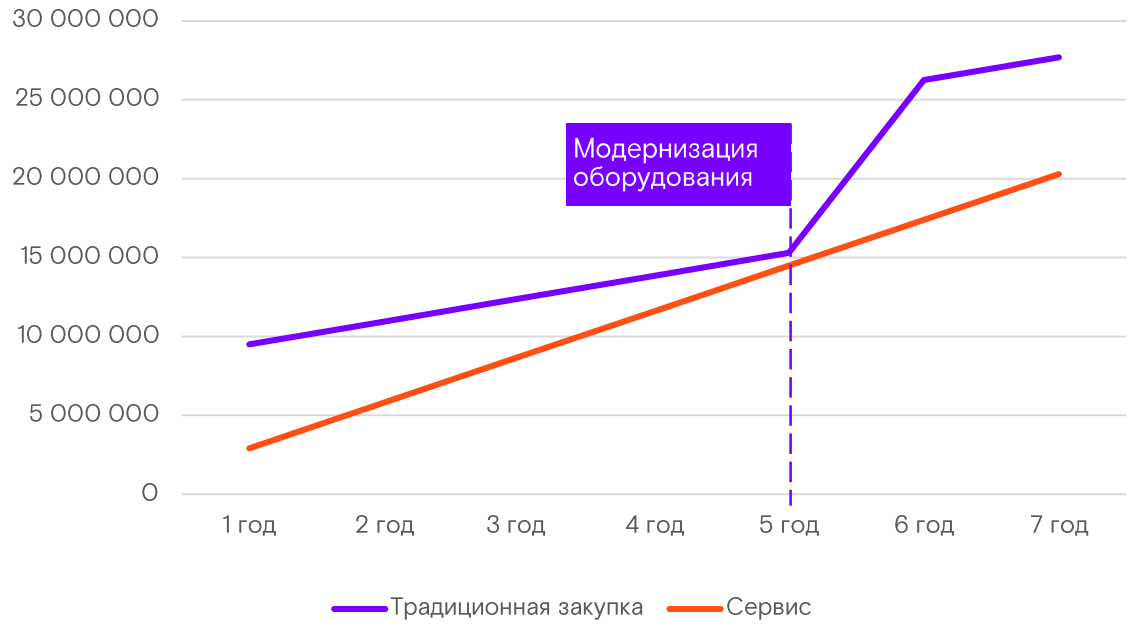
- Обнаружение сложно детектируемых угроз в почте и веб-трафике
- Снижение затрат на построение и эксплуатацию системы защиты
- Проверка скрытых угроз в зашифрованном трафике протоколов SSL/TLS
- Расширение возможностей сервисов UTM и SEG по противостоянию актуальным угрозам

Ключевые преимущества

- Подключение за 5 рабочих дней
- Анализ угроз незаметен для пользователей и не влияет на их работу
- Безопасный доступ к содержимому файла уже на этапе его анализа
- Защита от обхода, действующая на уровне процессора
- Детализированные отчеты об угрозах и анализируемом трафике
- В основе сервиса – лучшая песочница согласно отчету NSS Labs за 2019 год

Сравнение стоимости владения

Производитель: Check Point



Ростелеком
Солар

Web Application Firewall

Сервис защиты веб-приложений

Ростелеком
Солар

Сервис защиты веб-приложений (WAF) ЕПСК

Обнаруживает и блокирует атаки на веб-приложения, которые пропускают традиционные межсетевые экраны и системы обнаружения вторжений (атаки OWASP Top 10, 0-day, атаки L7)

Решаемые задачи

- Защита от атак из списка OWASP Top 10 (SQL-инъекции, XSS и т. д.)
- Защита от DDoS-атак уровня приложений
- Выявление аномального поведения и атак нулевого дня
- Защита от уязвимостей веб-приложений
- Круглосуточный мониторинг и реагирование

