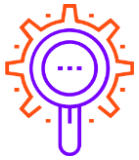
Сервисная модель как решение задач ИБ в условиях неопределенности

Solar MSS
Managed Security Services

Ростелеком
Солар

Продуктовый портфель «Ростелеком-Солар»



Сервисы

- Solar JSOC – первый и крупнейший в России коммерческий центр противодействия кибератакам
- Solar MSS - экосистема управляемых сервисов кибербезопасности по подписке

Технологии

- Solar Dozor – предотвращение утечек информации
- Solar webProxy – контроль доступа к веб-ресурсам
- Solar appScreener – анализ кода приложений
- Solar inRights – управление правами доступа
- Solar addVisor – организационное развитие и оценка продуктивности труда

Интеграция

Solar Интеграция

- Реализация комплексных проектов по кибербезопасности
- Кибербезопасность объектов КИИ и АСУ ТП

Киберполигон

- Национальный киберполигон - повышение квалификации сотрудников отрасли кибербезопасности

Обеспечение кибербезопасности

На первый взгляд

- Средства защиты
- Сотрудники ИБ-службы

Если приглядеться

- Процессы
- Методология
- Мониторинг угроз
- Актуальные политики безопасности
- Повышение осведомленности сотрудников о киберугрозах

Ростелеком
Солар

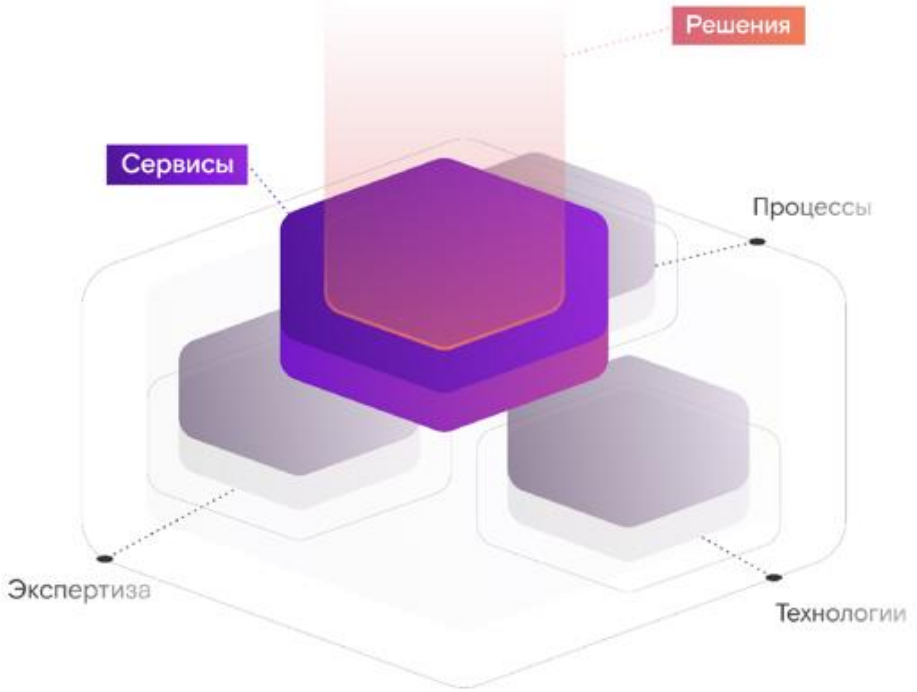
Проблемы и их решение

- Необходимо быстро найти замену продуктам иностранных вендоров, сохранив должный уровень защиты
- Нет платформ для развертывания СЗИ
- Трудно понять, какую задачу решать в первую очередь – за что хвататься?
- Не хватает персонала для решения ИБ-задач
- Нет возможности оперативно получить бюджет на капитальные расходы
- Нужен надежный партнер по кибербезопасности, которому не страшно доверить защиту ресурсов

Сервисы ИБ по подписке от национального провайдера кибербезопасности

Ростелеком Солар

Экосистема Solar MSS



- Мониторинг трафика и защита от DDoS-атак
- Защита веб-приложений
- Предотвращение сетевых атак
- Защита электронной почты
- Шифрование каналов связи
- Контроль уязвимостей
- Защита от продвинутых угроз (Sandbox)
- Управление навыками кибербезопасности

