



ПРОДУКТОВЫЙ ПОРТФЕЛЬ SOLAR

Продукты

Сервисы

Услуги

Узнайте больше о решениях «Солар»

Продукты

[Перейти](#)

Сервисы

[Перейти](#)

Услуги

[Перейти](#)

Обновленный личный кабинет

[Посмотреть](#)

Портфель решений «Солар»

 Для быстрого перехода к нужному разделу нажмите на его название

ПРОДУКТЫ

AI безопасность доступа, сети и данных	<u>Solar Dozor</u> (Высокопроизводительная DLP-система корпоративного класса)	Безопасная разработка	<u>Solar appScreener</u> (SAST, DAST, SCA, SCS)
	<u>Solar webProxy</u> (SWG) (Решение для управления доступом к сайтам и веб-приложениям, мониторинга действий сотрудников в сети и защиты трафика)		<u>Hexway ASOC</u> (Единая ASOC/ASPM-платформа для безопасной разработки)
	<u>Solar AI Firewall</u> (Шлюз безопасности класса LLM Firewall для работы с внешними и внутренними ИИ-моделями)	Автоматизация мониторинга и реагирования	<u>Luntry (Container Security)</u> (Решение для комплексной защиты контейнерных приложений и средств оркестрации на базе Kubernetes)
	<u>Solar inRights</u> (IdM/IGA) (Система для управления учетными записями и расследования инцидентов ИБ, связанных с правами доступа)		<u>Solar SIEM</u> (Автоматизация мониторинга, обнаружения и реагирования на инциденты)
	<u>Solar inRights Origin</u> Готовое IdM/IGA-решение		<u>Solar DNS RADAR</u> (Защита от атак, использующих протокол DNS)
	<u>Solar SafeInspect</u> (Платформа для эффективного управления привилегированными учетными записями и сессиями)	Защита инфраструктуры	<u>Solar LightHouse</u> (Платформа для комплексного управления безопасностью инфраструктуры)
	<u>Застава</u> (АПК защиты корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей)		

СЕРВИСЫ

Solar JSOC		Solar MSS	
Сервисы мониторинга и реагирования	<u>Выявление и реагирование на инциденты</u> (SOC)	Защита онлайн	<u>Защита веб-приложений</u> (WAF) <u>Защита от бот-трафика</u> (Antibot) <u>Мониторинг трафика и защита от DDoS-атак</u> (Anti-DDoS) <u>Защищенный доступ к веб-ресурсам</u> (ГОСТ TLS)
Сервисы предупреждения атак	<u>Solar AURA</u> (Мониторинг внешних цифровых угроз) <u>Контроль уязвимостей</u> (VM) <u>Solar TI Feeds</u> (Поток данных об актуальных угрозах) <u>Solar Security Awareness</u> (Повышение киберграмотности сотрудников)	Сетевая безопасность	<u>Шифрование каналов связи</u> (ГОСТ VPN) <u>Защита от сетевых угроз</u> (UTM)
Экспертные услуги			
Услуги форензики	<u>Расследование и реагирование на инциденты</u> (DFIR) <u>Выявление следов компрометации</u> (Compromise Assessment) <u>Подписка на реагирование на инциденты</u> (Retainer)		
Услуги оценки защищенности	<u>Тестирование на проникновение</u> (Пентест) <u>Анализ защищенности приложений</u>		

УСЛУГИ

Услуги консалтинга	<u>Управленческий консалтинг</u> <u>Построение и консалтинг SOC</u>
--------------------	---

Продукты



DLP-система Solar Dozor

- Контроль рабочего времени
- Защита информации от утечек в корпоративных каналах коммуникации и ИИ-сервисах
- Профилактика и расследование инцидентов безопасности



DLP-система Solar Dozor

DLP-система корпоративного класса для предотвращения утечек данных, корпоративного мошенничества, профилактики и расследования инцидентов.

[Подробнее на сайте](#)

Вызовы бизнеса

- Штрафы и санкции за несоблюдение требований по защите данных
- Снижение уровня доверия клиентов и финансовые потери из-за утечек данных
- Убытки от мошеннических атак и экономических инцидентов
- Снижение эффективности работы служб безопасности из-за перегрузки рутинными операциями и отсутствия автоматизации

Решение

- Обеспечение соответствия нормативным требованиям за счет гибких настроек политик безопасности
- Блокировка утечек в режиме реального времени во всех каналах перехвата
- Выявление и расследование инцидентов информационной, экономической и внутренней безопасности
- Автоматизация процессов защиты данных и расследования инцидентов

Зрелое решение

25+ лет

Solar Dozor защищает данные и формирует тренды в ИБ

Мировой уровень

480+ тыс.

агентов — самое масштабное внедрение в Европе, подтвердившее высокую производительность Solar Dozor

Лидер рынка

Входит в топ-3

вендоров DLP-систем России и стабильно удерживает лидерскую позицию

Доказанный опыт

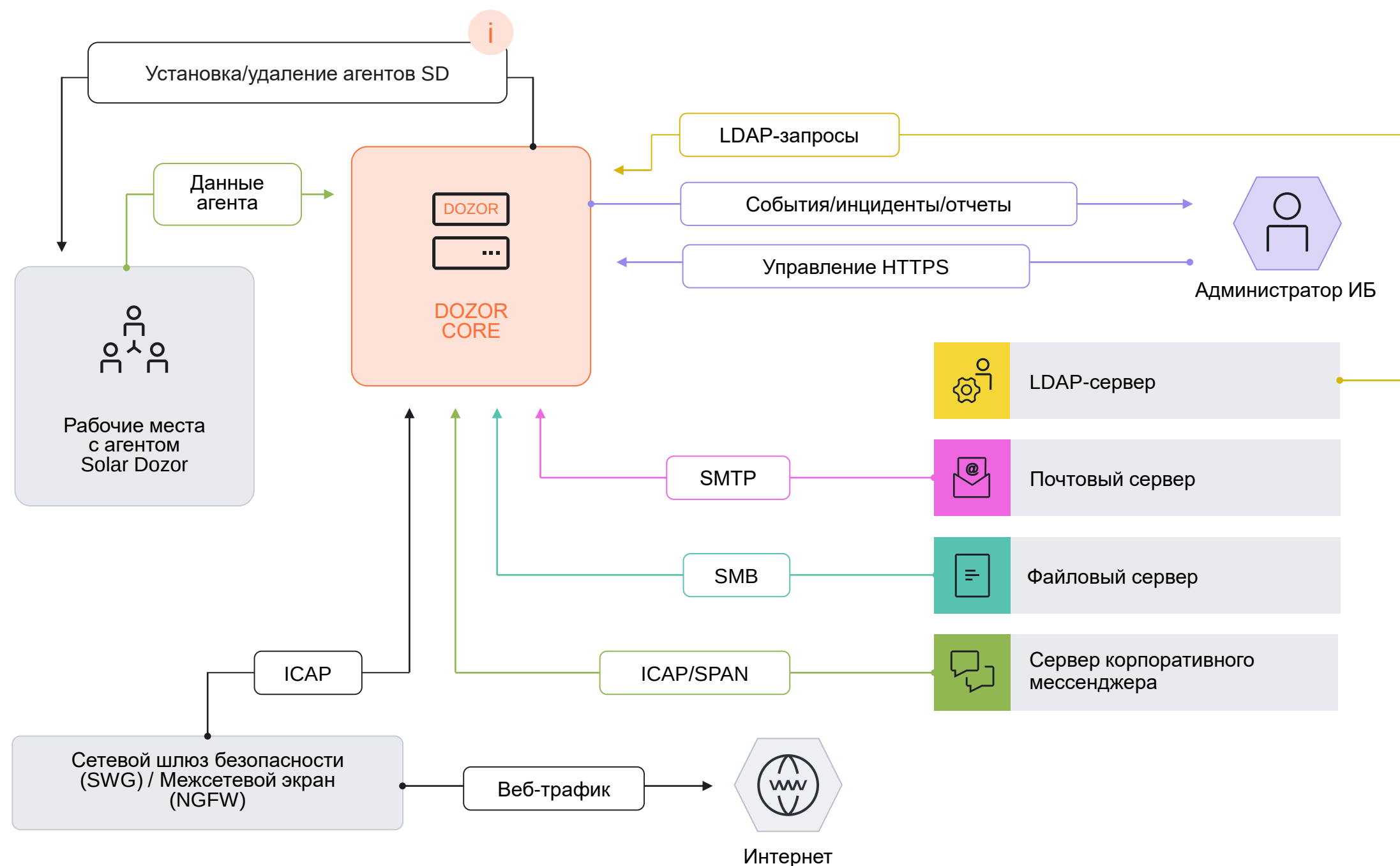
200+ внедрений

в коммерческие и государственные организации

Нам доверяют

[Больше историй внедрения на сайте](#)

Особенности решения



ТОПовые фичи

- Уникальные модули: MultiDozor – управление геораспределенными структурами, Detective – проведение расследований
- Полнофункциональный агент для Linux
- Сертификат ФСТЭК России № 4459 по 4-му уровню доверия, сертификат Минобороны № 7412



Как попробовать решение

- Онлайн-демонстрация
- Обучение
- Демостенд

Лицензирование

Solar Dozor имеет модульную структуру, позволяющую внедрять только необходимую функциональность, с возможностью апгрейда и масштабирования

Базовый модуль системы

Dozor Core

Модули-перехватчики

Dozor Mail Connector
Dozor Endpoint Agent
Dozor File Crawler
Dozor Traffic Analyzer

Модули-расширения

Dozor Dossier
Dozor UBA
Dozor Detective
Dozor Long-term Archive
Dozor OCR
MultiDozor
MultiConnector
DCAP

Метрики лицензирования

- **Базовая:** по количеству адресов электронной почты / учетных записей

Варианты лицензирования

- По подписке на 1 или 2 календарных года
- Бессрочные лицензии + ежегодная подписка на обновления

Свяжитесь с вашим менеджером «Солара» или оставьте заявку по QR-коду

Запросить консультацию



SWG-система Solar webProxy

- Защита веб-трафика от угроз и нежелательного контента
- Контроль доступа сотрудников к веб-ресурсам
- Защита информации от утечек через веб



SWG-система Solar webProxy

Зрелая standalone SWG-система для гибкого управления доступом сотрудников к веб-ресурсам, проактивной защиты от веб-угроз и предотвращения утечек конфиденциальной информации через веб-каналы — с учётом передовых мировых практик и глубокой российской экспертизы.