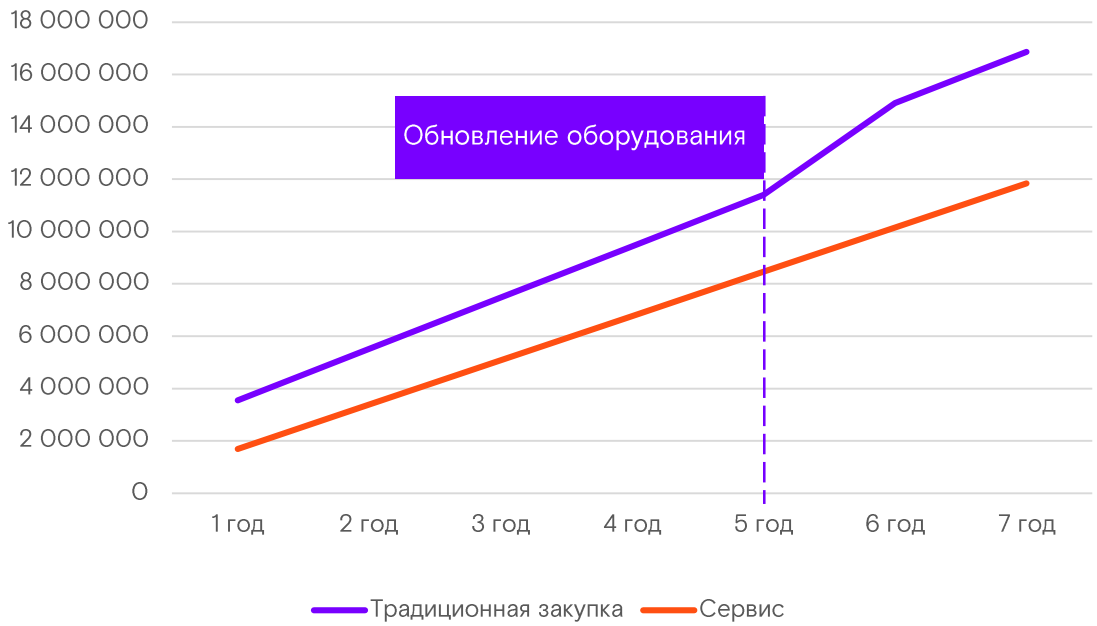
Ключевые преимущества

- Быстрое подключение новых точек
- Применение актуальных настроек и сигнатур
- Снижение затрат на персонал и оборудование
- Консультации по применению сервиса

Сравнение стоимости владения

Производитель: Positive Technologies

Производительность: 1000 RPS



Ростелеком Солар

Кейс: WAF для ритейлера

О заказчике

- Сфера деятельности: продажа электроники
- Регион: вся территория России
- Размер: 1 000+ магазинов

Задача

- Оперативное создание и внедрение сложных правил на WAF, в том числе для защиты от ботов и атак типа brute force для защиты интернет магазина
- Закрытие дефицита ИБ-специалистов (инженер ушел к конкуренту)
- Защита в режиме 24/7/365

Решение

- SLA (Service Level Agreement) – 99,5%
- Сервис оказывается в круглосуточном режиме
- Нет затрат на оборудование, новых специалистов, обучение
- Актуальные настройки и мониторинг работоспособности обеспечивают специалисты Ростелекома

Результат

- Стоимость подписки на сервис – 120 000 рублей в месяц
- Физический WAF заказчика был заменен на сервис
- Начальные затраты на 95% ниже, чем в проектной модели
- Заказчик может оперативно обновлять сайт без рисков для бизнеса

Anti-DDoS

Сервис защиты от DDoS-атак

Ростелеком
Солар

Сервис защиты от DDoS-атак (Anti-DDoS) ЕПСК

Предоставляет эшелонированную защиту от DDoS-атак. Противодействие осуществляется на всех уровнях модели OSI – от уровня канала до бизнес-логики приложения

Решаемые задачи

- Возможность предоставления чистого канала – защита от DDoS всех интернет-приложений клиента ■
- Защита от атак, направленных непосредственно на IP-адрес ресурса (Direct to Origin) ■
- Защита инфраструктуры – фильтрация атак уровня L3-L4 емкостью 5+ Тбит/с
- Защита приложений и служб – фильтрация атак уровня L7 полосой более 300 Гбит/с
- Ускорение веб-сайта за счет предоставления CDN ■
- Сервис защиты веб-приложений ■

Ключевые преимущества

- В отсутствие атаки трафик доставляется до защищаемого ресурса без перемаршрутизации ■
- Подключение даже во время атаки ■
- Мониторинг и реагирование на инциденты в режиме 24/7
- Отсутствие дополнительных платежей за количество и максимальную полосу атак ■
- Для использования сервиса необязательно быть клиентом Ростелекома
- Обработка трафика на территории России

■ Технические параметры и преимущества могут меняться в зависимости от варианта предоставления сервиса