Ростелеком
Солар

Обеспечиваем кибербезопасность по подписке

Просто

От 2 дней
на подключение сервиса –
и его можно использовать

75%
сервисов и решений
подключаются
без вмешательства
в инфраструктуру

Выгодно

Гибкие тарифы
основаны на клиентском опыте

на 40%
в среднем ниже вложения
в сравнении с интеграцией
on-premise-продуктов

Надежно

Высокий уровень
подготовки экспертов
по кибербезопасности

Ответственность
в рамках договорных
обязательств, соответствие
строгим SLA

Ростелеком
Солар

Кратный рост запросов на сервисы

С начала марта наблюдается значительное увеличение заявок и подключений сервисов, защищающих корпоративные сети и онлайн-ресурсы. Лидируют следующие сервисы:

Мониторинг трафика и защита от DDoS-атак (Anti-DDoS)

Защита веб-приложений (WAF)

Предотвращение сетевых атак (UTM)

На 220%

Выросло количество заявок на сервис по защите от DDoS-атак за март по сравнению с февралем

На 27%

Больше запросов на защиту веб-приложений было получено за март 2022 года в сравнении со всем 2021 годом

В 4,5 раза

Увеличился спрос на сервис по защите от сетевых атак в марте по сравнению с февралем

Ростелеком Солар

Сервис мониторинга трафика и защиты от DDoS-атак

Онлайн-ресурсы стабильно защищены и остаются доступными круглосуточно

- Отражение массивных атак до 5 Тбит/с без прерывания рабочего процесса
- Легкая масштабируемость при подключении новых офисов по всей территории России
- Снижение трудозатрат со стороны заказчика – все работы выполняют специалисты ПАО «Ростелеком» и «Ростелеком-Солар» в режиме 24/7

Ростелеком Солар

Сервис защиты веб-приложений

Технологии

Противодействие атакам на веб-приложения за счет эксплуатации многоступенчатых модулей защиты, включающих анализ трафика и блокировку атак

Экспертиза специалистов «Ростелеком-Солар»

- Круглосуточная эксплуатация решения
- Адаптация решения под специфику бизнеса клиента
- Многолетний опыт в противодействии кибератакам

Ростелеком Солар

Решаемые задачи

Круглосуточный мониторинг и отражение атаки в автоматическом режиме

Снижение рисков взлома, кражи информации, в том числе платежной, подмены информации на сайтах, отказа работы веб-приложений

Оптимизация затрат на обеспечение кибербезопасности информационных систем

Соответствие требованиям регуляторов

Ростелеком Солар

Сервис предотвращения сетевых атак

Технологии

Межсетевое экранирование, система обнаружения вторжений, контроль трафика запускаемых приложений и посещаемых веб-ресурсов

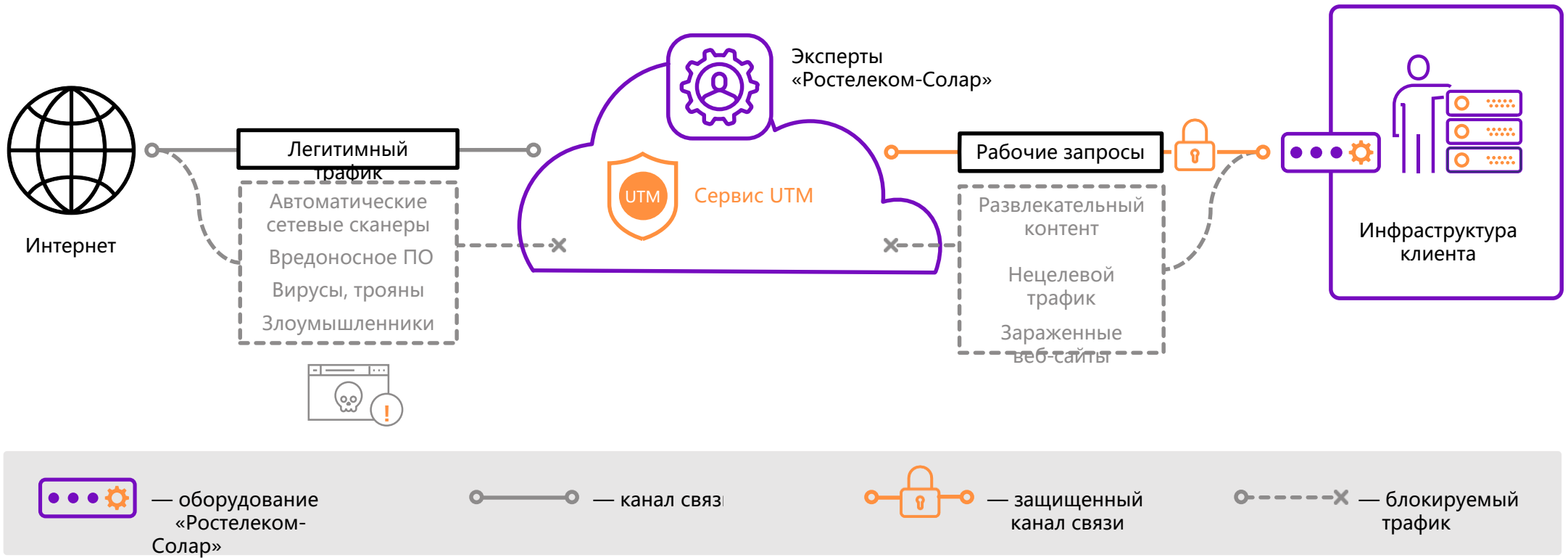
Экспертиза специалистов «Ростелеком-Солар»