[Подробнее на сайте](#)

Риски бизнеса

- Нет прозрачного контроля, как сотрудники используют интернет, облачные и GenAI-сервисы в рабочих процессах
- Растут риски утечек данных через веб-каналы: облака, файлообменники, мессенджеры, AI-инструменты
- Фишинг, вредоносные сайты и опасные загрузки скрываются в HTTPS-трафике и проходят незаметно
- Новые вредоносные домены и веб-угрозы меняются быстро — реакция средств защиты запаздывает
- HTTPS/SSL-инспекция на NGFW увеличивает нагрузку и может приводить к дорогому масштабированию периметра
- Расследования затягиваются из-за неполной хронологии веб-действий пользователей
- В филиалах и дочерних структурах возникают расхождения в политиках веб-доступа, что повышает риск инцидентов и усложняет контроль

Решение

- Контроль корпоративного доступа к интернету и GenAI-сервисам по политикам безопасности
- Снижение риска утечек через веб-каналы, включая облачные и GenAI-сервисы
- Защита от фишинга и вредоносного контента, в том числе в HTTPS-трафике
- Оперативная реакция на новые веб-угрозы за счёт ежедневной актуализации категоризации и TI-фидов
- Разгрузка NGFW и оптимизация CAPEX за счёт выноса HTTPS-инспекции в специализированный SWG
- Ускорение расследований и повышение прозрачности за счёт детализированной картины веб-активности (досье, журналы, отчёты)
- Централизованное управление политиками в распределённой инфраструктуре и филиальной сети

7 лет

экспертизы в защите корпоративного веб-трафика с учётом российской специфики

2 млн

пользователей — самое крупное внедрение SWG в России и Европе

1-я SWG

В России с контролем ИИ: фильтрация запросов/ ответов, загрузок и выгрузок файлов

Продукт в реестре отечественного ПО (№ 5984 от 19.11.19), сертифицирован ФСТЭК России (МЭ Б4 для «комплекс межсетевой экран solar»)

Нам доверяют



АБСОЛЮТ БАНК

И еще 150+ внедрений
в крупнейших коммерческих
и государственных организациях

[Кейсы использования на сайте](#)

Как получить доступ к системе

Конфигурации Solar webProxy

Категоризатор +
фиды угроз

Модуль Webcat

Антивирусная
защита

Модуль Antivirus

Обратный
прокси

Модуль Reverse

Агент конечной
станции

**Модуль
Endpoint agent**

Основные функции Solar webProxy

webProxy Core

HTTP(S)-прокси

Базовый (L3–L4) межсетевой экран

SSL-инспекция

SOCKS-прокси

Контроль ИИ

Маршрутизация исходящих соединений на разные IP

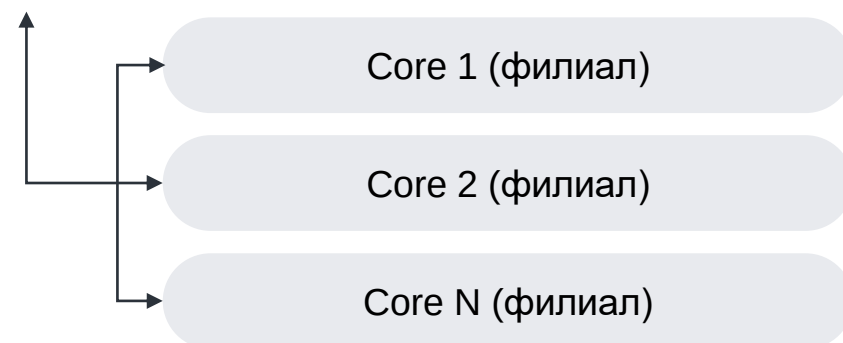
Досье

API

DPI

Централизованное управление политиками
фильтрации для независимых инсталляций

Модуль multiProxy



Модель внедрения и лицензирования

Условия внедрения Solar webProxy

Solar webProxy имеет модульную архитектуру, что позволяет внедрять только необходимую функциональность, а затем масштабировать и расширять решение по мере роста задач. Это поддерживает предсказуемую модель инвестиций в безопасность.

Метрики лицензирования

Все модули (кроме MultiProxy) лицензируются по числу уникальных пользователей (пользователи и IP рабочих станций, с которых осуществляется доступ в интернет)

MultiProxy лицензируется по количеству инсталляций с Core-лицензией

- Подписка: 1 / 2 / 3 года
- Обновления ПО включены
- Минимальное количество лицензий — 100 (возможны индивидуальные условия)

Как получить доступ к решению

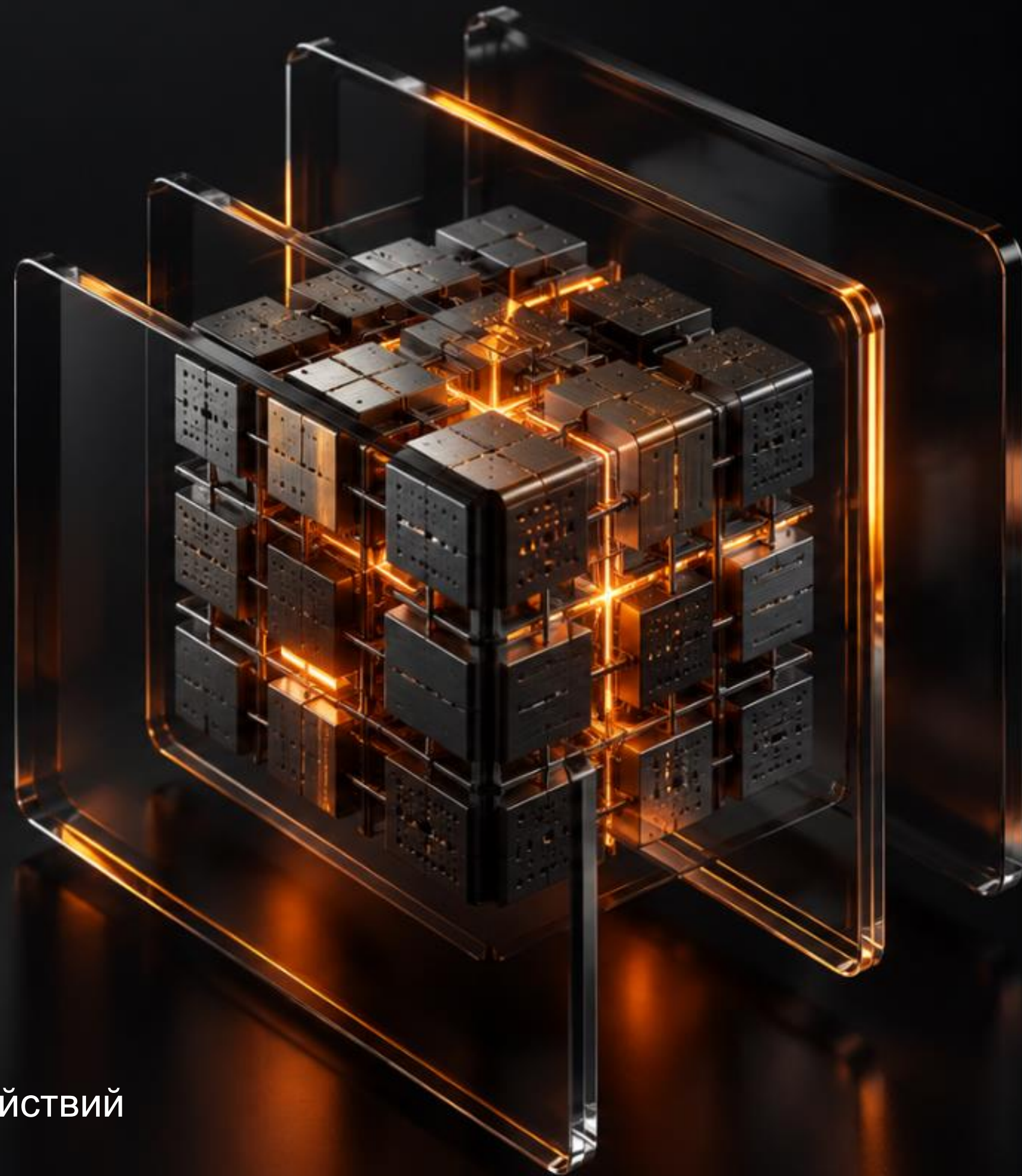
- Запросить консультацию
- Обсудить архитектурный сценарий (в т.ч. разгрузка NGFW / контроль AI)
- Подобрать конфигурацию под инфраструктуру и задачи
- Запросить демо / пилот



PRE-LAUNCH · продукт в разработке

Solar AI Firewall

Единый шлюз для двустороннего контроля ИИ-взаимодействий
Защита данных, корпоративных ИИ-сервисов и агентов
Управление доступом, потреблением и рисками ИИ



Solar AI Firewall

Специализированная система для контроля взаимодействий с внешними LLM и защиты корпоративных ИИ-сервисов и агентов от атак и утечек данных. Проверяет запросы, контекст и ответы до их передачи адресату. Объединяет политики безопасности, управление доступом и квотами, аудит и расследование инцидентов.

Вызовы бизнеса

Утечка ПДн и секретов во внешние LLM вместе с запросами и файлами.

Вредоносные инструкции в ответах внешних моделей.

Попытки изменить поведение корпоративного ИИ через запросы, документы и подключённые сервисы.

Незапланированные расходы на ИИ и перегрузка сервисов из-за бесконтрольных обращений.

Нет доказательной базы для расследования инцидентов с ИИ.

Решение

Проверка запросов и вложений: блокировка, маскирование или удаление данных.

Проверка ответов до выдачи сотруднику или приложению.

Выявление попыток обойти защиту и навязать ИИ опасные действия. Проверка ответов на ПДн и секреты.

Квоты бюджета, токенов, запросов и параллельных обращений для внешних и внутренних LLM.

Неизменяемый журнал: кто, к какой модели, что выявлено и почему принято решение.

Результаты внутренних испытаний*

94,6%

выявленных атак

6 247 из 6 605 атак на регрессионном наборе.

0,9%

ложных срабатываний

24 из 2 697 допустимых запросов.

Защита от скрытых инструкций

Находит опасные команды в запросах и документах — даже замаскированные или разбитые на несколько сообщений.

Проверка качества перед обновлением

Перед обновлением проверяем выявление атак, ошибочные блокировки и скорость. При ухудшении показателей обновление не выпускается.

*Источник: «Solar AI Firewall. Обзор решения», прогон 18.09.2026: 129 корпусов; допустимые запросы — тот же прогон. Внутренние регрессионные испытания. Результаты зависят от данных и настроек; качество в инфраструктуре заказчика проверяется на пилоте.

Как работает решение и его преимущества

Как работает Solar AI Firewall

Схема работы в разрыв трафика. Проверяются взаимодействия, проходящие через Solar AI Firewall.

Администратор задаёт политики, действия и квоты



Журнал и аналитика

Кто и к какой модели обращался; правило, фрагмент, действие и расход. Карточка расследования и передача событий в SIEM/SOAR.

Проверка содержимого не заменяет разграничение доступа к корпоративным источникам.

Ключевые преимущества

Защита ИИ, созданная профессионалами кибербезопасности

Опыт защиты крупнейших организаций и ресурсы «Солар»: единая команда разработки, внедрения и поддержки — от подключения до развития защиты.

Единый контроль ИИ-взаимодействий и расходов компании

Общие правила для запросов и ответов внешних и внутренних LLM. Учёт потребления и квоты по сотрудникам, подразделениям и моделям — для контроля бюджета и нагрузки.

Российские персональные данные и секреты под контролем

Паспорт, ИНН, СНИЛС и секреты доступа распознаются до передачи. Маскирование и обратимая подстановка сохраняют допустимую работу с ИИ.

Лаборатория атак для противодействия новым угрозам ИИ

До применения изменений ИБ может проверить выявление угроз, ошибочные блокировки и задержку на тестовых запросах. Лаборатория атак помогает оценить результат обновления и выбрать проверенную версию защиты.

Гибкое управление защитой ИИ и детальный разбор инцидентов

ИБ видит источник нарушения и причину блокировки: может разобрать инцидент, проверить жалобу сотрудника и обоснованно изменить правило.

Синергия экосистемы «Солар» для блокировки Shadow AI и анализа угроз

В связке с webProху и Dozor — контроль доступа к ИИ, конфиденциальности данных, запросов и ответов. Интеграции согласуются под инфраструктуру компании.

Как попробовать решение

Онлайн-демонстрация

Покажем контроль запросов и ответов, настройку политик, квот и разбор инцидентов.

Пилот на стенде Solar

Проверим атаки и рабочие запросы на согласованных тестовых наборах.

Пилот в компании

Подключим выбранный маршрут к LLM. Оценим детекцию, ложные срабатывания, задержку и работу квот.

IDM / IGA-система Solar inRights



Централизованное управление
доступом сотрудников

IdM/IGA-система Solar inRights

Solar inRights — IdM/IGA-решение для централизованного управления учётными записями и доступом с гибкой адаптацией без потери интеграций и бизнес-логики.

[Подробнее на сайте](#)

Вызовы бизнеса

- Долгое предоставление доступов замедляет бизнес-процессы
- Финансовые потери из-за инцидентов с несанкционированными правами доступа
- Бизнес-владельцы информационных ресурсов не знают, у кого кто есть доступ к информации в рамках их зоны ответственности
- Увеличение нагрузки на ИТ-отдел из-за отсутствия автоматизации процессов УД на основе кадровых событий

Решение

- IdM-система автоматически управляет правами доступа сотрудников на основе регламентов и ролевой модели, предотвращает инциденты и оперативно сообщает о несанкционированном доступе в службу ИБ
- Исключение ошибок и человеческого фактора при назначении прав
- Полная картина прав доступа сотрудников к информационным системам
- Непрерывность бизнеса: исполнение SLA и поддержка организационных изменений

150+

специалистов в центре экспертизы по консалтингу и внедрению

ГОСТ

на IdM, выступили инициаторами и соавторами стандарта

>15 лет

опыта реализации проектов разной сложности

200+ тыс.