Кейс: Anti-DDoS для банка

О заказчике

- Сфера деятельности: банк (топ-20)
- Регион: вся территория России

Задача

- Защита от DDoS-атак
- Защита в условиях шантажа со стороны злоумышленников
- Закрытие дефицита ИБ-специалистов

Решение

- SLA (Service Level Agreement) – 99,5%
- Нет затрат на оборудование, новых специалистов, обучение
- Актуальные настройки и мониторинг работоспособности обеспечивают специалисты Ростелекома

Результат

- Стоимость подписки на сервис – 80 000 рублей в месяц
- Паразитный трафик был эффективно отфильтрован
- Клиенты банка не заметили атаку

«Просим заплатить выкуп в 2 биткоина за то, что мы не будем атаковать ваш сайт и платежную систему. Текущий защитник 100% не справится с нашим DDoS. По результатам оплаты мы подскажем сервис, который в дальнейшем поможет вам эффективно защищаться от любого DDoS»

Ростелеком
Солар

Content Filtering

Сервис контентной фильтрации

Ростелеком
Солар

Сервис контентной фильтрации (CF) ЕПСК

Контролирует доступ в интернет, категорирует и фильтрует трафик клиента, что позволяет отсечь противоправный контент и выполнить требования российского законодательства

Решаемые задачи

- Контроль доступа сотрудников в интернет
- Защита от вредоносного ПО
- Категорирование ресурсов
- Фильтрация противоправного контента
- Выполнение требований российского законодательства

Ключевые преимущества

- Единая точка контроля веб-трафика
- Готовые политики для быстрого старта
- Полное соответствие требованиям импортозамещения
- Отказоустойчивость и масштабируемость
- Отсутствие затрат на внедрение, обновление ПО и последующую замену дорогостоящего оборудования
- Круглосуточная техническая поддержка

Кейс: CF для производственной компании

О заказчике

- Сфера деятельности: производство
- Размер: 500+ сотрудников

Задача

- Необходимость фильтрации противоправного контента
- Закрытие дефицита ИБ-специалистов

Решение

- Перевод капитальных затрат в операционные
- Нет затрат на оборудование, новых специалистов, обучение
- Актуальные настройки и мониторинг работоспособности обеспечивают специалисты «Ростелекома»

Результат

- Стоимость подписки на сервис – 400 000 рублей в год
- Годовые затраты на 55% ниже, чем в проектной модели
- Сервис защищает компанию от вредоносного ПО
- Обеспечен контроль доступа сотрудников в интернет