- Анализ сетевой инфраструктуры организации и подбор оптимального варианта сервиса. Своевременное обновление политик и программно-аппаратной части
- Формирование правил защиты и адаптация под бизнес-требования организации. Поддержка от квалифицированных сервис-менеджеров

Ростелеком Солар

Очистка трафика с помощью UTM

Решение предотвращает сетевые угрозы и позволяет контролировать доступ сотрудников к веб-ресурсам



Ростелеком Солар

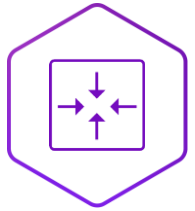
Вы получаете

Решение «все в одном»:

- межсетевой экран на периметре
- система обнаружения и предотвращения вторжений
- антивирусный шлюз
- веб-фильтр
- доступ удаленных пользователей
- личный кабинет

Снижение затрат на персонал и оборудование

Конфигурация и мониторинг работоспособности в режиме 24/7



Единые правила доступа для всех филиалов

Использование актуальных обновлений и сигнатур

Ростелеком Солар

Зачем нужно защищать почту

Электронная почта — один из ключевых инструментов коммуникации в организации.
Всего **одно** вредоносное письмо может нарушить бизнес-процессы, обернуться кражей персональных данных или денег.

75%
Сработавших сложных кибератак реализованы через фишинг

51%
Входящих писем — спам

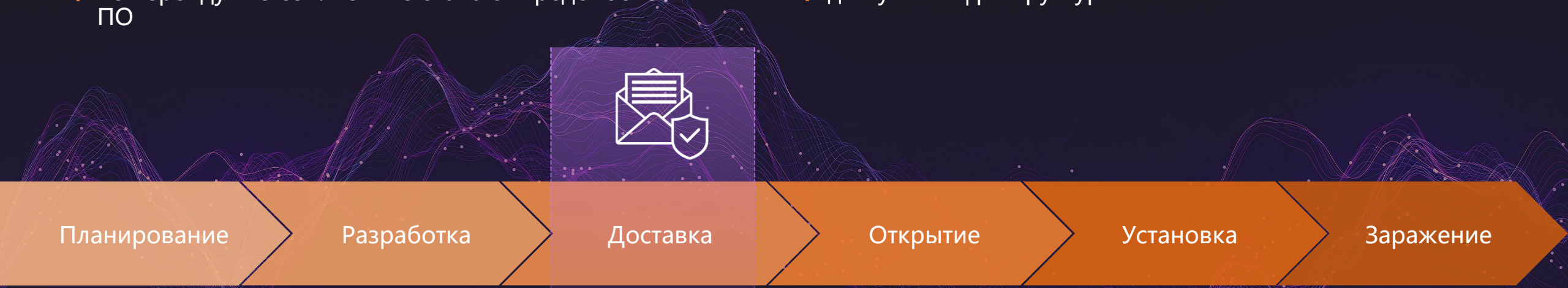
22%
Случаев утечки данных связаны с фишингом