максимальное количество подключенных пользователей в одном проекте

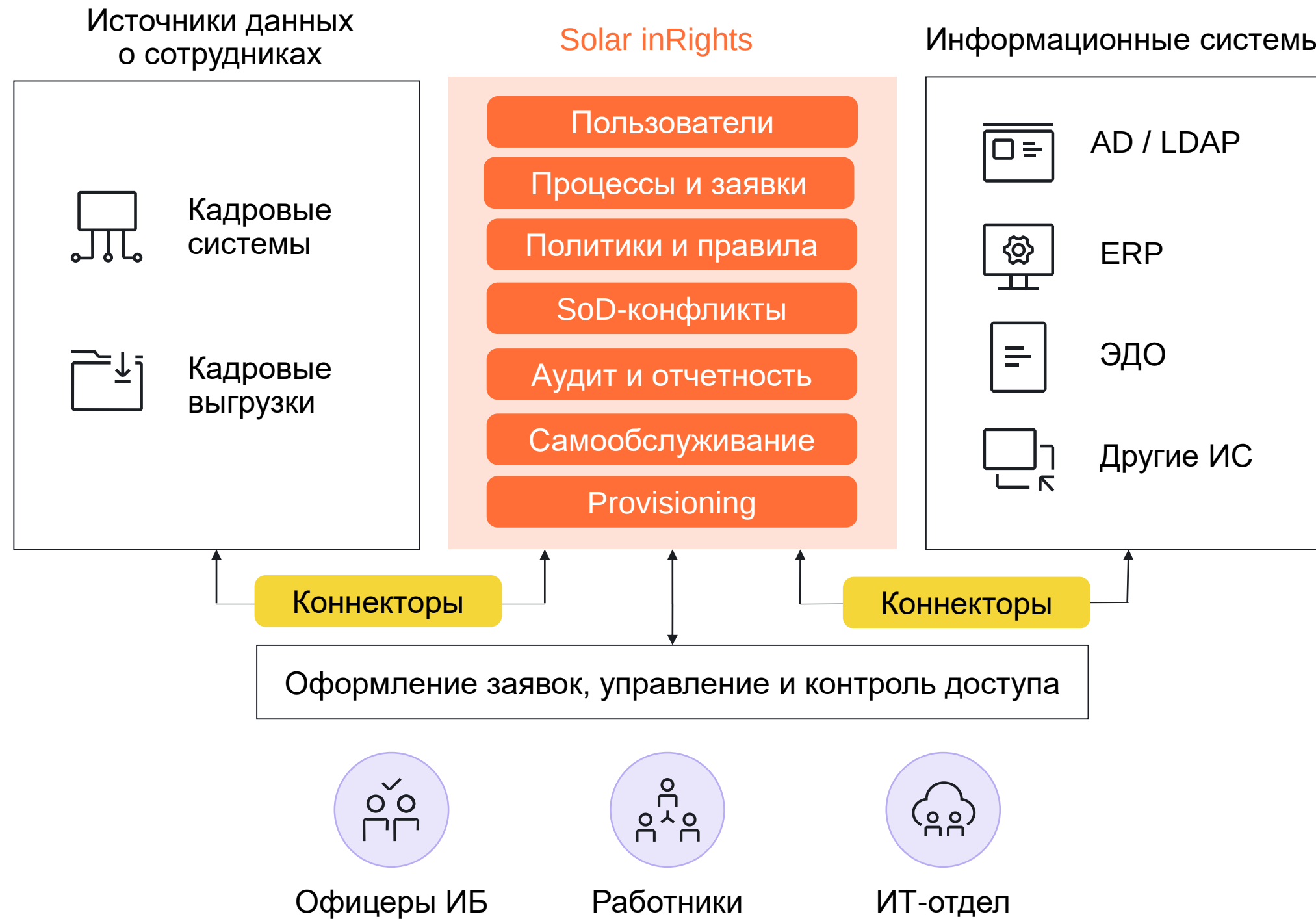
Нам доверяют



Соответствие законам РФ

В реестре отечественного ПО (запись 7759),
сертификат ФСТЭК (№ 4633 от 27.12.2022)

Особенности решения



ТОПовые фичи

- Интеграция с DRP-системами
- Управление доступом ИИ-агентов;
- Обновление ядра без потери кастомизаций, интеграций и бизнес-логики.
- Гибкий программный комплекс для решения любых задач по исполнению политик и регламентов управления доступом
- Кастомизация процессов и интеграций под нужды организации
- Использование процесса безопасной разработки и анализа кода для минимизации уязвимостей и инцидентов



Как попробовать решение

- Онлайн-демонстрация в формате ВКС
- Пилотный проект
- Технические вебинары

Лицензирование

Solar inRights лицензируется в виде программного комплекса с возможностью активации / деактивации функциональных подсистем.

Метрика лицензирования

количество лиц, правами доступа
которых требуется управлять



Варианты лицензирования

1. Срочная лицензия
 - по подписке на 1 год
 - по подписке на 1 месяц
2. Бессрочная лицензия



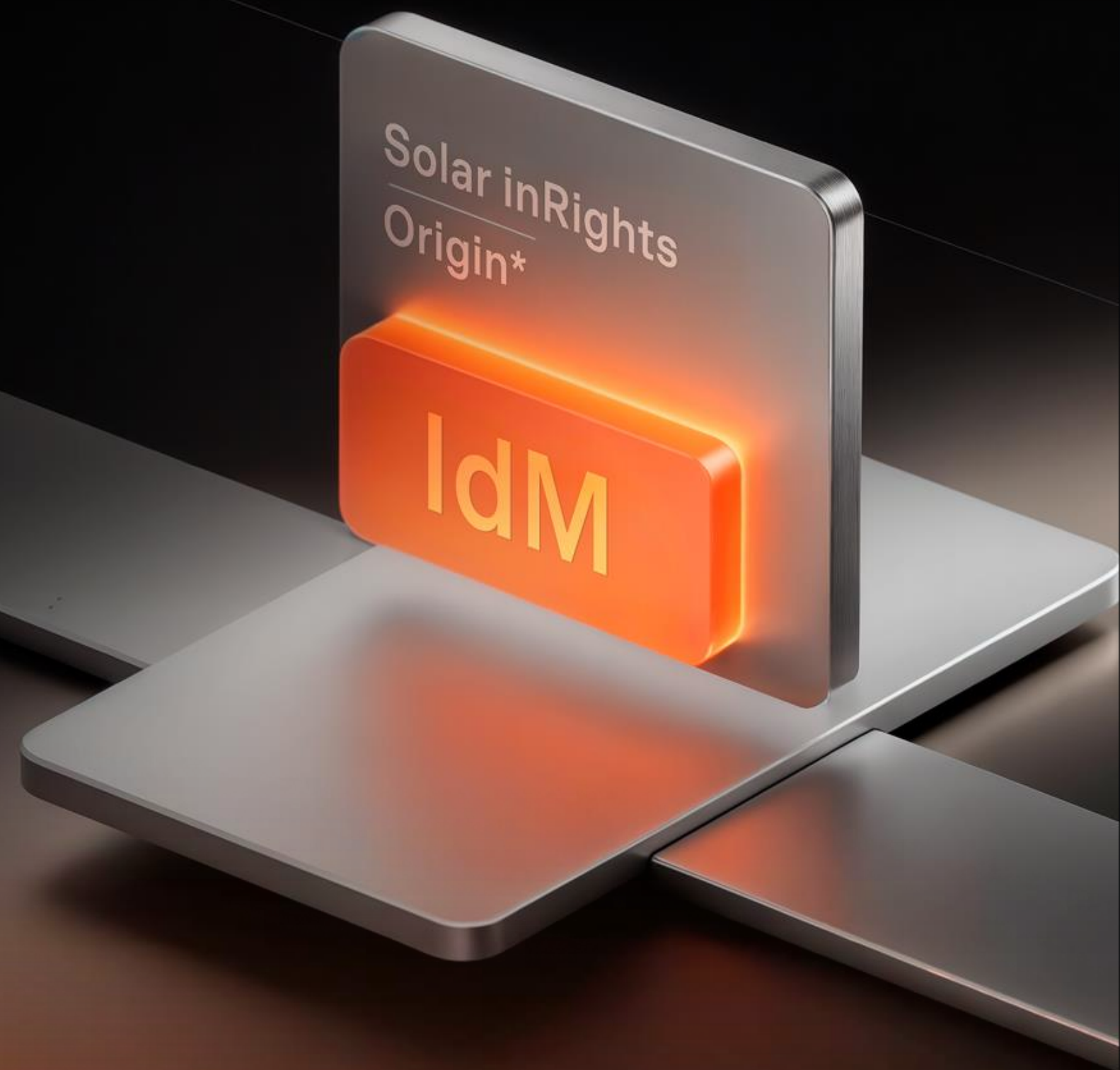
**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Готовое IdM/IGA-решение Solar inRights Origin

Централизованное управление
доступом сотрудников



Коробочное IdM-решение Solar inRights Origin

Готовое IdM/IGA-решение для компаний, начинающих системно выстраивать управление доступом, с 20+ преднастроенными сценариями и без необходимости долгого проектирования/глубокой кастомизации.

[Подробнее на сайте](#)

Вызовы бизнеса

- Слишком долгий процесс классического внедрения IdM-решений - в среднем 2-3 года
- Высокая стоимость IdM-продуктов на рынке - от 40 млн рублей
- Высокий порог входа в IdM-продукт, зависимость от вендора в администрировании и развитии системы
- Самописные скрипты частично закрывают задачу «автоматизации», но не закрывают проблему контроля доступов

Решение

- Сокращенный срок внедрения и введения эксплуатацию, который занимает от 3 до 6 месяцев
- За фиксированную цену - полнофункциональное IdM-решение
- Возможность самостоятельного внедрения по разработанной методологии без участия вендора
- Своевременное обновление прав доступа и снижение риска ошибок и инцидентов ИБ за счет автоматической обработки кадровых событий

20+

преднастроенных процессов (приём, увольнение, отпуск, права, ОШС, ИБ-события)

от 300 УЗ

минимальное количество для подключения

24/7

доступ к Нейропомощнику и базе знаний для поддержки

Соответствие законам РФ

в реестре отечественного ПО (запись 7759), сертификат ФСТЭК (№ 4633 от 27.12.2022)

Повышение эффективности с первых недель эксплуатации

~50%

экономия времени сотрудников благодаря автоматизации процессов УД

до 80%

снижение нагрузки на ИТ-отдел в части управления доступом

на 360°

видимость предоставления, изменения и удаления полномочий пользователей

до 10 минут

сокращение времени предоставления доступа к основным системам

Особенности решения



ТОПовые фичи

- Быстрое внедрение 1 инженером от заказчика по пошаговой инструкции (от 3 до 6 месяцев)
- Готовая конфигурация: базовые роли, процессы, отчеты
- Набор коннекторов к целевым системам (1C, MS Active Directory и ALD Pro, MS Exchange и CommuniGate)
- Доступ к базе знаний и Нейропомощнику
- Обучающие курсы для инженеров + лабораторный стенд для развития компетенций



Как попробовать решение

- Онлайн-демонстрация в формате ВКС
- Бесплатный пилот
- Экспертный вебинар по запросу

Лицензирование

Solar inRights Origin лицензируется в виде программного комплекса с типовым набором коннекторов

Метрика лицензирования

количество лиц, правами доступа
которых требуется управлять



Варианты лицензирования

1. Срочная лицензия
 - по подписке на 1 год для 1 000 пользователей
2. Бессрочная лицензия
 - на 2 000 УЗ (с возможностью продления по 1 000 УЗ)



**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



РАМ-система Solar SafeInspect

Управление привилегированным доступом



Solar SafeInspect

Полнофункциональная PAM-платформа. Контролирует доступ привилегированных пользователей, проактивно применяет политики безопасности и записывает все действия в сессии

[Подробнее на сайте](#)

Вызовы бизнеса

- У компании большое количество подрядчиков и удаленных администраторов, которых нужно контролировать
- Необходимо контролировать действия внешних и внутренних привилегированных пользователей с доступом к ИС
- Снижение рисков утечек данных и атак на системы безопасности и мониторинга, изменений инфраструктуры АСУ ТП и Legасу-систем.
- Необходимо быстро расследовать инциденты с повышением привилегий и находить источник превышения полномочий и повреждения инфраструктуры