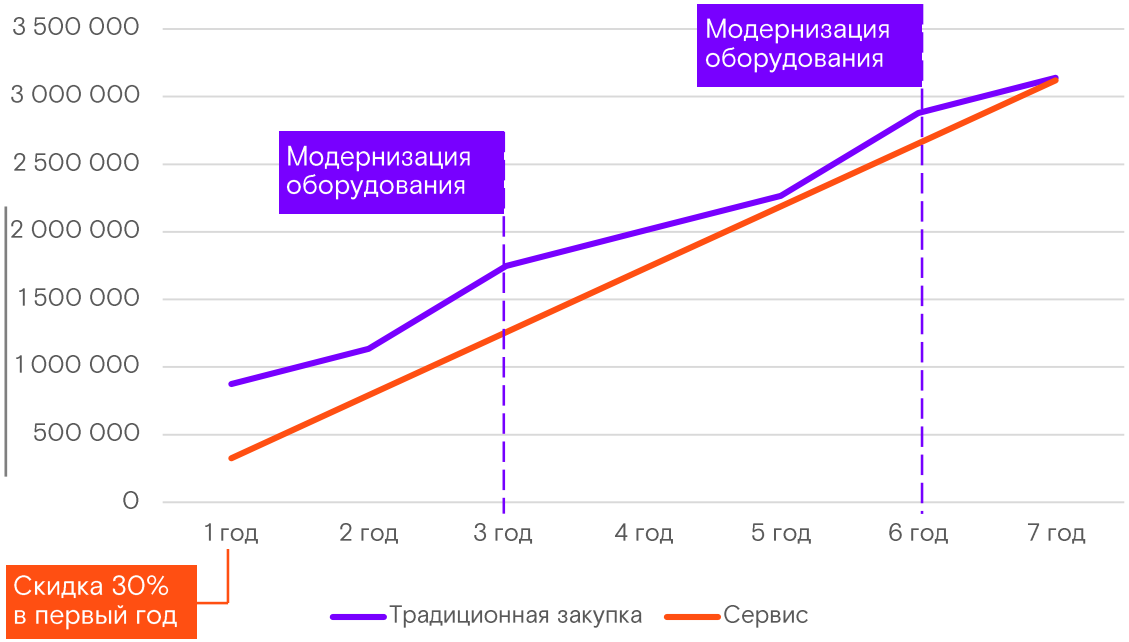
Сравнение стоимости владения

Решение в традиционной закупке

Ideco

Решение в основе сервиса

Solar webProxy



Ростелеком Солар

ГОСТ VPN

Сервис шифрования каналов связи

Ростелеком
Солар

Сервис шифрования каналов связи (ГОСТ VPN)

Защищает информацию при передаче по открытым каналам связи, обеспечивая конфиденциальность и целостность данных

Решаемые задачи

- Защита каналов уровня L2/L3 модели OSI
- Построение новых и обслуживание существующих защищенных сетей
- Предотвращение утечек данных
- Модернизация по запросу
- Быстрое развертывание

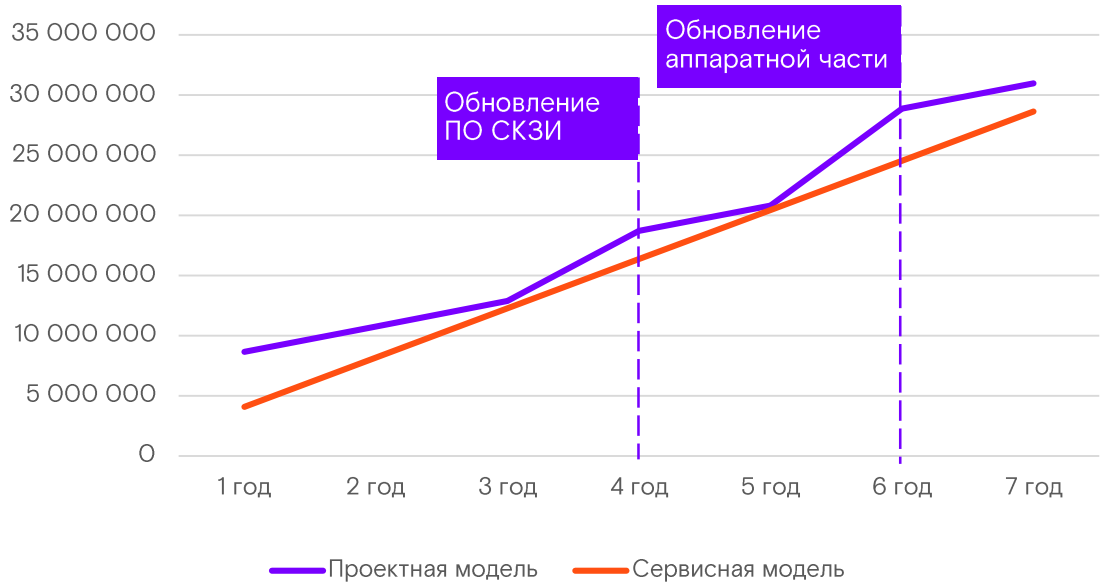
Ключевые преимущества

- Выполнение требований законодательства и регуляторов РФ
- Класс криптозащиты – КС3
- Сертификаты ФСБ России и ФСТЭК России
- Возможность подключения сервиса и услуг связи в рамках единого договора
- Мониторинг работоспособности с жестким SLA
- Снижение затрат на владение системой криптозащиты

Ростелеком
Солар

Сравнение стоимости владения

Производитель:	Инфотекс
Количество офисов:	1+49
Расположение персонала управления сетью:	Регионы (не Москва)



Ростелеком Солар

Кейс: ГОСТ VPN для учреждения здравоохранения

О заказчике

- Сфера деятельности: здравоохранение
- Региональный МИАЦ
- Размер: 2 000 человек в центральном узле + 200 лечебно-профилактических учреждений (ЛПУ)

Задача

- Выполнение требований Минздрава по шифрованию каналов связи по ГОСТ
- Стандартизация парка оборудования
- Кадровый дефицит
- Решение проблем работы с одним интегратором

Решение

- Платежи за сервис распределены по месяцам и полностью прозрачны
- Учет СКЗИ, актуальные настройки и мониторинг работоспособности обеспечивает Ростелеком
- Отсутствие проблем с выбором оборудования и его интеграцией в ИТ-инфраструктуру
- Класс защиты – КС3

