



Центр кибербезопасности Solar MSS

Managed Security Services

Крупнейшая в России экосистема
сервисов кибербезопасности
по подписке

Ростелеком
Солар



Тренды кибератак в 2021 году



Основные типы атак через ВПО и атаки на веб-приложения



Повышение темпа использования новых уязвимостей



Фишинг, смишинг и вишинг продолжают набирать обороты



Рост популярности атак через подрядчиков



Удаленная работа – основной катализатор изменений



Расслоение подходов злоумышленников к атакам на инфраструктуру

Ландшафт киберугроз

16%

компаний способны эффективно сопротивляться кибератакам

По данным Accenture, 2021 г.

50,8%

событий ИБ удается выявить лишь с помощью сложных интеллектуальных средств защиты или анализа событий

По данным Solar JSOC, 2021 г.

68%

анализируемых компаний, где выявлена активность ВПО

По данным Positive Technologies, 2021 г.

x2

рост атак через подрядчиков на объекты КИИ

По данным Solar JSOC, 2021 г.

+30%

рост атак на получение контроля над инфраструктурой организации

По данным Solar JSOC, 2021 г.

207 дней

среднее время обнаружения компанией взлома ее инфраструктуры

По данным Ponemon Institute, 2020 г.

Специфика кибератак в регионах России



Топ по количеству атак

1 — Москва

646 тыс. атак

Вредоносное ПО – 29%

Атаки на веб-приложения – 38%

DDoS-атаки – 7%

2 — Сибирский ф. о.

228 тыс. атак

Вредоносное ПО – 30%

Атаки на веб-приложения – 39%

DDoS-атаки – 6%

3 — Дальневосточный ф. о.

184 тыс. атак

Вредоносное ПО – 28%

Атаки на веб-приложения – 42%

DDoS-атаки – 8%

4 — Северо-Западный ф. о.

178 тыс. атак

Вредоносное ПО – 32%

Атаки на веб-приложения – 31%

DDoS-атаки – 11%

5 — Уральский ф. о.

161 тыс. атак

Вредоносное ПО – 33%

Атаки на веб-приложения – 27%

DDoS-атаки – 9%

6 — Приволжский ф. о.

127 тыс. атак

Вредоносное ПО – 43%

Атаки на веб-приложения – 24%

DDoS-атаки – 8%

7 — Центральный ф. о.

122 тыс. атак

Вредоносное ПО – 36%

Атаки на веб-приложения – 25%

DDoS-атаки – 8%

8 — Южный ф. о.

58 тыс. атак

Вредоносное ПО – 41%

Атаки на веб-приложения – 29%

DDoS-атаки – 6%

Сервисная модель – решение проблем

Предпосылки

- | Рост количества атак на компании
- | Оптимизация расходов
- | Дефицит кадров

Каждая 10-я компания

ежегодно подключает управляемые сервисы кибербезопасности*

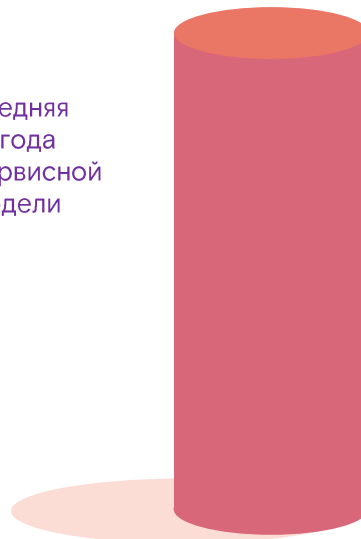
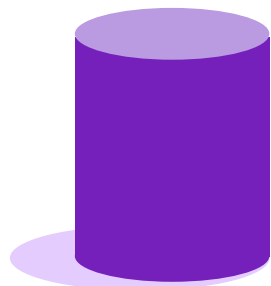
* По данным MSSP Alert, 2021