Решение

- Гибкая и оперативная организация привилегированного доступа под любые задачи
- Эффективное и безопасное хранение записанных данных: данные размечаются по времени, базы защищены шифрованием, периоды бездействия не записываются, записи компактны
- Мониторинг работы в реальном времени с возможностью прерывания сессии, гибкие возможности анализа и составления отчетов
- Запись всех привилегированных сессий с возможностью просмотра видео для быстрого расследований инцидентов и восстановления инфраструктуры

Ключевые факты

Гибкость

Работа без использования агентов и минимальное вторжение в инфраструктуру, интеграция в трех режимах L2, L3 (незаметны для пользователя) и L7 (предполагает явную авторизацию)

Скорость

Быстрое развертывание (инсталляция занимает не более 20 минут, развертывание с настройками для полноценной работы – менее 2 часов)

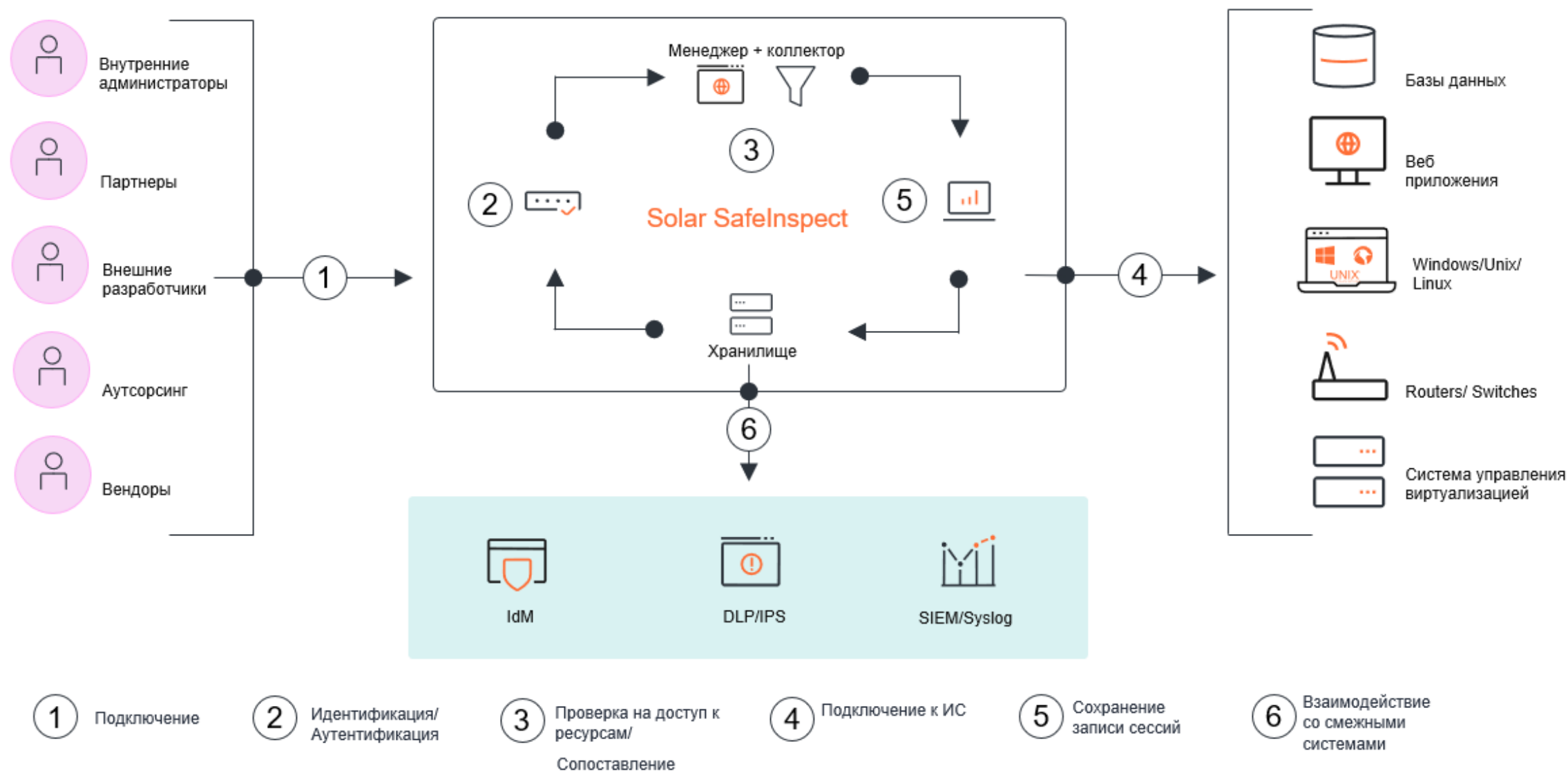
Безопасность

Данные под защитой шифрования. Сведения, записанные системой, компактно упакованы для хранения. Периоды простоя не требуют дополнительного места.

Соответствие законам РФ

В реестре отечественного ПО (запись № 3341). сертификат ФСТЭК России № 4816 ОТ 30.05.2024
Соответствует приказу №117

Особенности решения



ТОПовые фичи

- Безагентская архитектура
- Глубокий контроль с посимвольной записью/OCR/блокировкой команд
- WEB-портал удалённого доступа без VPN
- Контроль доступа к целевым системам и контроль работы привилегированных пользователей в режиме реального времени
- Запись сеансов работы привилегированных пользователей
- Информации для расследований инцидентов и отчетность

Как попробовать решение

- Онлайн-демонстрация
- Пилотирование

Лицензирование

Solar SafeInspect может поставляться по бессрочной или срочной лицензии

Метрики лицензирования

Возможно бессрочное и срочное лицензирование.

1. Количество одновременных соединений
2. Количество целевых ИС (хостов)
3. Количество привилегированных пользователей



Варианты лицензирования

- Бессрочное
- Годовое
- Ежемесячное



**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



АПК «Застава»

Профессиональная защита
каналов связи и удаленного
доступа от соавторов IPsec

- Защита на базе ГОСТ и IPsec
- Стабильная работа на любых масштабах инфраструктуры
- Централизованное управление сетями с сотнями тысяч объектов



АПК «Застава» (Гост VPN)

Отказоустойчивое решение для защиты каналов связи и удаленного доступа на основе Российской криптографии и IPsec/ IKEV2

[Подробнее на сайте](#)

Риски бизнеса

- Повышение ответственности за инциденты ИБ
- Увеличение объектов связи, в том числе IoT
- Уход западных вендоров и риск потери вендорской поддержки
- Сложность гибридных рабочих мест: Вызов — создать единый защищенный периметр
- Защита подключения к централизованным
- ГИС, типа ЗАГС, ЕМИАС.
- Защита передачи телеметрической информации

Решение

- Защита конечных устройств, сетей и каналов связи от внутренних и внешних угроз
- Администрирование всей системы из одного интерфейса, масштабируемость до 10v000 узлов
- Надежный VPN-туннель для мобильных сотрудников и филиалов без риска утечек
- Прозрачная работа для пользователей и приложений без снижения скорости
- Гибкое разграничение прав доступа и возможность ограничения выхода в интернет

Зрелое решение

30 лет

АПК «Застава» защищает каналы связи и удаленный доступ

Федеральный уровень

480+ тыс.

Самая крупная инсталляция в России 45 000 пользователей (Минздрав Татарстана)

Методолог рынка

Соавтор IPsec

Набор международных протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP

Доказанный опыт

50+ тыс.

внедрений в коммерческих и государственных организациях

Нам доверяют



ФЕДЕРАЛЬНАЯ
НАЛОГОВАЯ СЛУЖБА



ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ



МИНИСТЕРСТВО
ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ ТАТАРСТАН

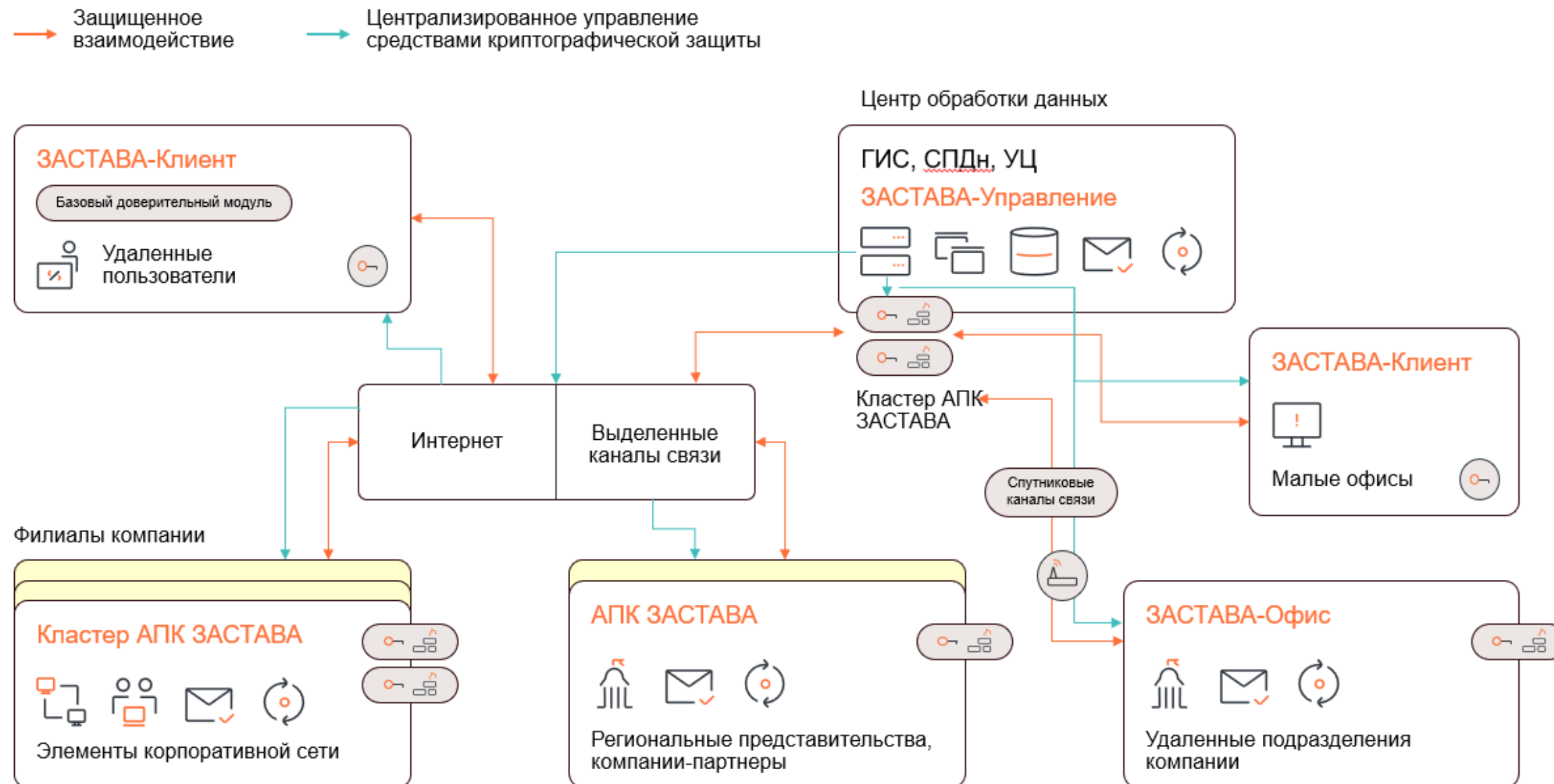


ЕМТС САНКТ
ПЕТЕРБУРГА

А также другие
госкомпании
и коммерческие
корпорации

Особенности решения

Как выглядит экосистема защищенных каналов



ТОПовые фичи

- Реализация IPsec, IKEV2
- Гибкое централизованное управление
- Возможность гибкой индивидуальной настройки и автоматической балансировки клиентов между криптошлюзами
- Возможность одновременной работы в режиме L2 И L3
- Обратная протокольная совместимость



Как попробовать решение

- Онлайн-демонстрация
- Обучение

Лицензирование

Модульная архитектура позволяет собрать нужную конфигурацию и масштабировать производительность или объем решения по мере роста бизнеса

ПО «Застава-Управление»

Приобретается по требуемому количеству центров управления. Как правило, это один или два для катастрофо-устойчивости



VPN-шлюз

Программное исполнение шлюза. Приобретается по количеству инсталляций на серверные платформы



ПО «Застава-Клиент»

Приобретается по количеству удаленных пользователей



Для заказчиков доступны два варианта лицензирования



ПАК



ПО

Свяжитесь с вашим менеджером «Солара» или оставьте заявку по QR-коду

Запросить консультацию



Solar appScreenener



Комплексное решение
для контроля безопасности ПО

Комплексное решение для контроля безопасности ПО

Solar AppScreener — лидер среди отечественных решений — по числу поддерживаемых языков программирования

[Подробнее на сайте](#)

Вызовы бизнеса

- Внедрение НДВ и вредоносного кода в состав российского ПО
- Закладки в open-source-библиотеках (к примеру, Ukrainian Malware)
- Дефицит времени. Сокращение Time-to-market для программных продуктов
- Рост числа кибератак на российские компании, в том числе, в отношении госорганов, информационных ресурсов РФ, КИИ — в следствие чего происходит ужесточение регуляtorики

Решение

- Собственная технологическая платформа Solar appScreener для комплексного анализа безопасности приложений
- Основные виды анализа в едином интерфейсе: SAST, DAST, OSA (SCA и SCS), а также ИИ-плагин к модулю SAST
- Возможность корреляции результатов нескольких видов анализа
- Контроль безопасности как собственного кода, так и сторонних компонентов

10 лет

на рынке

в 1 решении

4 вида анализа

Соответствие законам РФ.