Результат

- Каналы связи защищены, требования Минздрава выполнены, SLA - 99,5%
- Стоимость подписки на сервис – 650 000 рублей в месяц
- Начальные затраты на 90% ниже, чем в проектной модели
- Подключены все площадки без снижения пропускной способности каналов

Ростелеком
Солар

Vulnerability Management

Сервис контроля уязвимостей

Ростелеком
Солар

Сервис контроля уязвимостей (VM)

Комплексный сервис на базе облачного решения ведущего мирового вендора Qualys обеспечивает полный контроль над уязвимостями сетевой инфраструктуры заказчика

Решаемые задачи

- Исследование внешнего периметра и локальной сети заказчика
- Инвентаризация, поиск уязвимостей, конфигурационный анализ и проверка на соответствие политикам безопасности
- Подготовка технических и аналитических отчетов, проверка возможности эксплуатации найденных уязвимостей
- Разовое и периодическое сканирование или постоянный мониторинг в режиме 24/7

Ключевые преимущества

- Экспертиза – в распоряжении заказчика все силы и средства «Ростелеком-Солар»
- Оперативность – подключение сервиса на следующий день после обращения
- Кастомизируемость – анализ корпоративных порталов, маршрутизаторов, АРМ удаленных сотрудников и т.д.
- Безопасность – облако Qualys размещено на территории России в ЦОД «Ростелеком»
- Масштабируемость – от 10 IP сегодня к 100 000 завтра
- Синергия – контроль уязвимостей, пентест, услуги Solar JSOC

Ростелеком
Солар

Кейс: VM для производственной компании

О заказчике

- Сфера деятельности: автомобилестроение
- Размер: 200+ сотрудников

Задача

- Оперативный анализ защищенности
- Подготовка материалов для предоставления в суде по делу о недобросовестной конкуренции

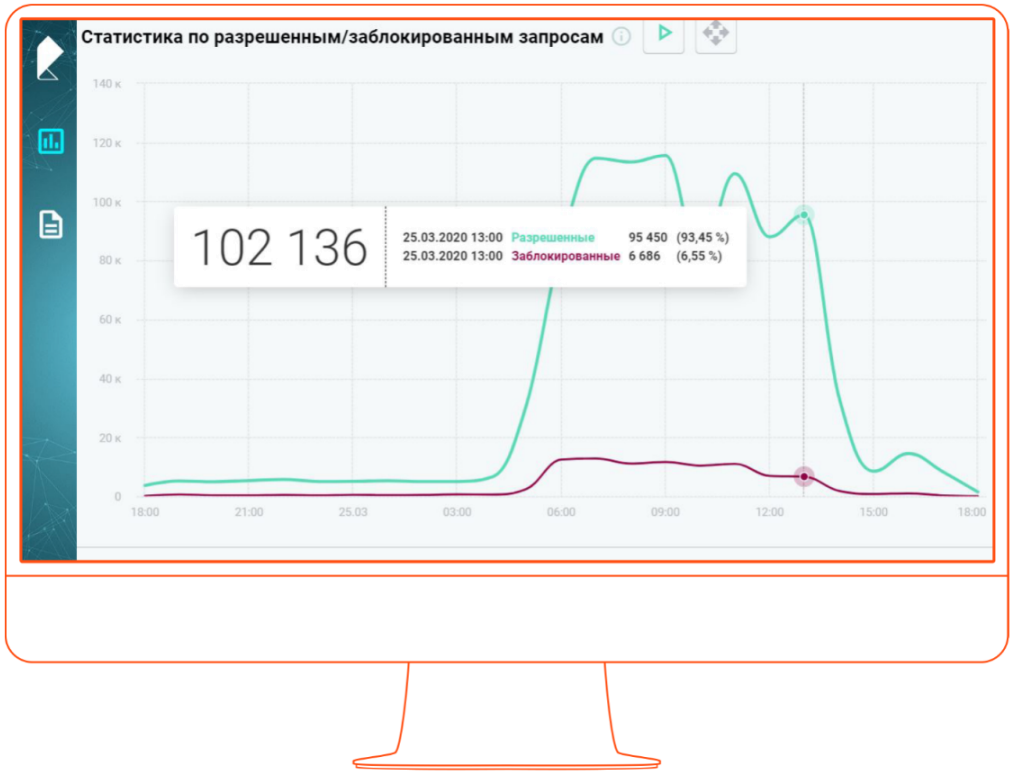
Решение

- Использование сервиса для однократного расширенного сканирования ресурсов внешнего периметра
- Проверка возможности эксплуатации найденных уязвимостей
- Подготовка аналитического отчета по результатам