Ростелеком
Солар

Сервисная модель

35%

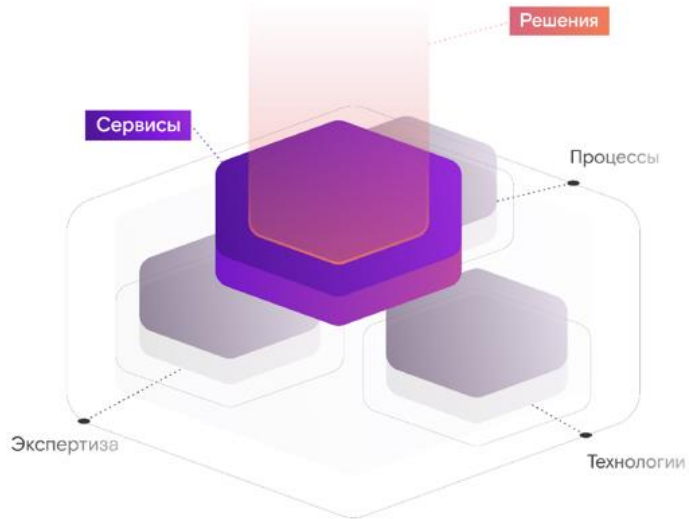
средняя выгода сервисной модели



Построение кибербезопасности своими силами

- Подписка на сервис + лицензии
- Содержание специалистов
- Запасное оборудование
- Меньше скидка на закупку
- Аппаратное обеспечение
- Аренда помещения
- Закупка оборудования и замена своими силами

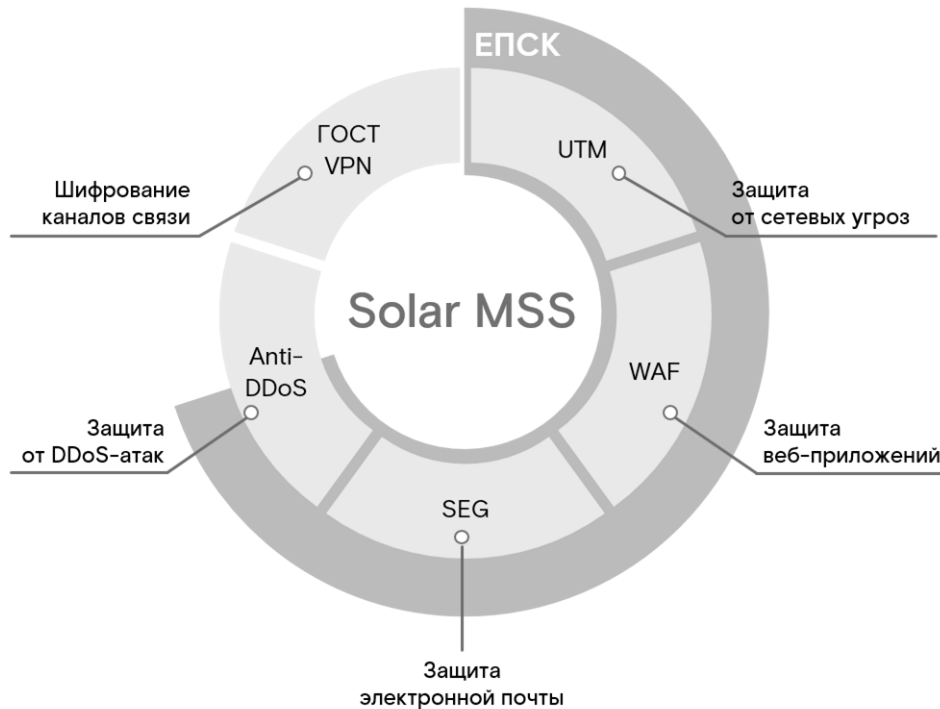
Экосистема Solar MSS сегодня



Solar MSS – крупнейшая в России экосистема сервисов кибербезопасности по подписке. Сервисы защищают от всего спектра угроз и решают комплексные задачи кибербезопасности.

Эксперты «Ростелеком-Солар» осуществляют все работы с учетом специфики каждого региона, профиля и масштаба компании в режиме 24×7. Разнообразие технологий в составе экосистемы и партнерство с ведущими поставщиками ИБ позволяют предоставить клиентам широкий выбор вариантов сервисов и снизить санкционные риски.

Solar MSS – первый провайдер сервисов в России



Экосистема в 2018 г.