В реестре отечественного ПО:

- SAST — запись № 7763
- DAST — запись № 19649
- SCA — запись № 20486
- SCS — запись № 22627
- Сертификат ФСТЭК России № 4825 ОТ 3.06.2024

Нам доверяют

[Больше историй внедрения на сайте](#)

Две задачи — один плагин для результатов SAST-анализа

On-premise | 7 лет обучения | Создан при поддержке мирового AppSec-производителя

TRIAGE

Интеллектуальный триаж/разметка SAST-результатов

Что делает:

Берет «сырые» результаты сканирования, автоматически разбирает каждую уязвимость по контексту и выдает чистый список только реальных угроз

Зачем это нужно:

1. **Для AppSec:** отсутствие ложных срабатываний, благодаря чему команды не тратят часы на их разбор
2. **Для разработки:** получают готовый приоритетный список благодаря Triage и сгенерированные исправления для подтвержденных уязвимостей (с помощью CodeFix)
3. **Для всех команд:** быстрее релизы — отчет готов за минуты, а не недели, выпуск вашего ПО ускоряется в разы. При этом сохраняется высокий уровень безопасности разрабатываемого ПО



Мы полностью пересмотрели подход к обработке ложных срабатываний

CODEFIX

Автоматическое исправление уязвимостей и готовый код

Что делает:

Плагин генерирует готовые, контекстные патчи кода

Зачем это нужно:

1. Качественный готовый код для исправления подтвержденных уязвимостей
2. В 10 раз увеличивается продуктивность. Внимание команды фокусируется на создании, а не на исправлении
3. Поддержка качества кода: исправления создаются по стандартам кодирования. Они сохраняют читабельность, производительность и безопасность
4. Обучение команд: каждое исправление содержит подробное объяснение того, почему и что было изменено

Виды лицензирования

Лицензирование

- По количеству пользователей (количество адресов электронной почты / учетных записей)
- По количеству параллельных потоков сканирования (количество параллельно выполняемых задач на сканирование)

Варианты

- Годовая лицензия (1 год использования Solar appScreener + пакет обновлений)
- Бессрочная лицензия (бессрочное использование Solar appScreener + пакет обновлений, далее – пакет обновлений 20% GPL ежегодно)



Как попробовать решение:

Пилот

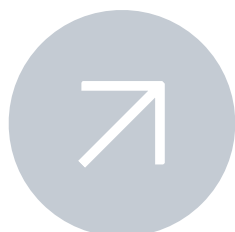
1–2 месяца (передача продукта заказчику, техническая и консультационная поддержка, встречи по результатам для сбора обратной связи)

Демостенд

1–2 недели (доступ к облачному демостенду Solar appScreener)

Вебинар

1,5 часа (живая онлайн-демонстрация продукта)



Запросить консультацию

Hexway ASOC



Единая ASOC-платформа для безопасной разработки

Hexway ASOC

Российская ASOC/ASPM-платформа для DevSecOps, которая объединяет результаты любых сканеров (SAST, DAST, SCA) и содержит встроенные инструменты для поиска уязвимостей. Она автоматически приоритизирует уязвимости и формирует управляемый процесс их исправления; это первый на рынке продукт класса ASOC/ASPM с интеграцией как публичных, так и локальных ИИ для интеллектуальных рекомендаций по исправлению кода прямо в интерфейсе.

Подробнее на сайте

Вызовы бизнеса

- Сканеры находят тысячи findings — половина из них дубли или «шум»
- MTTR по критическим уязвимостям превышает 40 дней, SLA по исправлению часто срываются
- Команда AppSec загружена на 120%, новых специалистов не найти
- Каждая команда использует свой инструмент — единой картины нет

Решение

- Для CISO и СТО: дашборды с ключевыми метриками (MTTR, TTM, ТОП риски), аналитика, отчеты для PCI DSS, ISO, ГОСТ
- Для команды ИБ: -60% шума от дублей и ложных срабатываний, false positive; на 30% выше эффективность работы с репозиториями
- Для разработчиков: четкие задачи с приоритетами на исправление, проверенные продукты для релизов

Ключевые факты

Прозрачное ценообразование

Количество репозиториев — главная метрика для формирования цены

Для всех уровней зрелости DevSecOps

Гибкость решения для настройки под свои критерии безопасности. Легко масштабируется.

Поддержка

- Собственная команда разработки
- Стандартная ТП входит в стоимость
- Возможности расширенной ТП для фиксации SLA

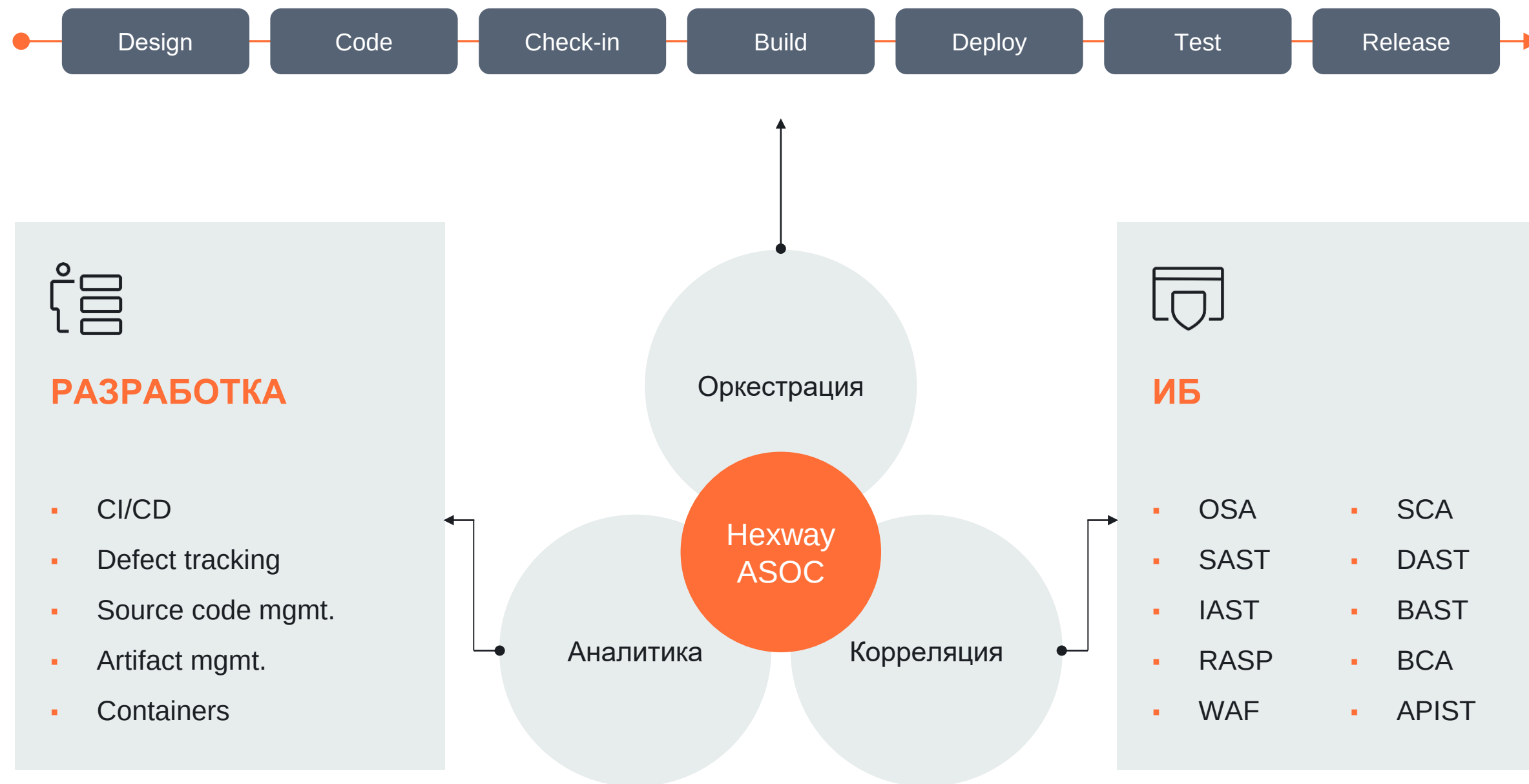
Соответствие требованиям регуляторов

В реестре отечественного ПО (запись №27364)

Соответствует требованиям в части построения процессов РБПО (ГОСТ Р 56939-2024)

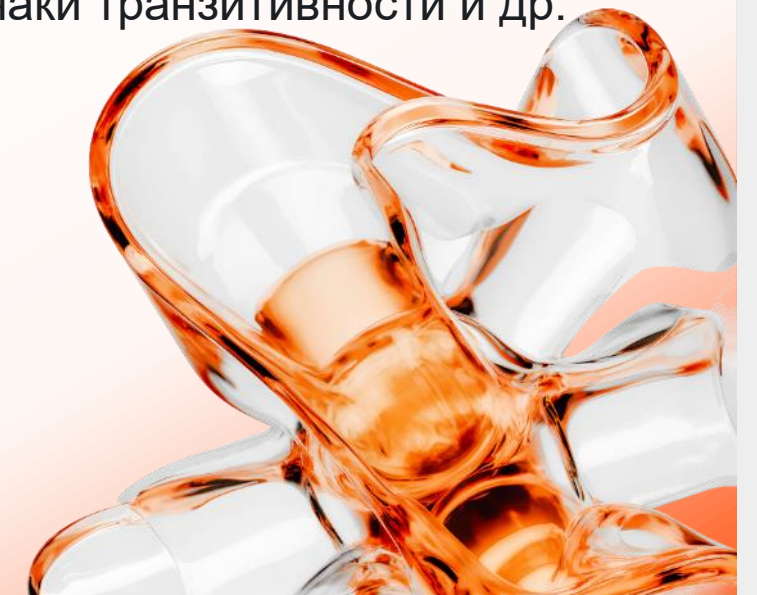
О решении

Место ASOC-платформы в DevSecOps



ТОПовые фичи

- Агрегация, дедупликация и приоритизация отчетов сканеров (коммерческих и opensource)
- Встроенные opensource сканеры SAST, DAST, SCA
- Интеграция с локальными и публичными LLM (Gigachat, DeepSeek, ChatGPT, Ollama и др.)
- Приоритизация уязвимостей по риску на основе следующих критериев уязвимостей:
 - Наличие эксплойта
 - Метрики CVSS
 - База БДУ ФСТЭК
 - Кастомная критичность
 - Признаки транзитивности и др.