Результат

- Стоимость – 185 000 рублей
- Сканирование, речек найденных уязвимостей и подготовка отчета проведены в рекордные сроки – 10 дней
- Отчет представлен в суде, заказчик выиграл дело

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

Сервисная модель

Экономия и эффективность

Снижение стоимости владения

Совокупная стоимость владения сервисами дешевле покупки, внедрения и последующей поддержки ИБ-решений

Устранение дефицита кадров

Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов

Экономия

Снижение затрат на оборудование и персонал, перевод капитальных издержек в операционные

Профессиональная команда

Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли

Технологичность и надежность

Доступность

Защита и мониторинг 24 часа в сутки без перерывов и выходных

Надежность

Эксплуатация распределенной отказоустойчивой инфраструктуры

Гибкость

Простая масштабируемость и быстрое изменение параметров услуги

Скорость

Быстрое подключение к сервисам и оперативное реагирование на инциденты

Соблюдение законодательства

Соответствие требованиям

Выполнение требований по информационной безопасности

Подходящие средства защиты

Эксплуатация сертифицированных решений лидирующих вендоров

Лицензии регуляторов

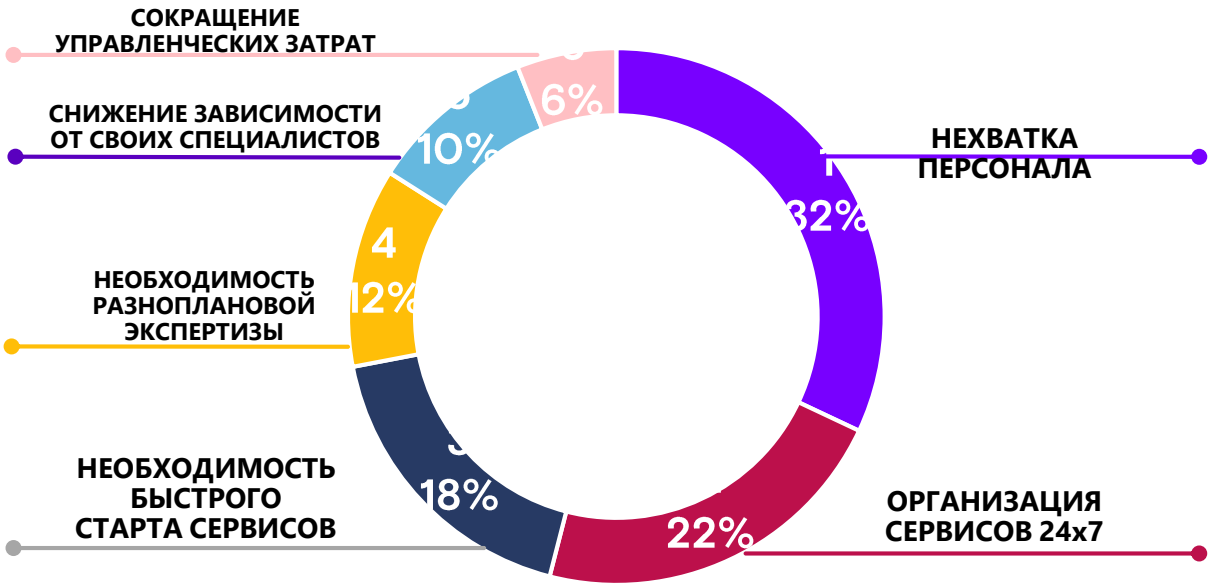
Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России

Отслеживание изменений

Меры защиты всегда соответствуют всем новым законам и регламентам

Ростелеком
Солар

Почему обращаются к сервисам



Почему мы?

- Сервисы удобнее и дешевле. Есть бонусы и плюшки
- Традиционный подход к защите дорог и не является профильной деятельностью компании
- Можно сфокусироваться на основном бизнесе и расширить возможности по привлечению клиентов за счет снижения затрат
- Экосистема сервисов постоянно развивается с учетом всех потребностей и требований законодательства
- Сервисная модель – тренд трансформации спроса на примере всех рынков

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Узнать подробнее или заказать сервис

presale@rt-solar.ru

Ростелеком
Солар