- | Предоставление технологий в аренду
- | Небольшое количество сервисов
- | Фокус на защите от отдельных угроз

От предоставления технологий к комплексному закрытию рисков

Было



Защита клиента от отдельных угроз



Предоставление технологий
по сервисной модели



Стало

Защита с фокусом на бизнес-активах

Комплексное решение задач клиента

Полноценная внешняя команда экспертов
с единой точкой взаимодействия

Сервисы Solar MSS

Защита от сетевых угроз (UTM)



Защита веб-приложений (WAF)



Управление навыками ИБ (SA)



Контроль уязвимостей (VM)



Защита электронной почты (SEG)



Контентная фильтрация (CF)



Шифрование каналов связи (ГОСТ VPN)



Защита от продвинутых угроз (Sandbox)



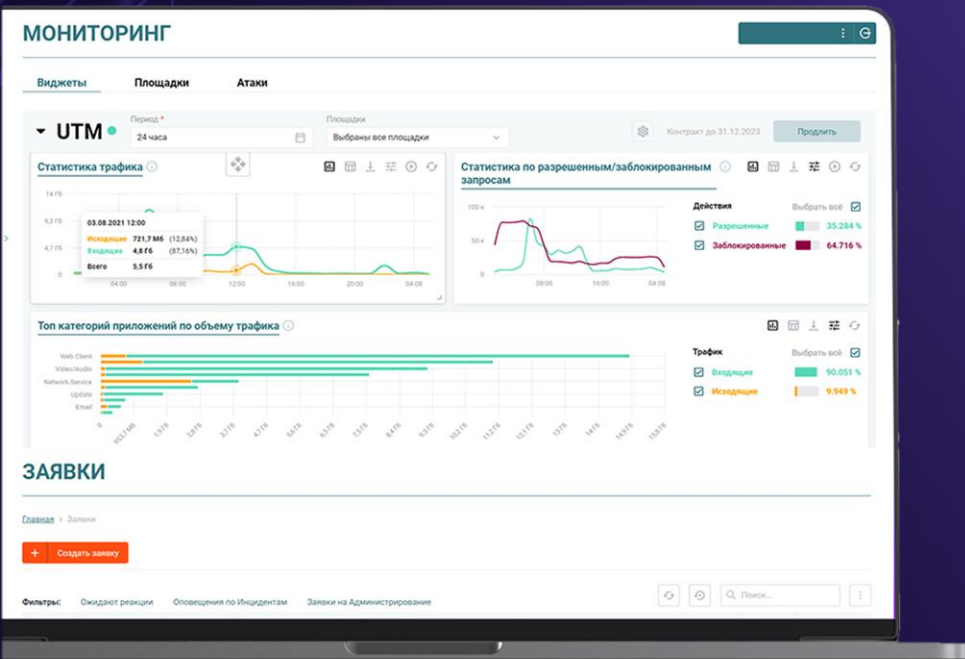
Защита от DDoS-атак (Anti-DDoS)



Регистрация и анализ событий ИБ (ERA)



Больше чем просто сервисы



Сервисы Solar MSS объединены в экосистему на трех уровнях:

| технологический

обмен информацией между сервисами и создание общих политик безопасности;

| пользовательский

единая точка взаимодействия с клиентом и визуализации работы;

| аналитический

оценка эффективности решения комплексных задач.

В рамках данного подхода мы полностью отвечаем за безопасность компании, позволяя клиентам сфокусироваться на основной деятельности.

Экспертная база Solar MSS

Выделенный опорный центр

В качестве ключевого офиса региональной экспертизы Solar MSS создан опорный центр в Самаре (более 50 специалистов, которые работают в круглосуточном режиме). Это помогает учитывать специфику регионального бизнеса, регуляторов и реализации атак.

Повышение экспертизы

Компания ежегодно проводит стажировки более 200 человек по всей России, организует CTF (Capture the flag или Захват флага) и хакатоны. Это позволяет повысить уровень экспертизы и защищенности регионов.