Как получить доступ к решению

Лицензирование

- Enterprise лицензия
- SE-версия (бесплатно, ограниченный функционал)

Метрики лицензирования

- Количество репозиторийев

Варианты лицензирования

- Сроки лицензирования — от 12 месяцев
- Бессрочная лицензия может обсуждаться индивидуально

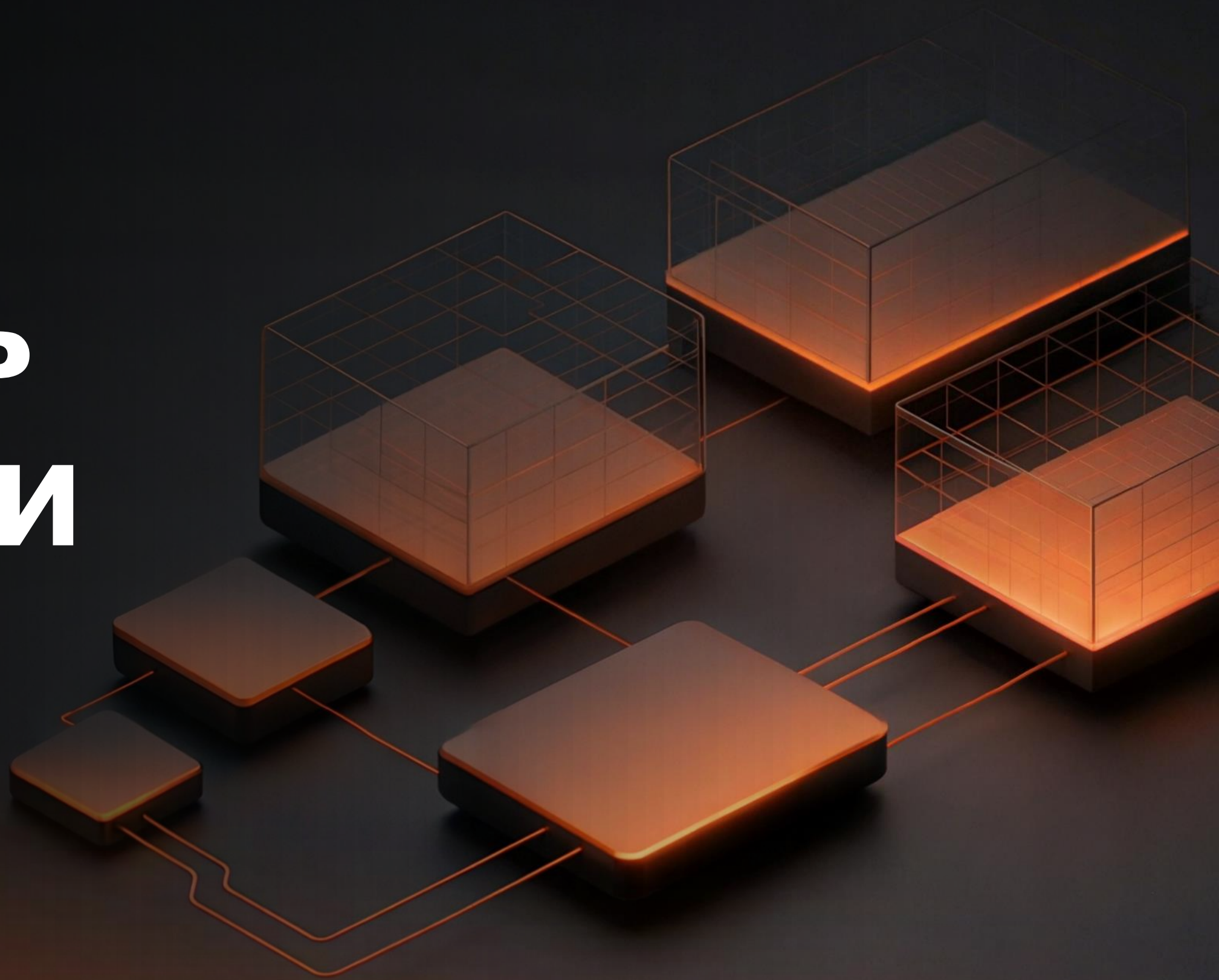
Как попробовать решение

- Онлайн-демонстрация
- Триал-версия по запросу
- Пилот
- Бесплатная Community-версия

Запросить консультацию



Luntry. Безопасность контейнеров и Kubernetes



Luntry. Безопасность контейнеров и Kubernetes

Комплексная защита контейнеров и Kubernetes на всех стадиях жизненного цикла приложения. Решение обеспечивает исключительный уровень безопасности процессов, помогает создать инфраструктуру без слепых зон и наладить бесшовную коммуникацию между командами ИТ и ИБ даже в самых крупных проектах.

[Подробнее на сайте](#)

Вызовы бизнеса

- 95% проблем, приводящих к компрометации в кластере, связаны не с CVE, а с неправильной конфигурацией
- 41% компаний назвали обеспечение безопасности главным стопором при работе с Kubernetes
- 36% компаний обладают недостатком компетенций в команде в области обеспечения безопасности Kubernetes
- 90% компаний не занимаются анализом и контролем RBAC, что приводит к компрометации всего кластера
- 100% компаний не наблюдающих за Runtime, пропускают инциденты безопасности

Решение

- C-LEVEL - снижение затрат на устранение уязвимостей и быстрый вывод продукта на рынок без компромиссов в безопасности
- СЛУЖБА ИБ - глубокая интеграция с Kubernetes для эффективного управления рисками и защиты контейнеров в реальном времени
- ИТ - автоматизированная безопасность без потери производительности, упрощенное реагирование на инциденты и удобный контроль политики
- SOC - усиление защиты и ускорение реагирования с помощью данных, позволяющих расследовать инциденты и обнаруживать первопричины сбоев

Ключевые факты

Быстрая установка

1-2 дня.
Нет предаудитов, сайзинга, проектирования, изменения инфраструктуры

Поддержка

Самая экспертная команда на рынке СНГ, собственная команда разработки и RnD и база знаний

End-to-end

Одно решение закрывающее ВСЕ аспекты / домены безопасности в контейнерных средах

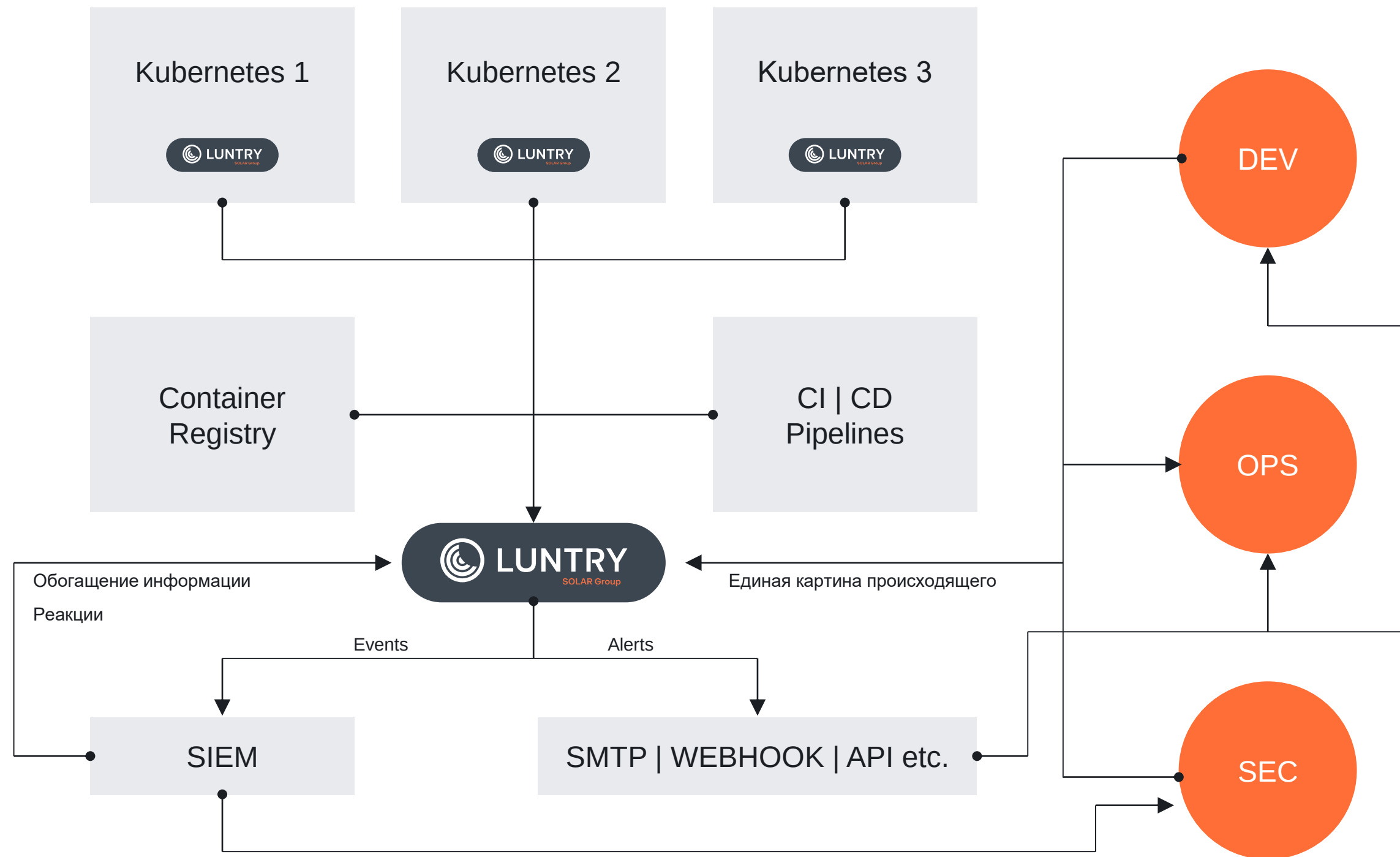
Универсальность

Ценность для ИТ и ИБ. Подходит как отдельным командам, так и для межкомандного взаимодействия

Соответствие законам РФ

В реестре отечественного ПО (запись № 15188).
Сертификат ФСТЭК России (4 квартал 2026)

Особенности решения



ТОПовые фичи

- Гибридный детект опасных действий
- Сканирование образов на всех этапах жизненного цикла
- Анализ сетевых коннектов и автоматическая генерация сетевых политик



Как попробовать решение

- Онлайн-демонстрация
- Пилот

Лицензирование

Лицензирование

1 продукт
1 вид лицензии
1 вариант поставки



Метрики лицензирования

- Количество нод



Варианты лицензирования

- Enterprise



Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду

Запросить консультацию



Solar SIEM



Программный комплекс автоматизации
ситуационного центра ИБ

Solar SIEM

Автоматизированный программный комплекс, который обеспечивает сбор и обработку событий ИБ в режиме реального времени, интеллектуальный анализ угроз и автоматизацию процессов реагирования на инциденты ИБ

Подробнее на сайте

Вызовы бизнеса

- Разрозненность решений: для полноценного реагирования требуются SIEM и SOAR
- Дефицит кадров и рост стоимости ИБ-решений
- Сокращение Time-To-Attack: автоматизация и ИИ используются не только защитниками, но и злоумышленниками
- Выполнение требований законодательства и отраслевых регуляторов в части импортозамещения (Указы Президента РФ № 250 и №166, 187-ФЗ)
- Внедрение SIEM требует значительных усилий по интеграции и настройке всех компонентов

Решение

- Объединение SIEM и SOAR в одной коробке для предоставления полного цикла защиты в одном окне и снижения совокупной стоимости владения (TCO) на 40%
- Автоматизированная аналитика и мгновенное реагирование на инциденты без перегрузки персонала
- Готовность к работе «из коробки», без недель на настройку конфигурации
- Встроенные сценарии реагирования
- AI-помощник для снижения порога вхождения специалистов первой линии

x3

скорость поиска угроз

90%

Рутины автоматизировано (плейбуки, реагирование, сбор данных)

до x16,6

Коэффициент сжатия данных при хранении

РОПО

Запись № 21682 от 07.03.2024

Ключевые преимущества

Единое облако данных

Централизованный сбор и анализ логов, событий и трафика из всех ключевых IT-систем и СЗИ