18%
Организаций, подвергшихся фишинговой атаке, несут финансовые потери

Почему вредоносное ПО важно найти на этапе доставки

Раннее сканирование минимизирует риски: сотрудники не откроют вредоносные письма, не перейдут по ссылке и не скачают вредоносное ПО

Вредоносное ПО не будет установлено на устройство, злоумышленники не получат доступ к инфраструктуре



Сервис защиты электронной почты перехватывает вредоносное программное обеспечение на этапе доставки. Это самый надежный вариант защиты от вирусов: нелегитимные письма не будут доставлены сотрудникам.

Ростелеком Солар

Сервис защиты электронной почты

Технологии

Защита от угроз, связанных с использованием электронной почты: фишинга и вредоносного ПО. Фильтрует спам, снижает нагрузку на почтовый сервер и освобождает время сотрудников на целевые задачи

Экспертиза специалистов «Ростелеком-Солар»

Подключение и обновление защиты, настройка политик фильтрации
командой «Ростелеком-Солар»

Ростелеком Солар

Сервис управления навыками кибербезопасности

Сотрудники вашей организации повышают киберграмотность, процесс обучения проходит под контролем экспертов

- Эффективное обучение сотрудников
  С помощью курсов и проверочных тестирований сотрудники изучают все основные темы, посвященные кибербезопасности, и закрепляют знания на практике, реагируя на учебные фишинговые рассылки

- Экспертиза
  Обучающие курсы и тренировочные фишинговые рассылки готовят сотрудники «Ростелеком-Солар» на основе актуальных угроз кибербезопасности

Ростелеком Солар

Почему важно тренировать навыки на практике

Традиционные методы обучения: брошюры, учебники и лекции – неэффективны

Почему?

- Недостаточно интересный материал
- Непонимание масштаба проблемы
- Нехватка мотивации
- Неправильная оценка работы ИБ-отдела

49%

пользователей меняют поведение в течение года после тренировки навыков через имитированные атаки

По данным «Ростелеком-Солар»

Эффективность интерактивного обучения, которое требует принятия конкретных решений, в 9 раз выше

По данным InfoSec Institute

Ростелеком Солар

Типовой график оказания сервиса

В рамках регламента каждая группа сотрудников проходит 2 цикла. После этапа обучения предусмотрен перерыв, чтобы повысить сложность атаки на этапе проверки знаний.

- прохождение курсов и тестов

- рассылка тренировочных фишинговых рассылок

График адаптируется под заказчика и зависит от срока оказания сервиса. Интенсивность циклов зависит от количества пользователей.

Сервис контроля уязвимостей

Технологии

Поиск уязвимостей и информационных активов в сетевой инфраструктуре организации

Экспертиза специалистов «Ростелеком-Солар»

- Обработка результатов сканирования
- Разработка рекомендаций по устранению уязвимостей
- Контроль выполнения рекомендаций

Ростелеком Солар

Как работает сервис

3. Обработка

Обогащаем результаты данными базы киберугроз и экспертизой аналитиков «Ростелеком-Солар», приоритизируем и проверяем на практике, можно ли эксплуатировать выявленные
в инфраструктуре уязвимости

2. Сканирование

Проводим инструментальный поиск уязвимостей

1. Инвентаризация

Осуществляем сбор данных о всех информационных активах в организации.