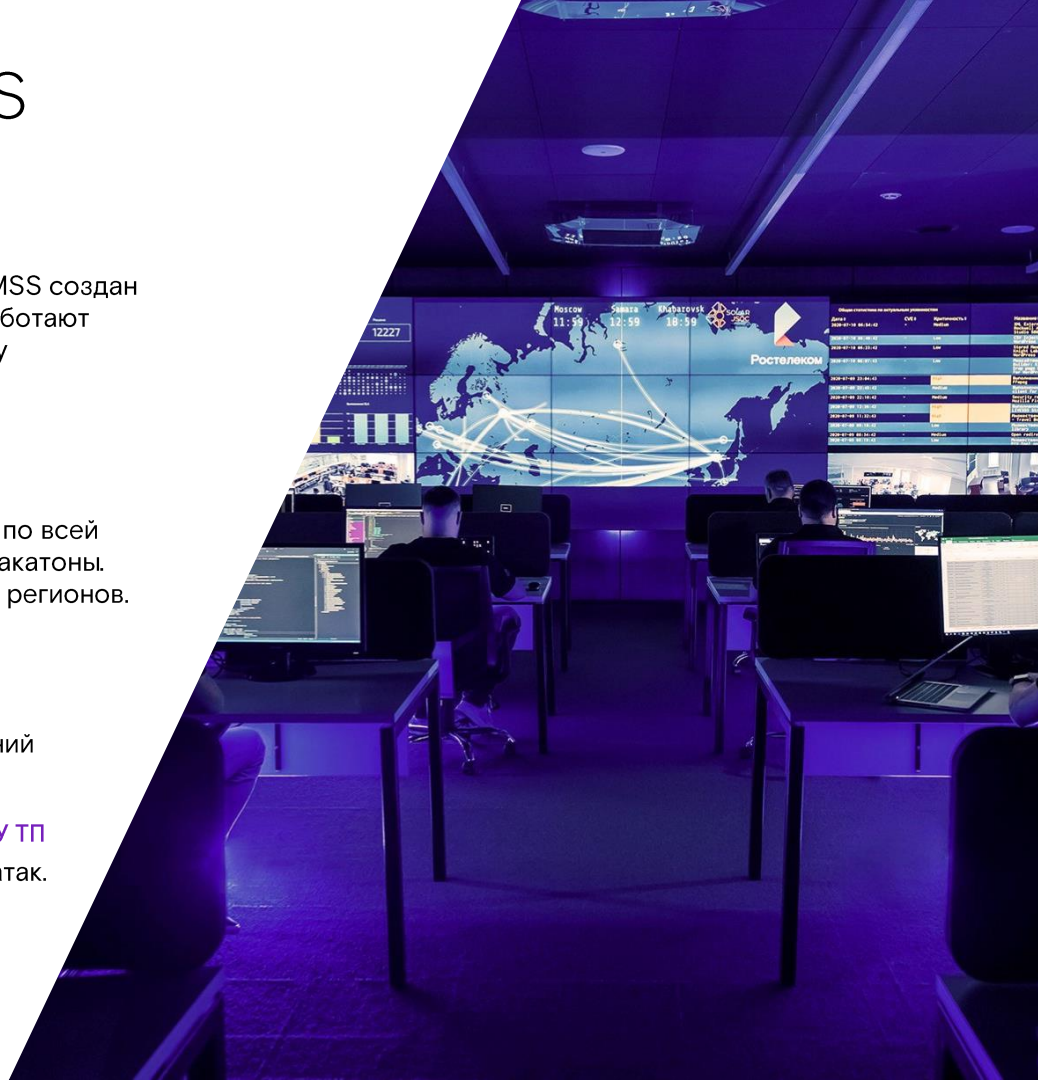
Обогащение информацией

Solar MSS взаимодействует с целым рядом продуктов и решений компании:

| Solar JSOC | Национальный киберполигон | Лаборатория АСУ ТП

Это позволяет своевременно реагировать на новые векторы атак.

Ростелеком
Солар



Решения Solar MSS



ЗАЩИТА ОТ ФИШИНГА И ШИФРОВАЛЬЩИКОВ

Безопасность компании в эпоху
интернет-мошенничества



ЗАЩИТА ОНЛАЙНА

Бесперебойная доступность
онлайн-ресурсов компании



ЕДИНАЯ СЕРВИСНАЯ МОДЕЛЬ ДЛЯ РОИВ

Обеспечение кибербезопасности
всего региона



Больше решений
в ближайшем будущем

Обеспечиваем кибербезопасность по подписке

Просто

Оперативность

от 2 дней нужно для подключения сервисов и решений

70%

сервисов и решений экосистемы подключаются без вмешательства в инфраструктуру

Прозрачность

удобное управление и визуализация работы сервисов в личном кабинете

Выгодно

Гибкость

большое количество тарифов для разных потребностей клиентов

40%

средняя экономия на горизонте 5 лет в сравнении с классической моделью закупки и внедрения технологий

Комплексность

решение задач клиентов вместо обычного предоставления средств защиты в аренду

Надежно

Ответственность

финансовая ответственность в рамках договорных обязательств

99,5%

стандартный гарантированный уровень оказания сервисов (Service Level Agreement, SLA)

Отказоустойчивость

12 500 стоек в современных ЦОД класса Tier III

Контакты

Центральный офис

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

Запросите бесплатную
консультацию эксперта

solar@rt-solar.ru