Профилирование данных

Оптимизация обращений к ретроспективным данным

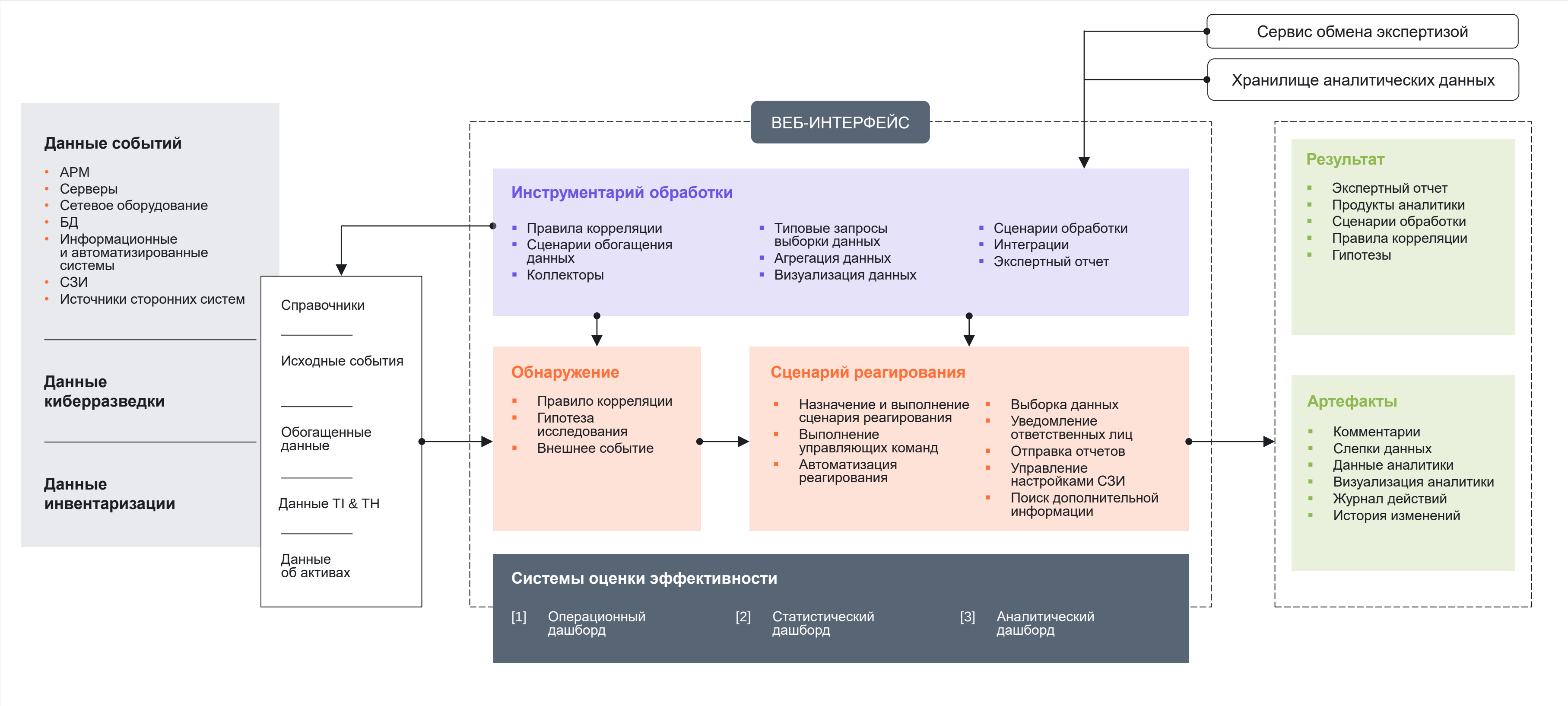
Конструктор сценариев реагирования

Гибкая настройка сценариев реагирования в UI

Автоматизированная раскатка контента

Непрерывная доставка новых правил корреляции, типов источников и парсеров

Особенности решения



Как получить доступ к решению

Лицензирование

- Количество EPS в диапазоне от 250 до 499 999
- Уровень предоставляемой поддержки (SLA):
 - «Стандарт»
 - «Премиум»
- Дополнительные возможности:
 - «Повышенная доступность»
 - «Поддержка ГосСОПКА»
 - «Поддержка ГосСОПКА. Повышенная доступность»



Комплектация

- Solar SIEM лицензируется в виде программного комплекса в составе всех подсистем



Сроки лицензирования

- 1 год / 2 года / 3 года
- Продление лицензии возможно на 1 год



Как попробовать решение

- Онлайн-демонстрация
- Подготовка к пилотному тестированию
- Пилотное тестирование

Запросить консультацию



Solar DNS RADAR

THREAT DETECTED
COORD: 45.290°N, 12.505°E
BINARY: 01100011 01111001 01100010 01100101 01110010
ATTACK ORIGIN: NODE 7A-9B

Защита от атак, использующих протокол DNS

Solar DNS RADAR

Система для выявления и блокировки вредоносной активности в DNS-трафике. Предотвращает развитие атак, в которых злоумышленник использует DNS-трафик.

[Подробнее на сайте](#)

Риски бизнеса

- Риск утечки конфиденциальных данных
- Репутационные риски и финансовые убытки по причине вредоносных воздействий на инфраструктуру
- Высокая нагрузка на специалистов ИБ из-за недостатка автоматизации процессов выявления и расследования инцидентов
- Нарушение корпоративных политик доступа в интернет

Решение

- Анализ DNS трафика с применением TI Feeds и данных ПАО «Ростелеком»
- Применение ML моделей для обнаружения утечек по скрытым каналам (DNS-туннелирование) и попыток обращения к автоматически сгенерированным доменам
- Защита от угроз нулевого дня с помощью ограничения доступа к новосозданным доменам
- Контент-фильтрация DNS-трафика по категориям веб-сайтов

Solar DNS RADAR основан на

- экспертизе центра исследований киберугроз **SOLAR 4RAYS**
- данных с сетей крупнейшего оператора **ПАО «Ростелеком»**

Российское ПО

ПО находится в реестре программного обеспечения. Реестровая запись № 30153 от 22.10.2025

Условия пилота

1 месяц - бесплатно

Особенности решения

Структура решения



Базовый модуль системы



DNS RADAR CONTROL CENTER

Методы анализа



- **Solar TI Feeds «из коробки»**
- 80+ категорий ресурсов (webCat)
- ML-модели для детекта DNS-туннелей и DGA-доменов
- Модуль Zero Trust
- Passive DNS
- Черные/белые списки
- DNS Rebinding Protection

Модуль для анализа всего DNS-трафика



DNS PROXY

Анализ всего DNS-трафика внутри инфраструктуры.

Отторгаемый модуль для более гибкой имплементации внутри инфраструктуры, а также более точной локализации заражения.

Функциональность DNS Radar



Обнаружение угроз

- Выявление вредоносных и фишинговых доменов в DNS-трафике
- Детектирование командных серверов (C2) и DGA-доменов
- Распознавание активных APT-группировок
- Распознавание DNS-туннелей

Контекст и аналитика

- Подробные карточки сработок: источник, домен, контекст
- Исторический анализ запросов по новым индикаторам компрометации
- Полноценный Log Management для фильтрации и хранения событий

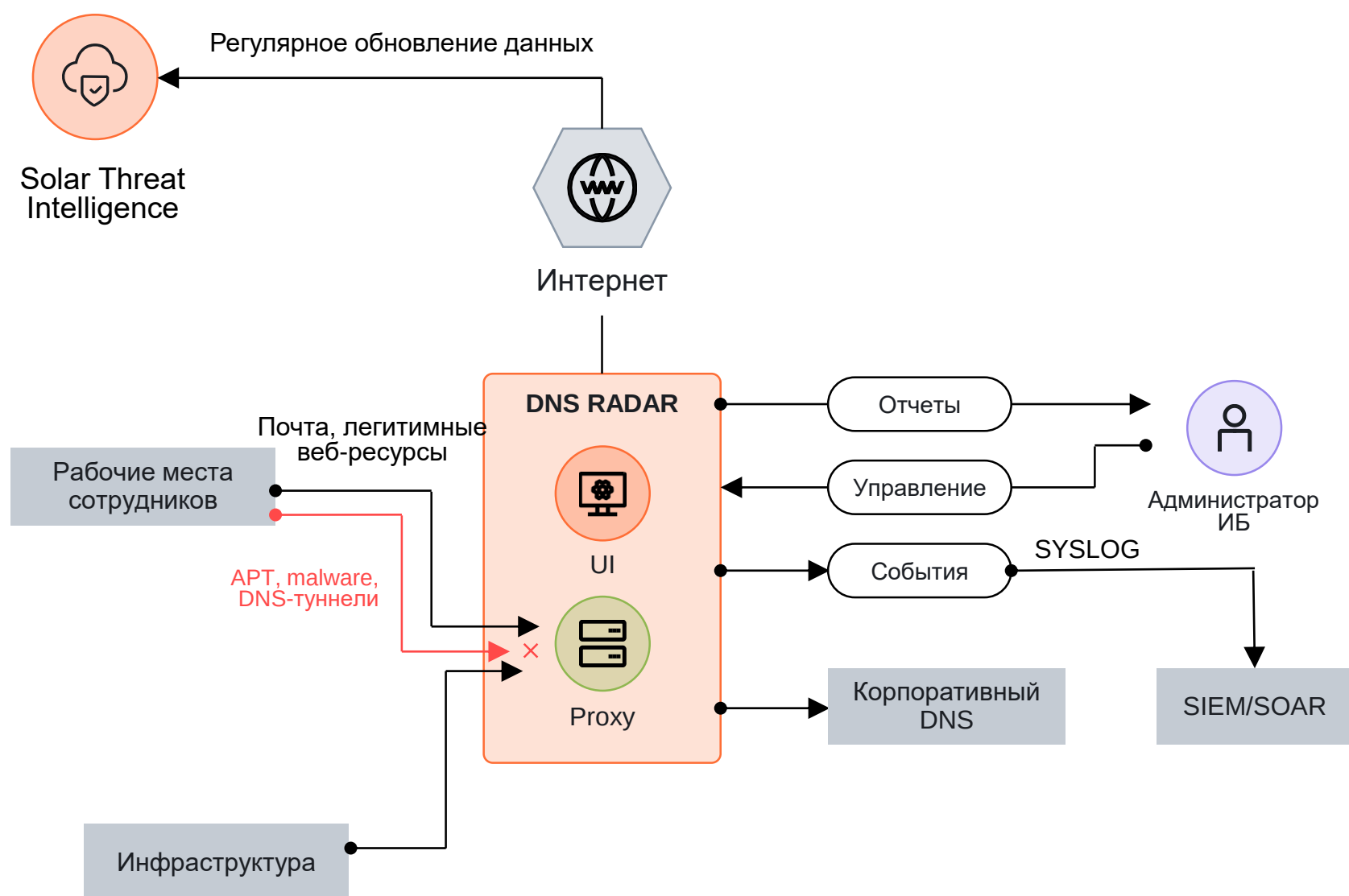
Блокировка и фильтрация

- Возможность автоматической блокировки DNS-запросов к вредоносным доменам
- Категоризация сайтов (социальные сети, азартные игры, VPN и др.)
- Возможность использования собственных черных/белых списков для фильтрации трафика

Интеграция и отчетность

- Интеграция с различными СЗИ по syslog, по API
- Экспорт журнала событий. Возможность самостоятельно выгружать пользователю информацию о событиях в формате .csv
- Информирование о сработках по smtp

Как получить доступ к решению



Варианты поставки

- Cloud
- Гибрид
- ON PREM

Лицензирование

- Лицензируется по варианту поставки, количеству запросов в секунду (RPS)
- On premise — годовые лицензии
- Облако/гибрид — ежемесячно или сразу на год

Дополнительные возможности

Возможна установка дополнительного прокси-DNS-сервера в инфраструктуре заказчика. Использование прокси позволит определить конкретную рабочую станцию, которая отправила DNS-запрос

Облачное подключение

- За один день
- Не требует дополнительных ресурсов для установки и специальной подготовки инфраструктуры