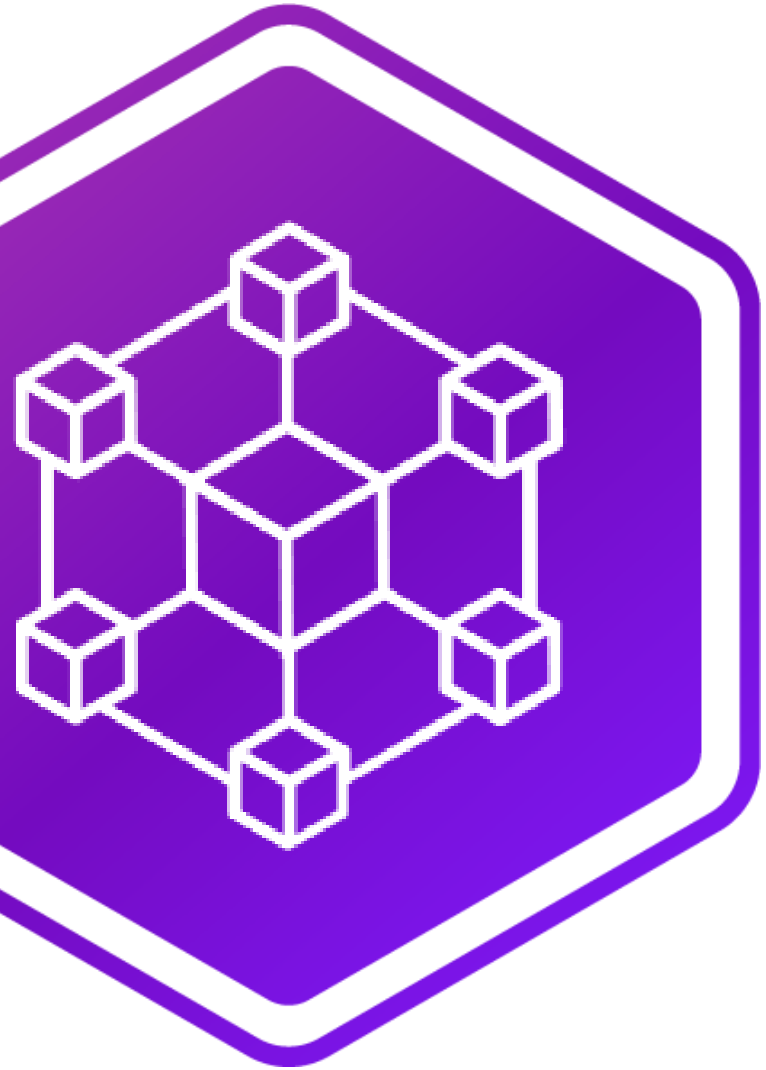
4. Устранение

Разрабатываем меры по повышению уровня защищенности, в т. ч. помогаем спланировать закрытие уязвимостей

5. Контроль

Проверяем выполнение плана устранения уязвимостей

Ростелеком Солар



Сервис шифрования каналов связи

Построение и эксплуатация защищенных сетей для компаний любых регионов с помощью сертифицированных СКЗИ по подписке.

Сервис обеспечивает конфиденциальность и целостность данных,
а все работы выполняют специалисты ПАО «Ростелеком» и «Ростелеком-Солар».

Ростелеком Солар

Параметры сервиса

1

В рамках сервиса используются СКЗИ, сертифицированные ФСБ России по классу КС3

2

Использование СКЗИ ведущих вендоров: С-Терра, ИнфоТеКС, Код Безопасности

3

Высокий уровень доступности, SLA – 99,5 %

4

Круглосуточная эксплуатация «Ростелеком-Солар»

Ростелеком Солар

Решаемые задачи

Защита сетей

Предоставление и эксплуатация защищенных сетей силами специалистов «Ростелекома» и «Ростелеком-Солар»

Оптимизация бюджетов

Решение проблемы нехватки бюджетов за счет более низкой стоимости сервиса и разбиения платежей на удобные части

Работа во всех регионах

Поддержка распределенных филиальных сетей во всех регионах страны

Работоспособность сети

Обеспечение высокой эффективности работы сети в режиме 24/7 и SLA не менее 99,5%

Ростелеком Солар

Пример реализации ГОСТ VPN в ПАО «Банк ВТБ»

Высочайшая надежность по всей России

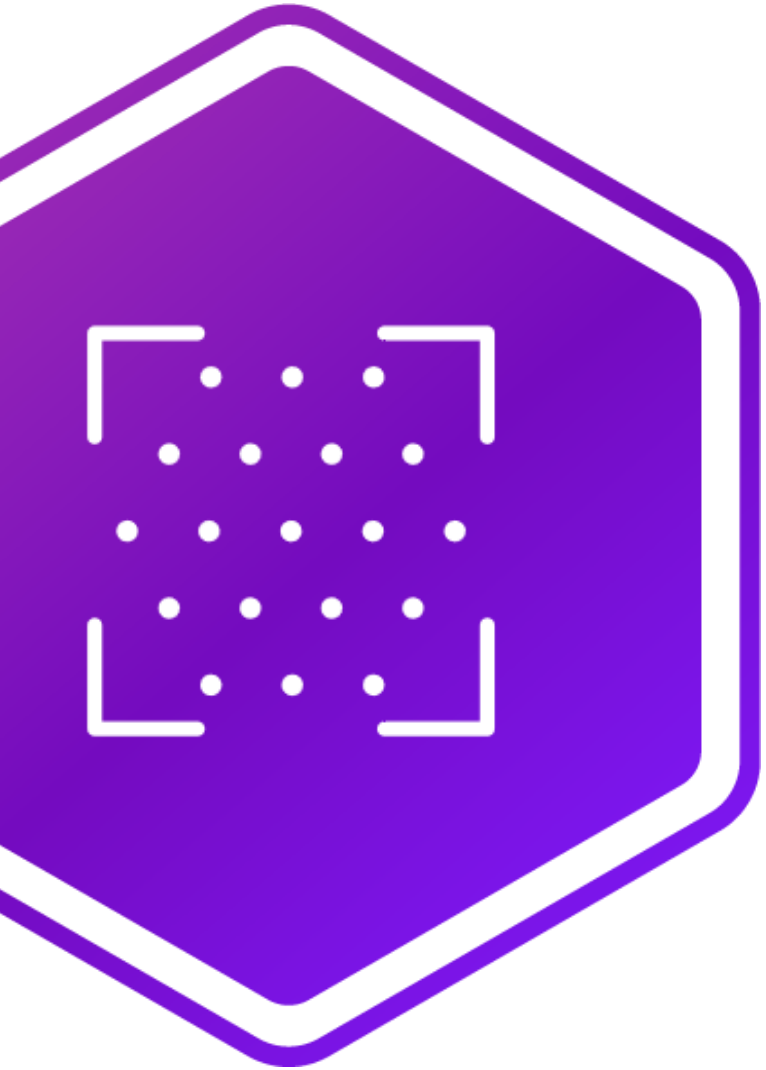
Профиль заказчика

- Сфера деятельности: федеральный банк
- Регион: вся территория РФ
- Размер: ЦОД и 1500 филиалов

Результат

- Предоставлены каналы связи с криптозащитой, а также Anti-DDoS
- Реализовано резервирование каналов связи и криптошлюзов, SLA – 99,99%
- Выполнены требования ФСБ России
- Поддержка 3000 каналов и криптошлюзов осуществляется в режиме одного окна
- Ведение журналов учета СКЗИ и ключевой информации, а также перечня лиц, администрирующих СКЗИ, находится в зоне ответственности провайдера

Ростелеком Солар



Сервис защиты от продвинутых угроз

Технологии

- Автоматическая защита от неизвестных и маскирующихся угроз в почтовом и веб-трафике
- Проверка на уровне операционной системы и центрального процессора
- Мгновенная доставка копии файла пользователю

Экспертиза

- Анализ ИТ-инфраструктуры и формирование оптимального для клиента варианта защиты от продвинутых угроз
- Конфигурирование правил блокирования файлов, настройка соответствующих изолированных сред
- Поддержка от квалифицированных сервис-менеджеров

Ростелеком Солар

Преимущества сервиса защиты от продвинутых угроз

Защита от техник обхода песочниц с помощью механизма Anti-Evasion

Проверка на вредоносность осуществляется на уровне CPU, т. е. до того момента, как вредоносное ПО попытается проникнуть и скрыться в инфраструктуре

Создание безопасной копии проверяемого файла без потери времени

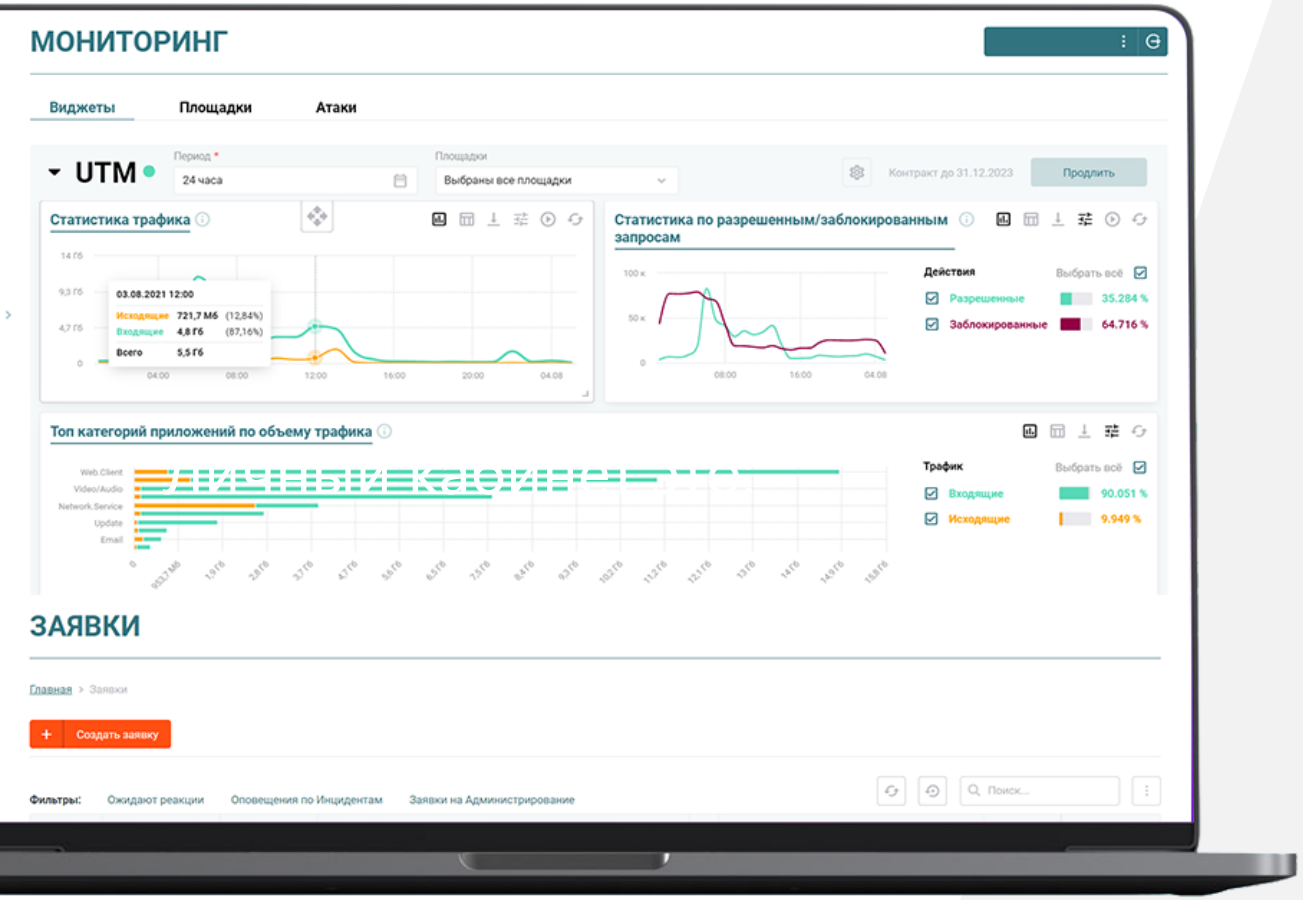
Безопасная копия файла создается мгновенно (Threat Extraction), поэтому сотрудникам не нужно ждать завершения проверки, и процесс работы не прерывается

Подробный анализ вредоносного кода и блокировка опасных объектов

Все электронные письма проходят специальную проверку (Threat Emulation), которая позволяет обнаружить вредоносные объекты и блокировать опасные и подозрительные ссылки

Ростелеком Солар

Высокотехнологичное управление



Личный кабинет – это:

- ✓ Оперативная связь с личным менеджером
- ✓ Актуальные статусы подписок
- ✓ Детализированные отчеты для руководства
- ✓ Индивидуально настраиваемые виджеты по работе сервисов
- ✓ Информативные ответы на частые вопросы
- ✓ Подробная информация о заявках в техническую поддержку

Подробнее о личном кабинете

Ростелеком Солар

Контакты

Центральный офис

125009 г. Москва
Никитский переулок, 7с1
+7 (499) 755-07-79

Запросите бесплатную
консультацию эксперта

solar@rt-solar.ru