Гибридное подключение

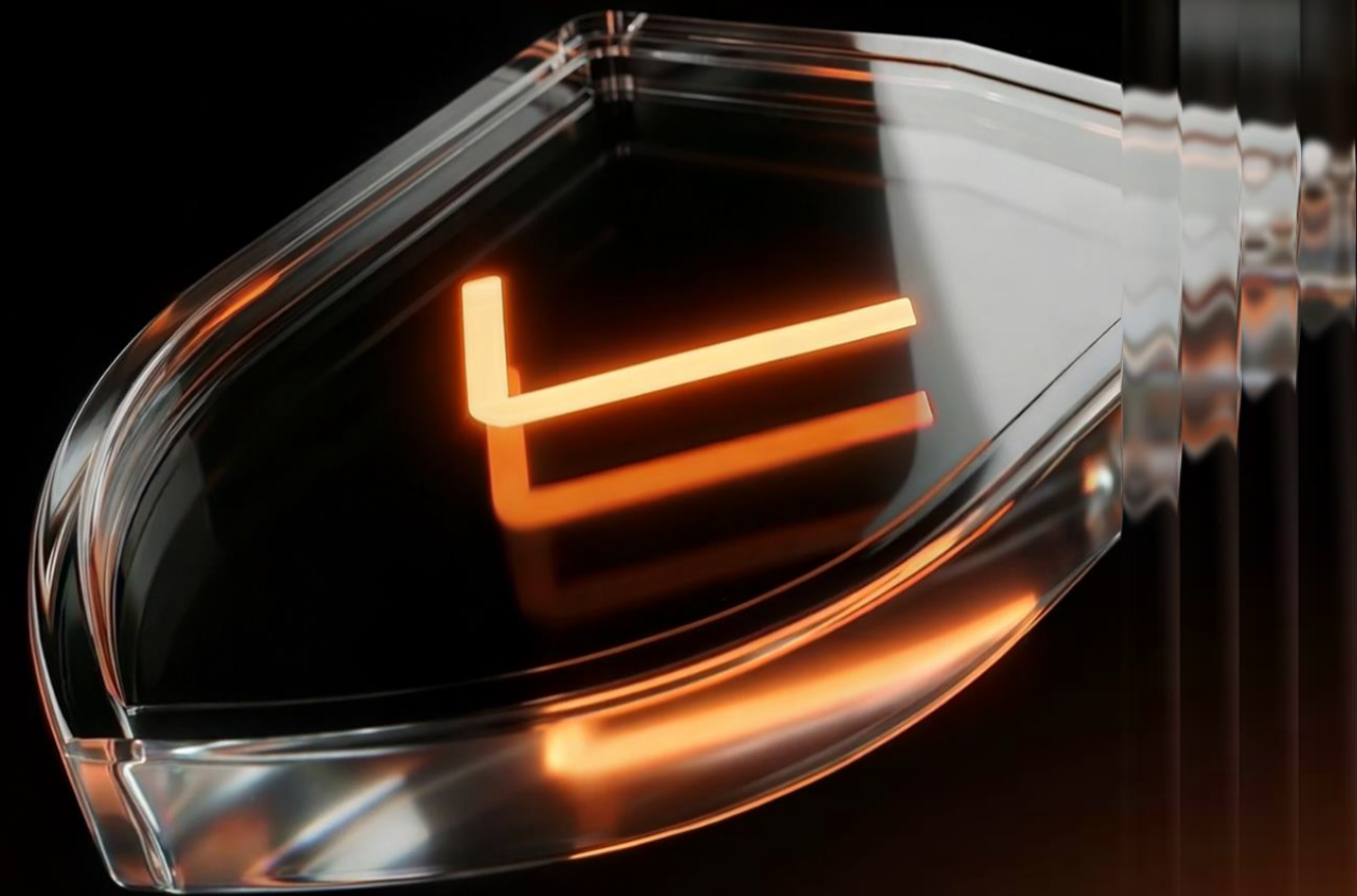
DNS проху — легкий, не требует много места для разворачивания

On-premise

Подходит организациям с жесткими требованиями к передаче информации вовне

[Запросить консультацию](#)

Solar LightHouse



- Инвентаризация
- Безопасность конфигураций
- Контроль процессов

Solar LightHouse

Продукт для централизованного управления безопасностью инфраструктуры. От непрерывного анализа состояния активов, мониторинга СЗИ до проактивной защиты на уровне процессов, конфигураций и архитектуры.

[Оставить заявку](#)

Вызовы бизнеса

- Нет понимания состава и состояния активов в ИТ-инфраструктуре, какое ПО и ОС устарели, какие учетные записи нужно удалить и т.д..)
- Нет понимания какой процент инфраструктуры покрыт политиками безопасности

Solar LightHouse

- Единое окно для контроля и управления состоянием инфраструктуры
- Инструмент для постоянного контроля и управления изменениями состояний и параметров активов

Результат

- **Достоверная и управляемая инфраструктура без серых зон**
- **Инфраструктура, готовая к росту и требованиям регуляторов**

EAP

LightHouse относится к новому классу решений ИБ

для непрерывного обнаружения, агрегации, приоритизации и устранения рисков и уязвимостей



Функциональные особенности

Полная видимость инфраструктуры

Solar LightHouse собирает данные из разных источников — обнаруживает забытые объекты

- Хосты, сервисы и сетевые компоненты, ОС, прошивки
- Учетные записи пользователей и сервисов
- Домены, зоны доверия и сегменты сети
- ИТ-системы, состоящие из компонентов



Анализ конфигураций

Solar LightHouse проверяет параметры активов и отслеживает изменения состояния

- Корректность конфигураций систем и сервисов
- Соответствие принципу минимально необходимых привилегий
- Избыточный, устаревший, неявный доступ
- Корректность сетевой сегментации



Контроль учетных записей

Solar LightHouse выявляет отклонения и избыточность привилегий, предоставляет рекомендации для устранения

- Пользовательские, сервисные и технические
- Административные и привилегированные
- Атрибуты требующие дополнительного контроля (вечный пароль, требования к персонализации и прочее)
- Зависимости между аккаунтами и инфраструктурными компонентами
- Локальные учетные записи и их привилегии



Контекст для работы с обновлениями

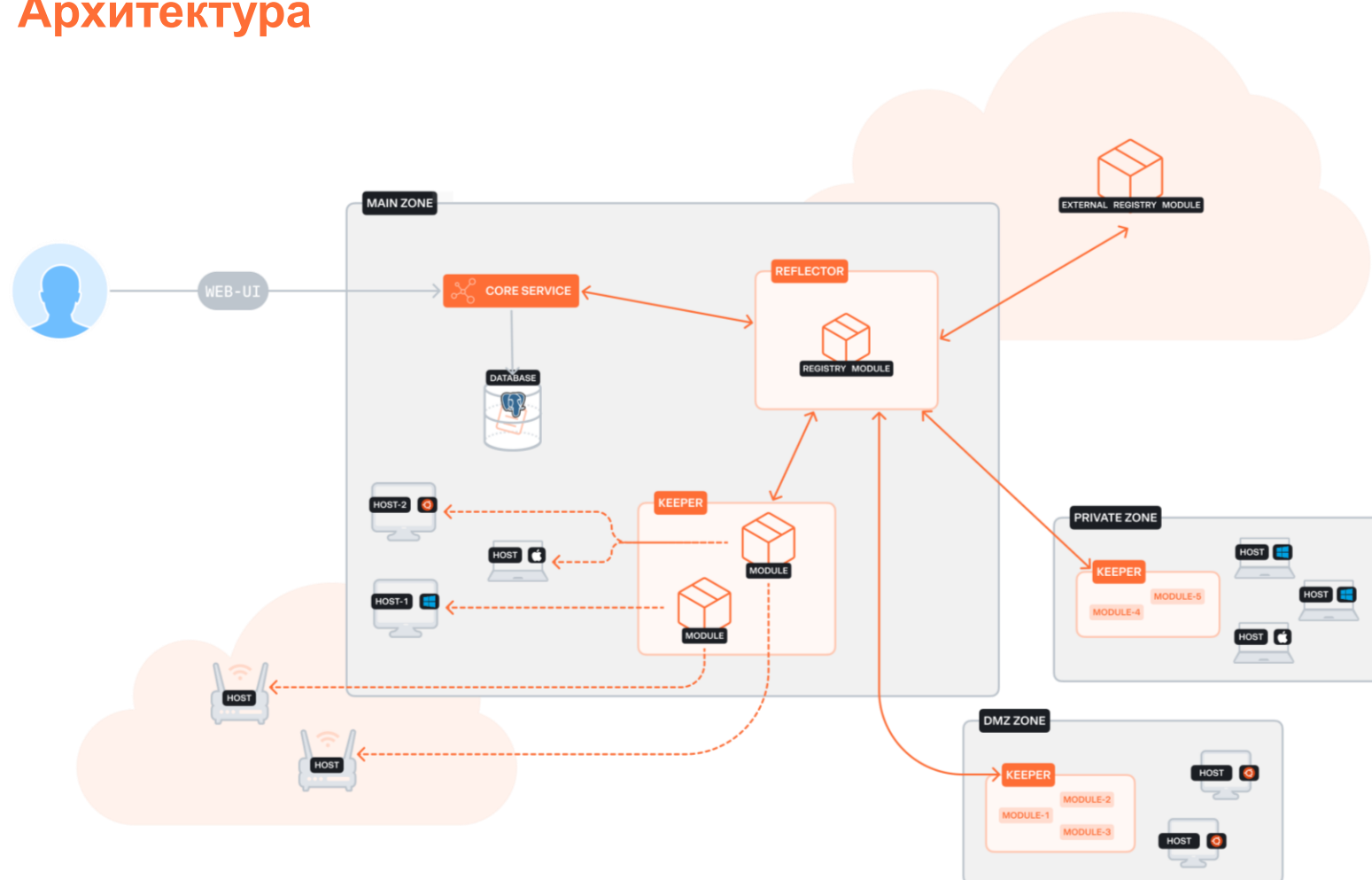
Solar LightHouse улучшает процесса патч менеджмента посредством конкретных рекомендаций

- Указывает, какие конкретные обновления или патчи применить
- Использует знания об объектах инфраструктуры для управления приоритетами
- Приоритизация объектов для обновления



Особенности решения

Архитектура



Технические характеристики

- **Архитектура:** сервер управления и коллекторы для удаленных площадок и закрытых сегментов сети
- **Без агентов** на конечных точках
- **Модульная архитектура** — адаптируется под любую инфраструктуру
- **Разграничение прав:** разделение видимости для разных площадок, филиалов и холдинговых структур централизованными политиками
- Боевая инсталляция от 2 ядер и 4 ГБ ОЗУ

Интеграции в ИТ-ландшафте

- Windows, Linux и другие ОС с CLI
- Каталоги пользователей, DNS, DHCP, почтовые сервисы
- Средства защиты информации
- Сетевое оборудование
- Среды виртуализации
- Базы данных
- Интерфейсы управления (iLO, iDRAC, IPMI)

Запросить консультацию

Лицензирование

- По количеству хостов в инфраструктуре (от 100 шт.)
- **ON PREM**

Поддерживаемые ОС для установки

- Astra Linux
- RedOS
- Ubuntu / Debian / CentOS (с Docker)

Сервисы



Выявление и реагирование на инциденты ИБ (SOC)

Оперативное выявление и анализ
инцидентов ИБ

JSOC ONE

Флагманский SOC с гарантией

Для компаний, которым защита нужна сейчас, а не через 9 месяцев

[Подробнее на сайте](#)

✗ Классический проект

3–9 месяцев внедрения

Высокий CAPEX + интеграция
Требует зрелой инфраструктуры
Только для крупного бизнеса

✗ In-house SOC

Дорого и дефицитно

Нет экспертизы по новым атакам
Нет уверенности в покрытии 24/7
Теучка кадров = риск

✓ JSOC ONE

Подключение от 1 дня*

Фиксированная стоимость от 3 млн ₽
Мониторинг 24/7 с первого дня
Экспертиза 14 лет на рынке

0,001% Событий доходит до вашей команды. Шум разбираем мы

20^{мин} Оповещение при критичном инциденте

30^{мин} Реагирование при критичном инциденте

Нам доверяют**

УБРИР

ГРУППА КОМПАНИЙ
СОДРУЖЕСТВО

МСП
корпорация

БСПБ

ТМК
СинТЗ

ГОСУДАРСТВЕННАЯ НАВИГАЦИОННАЯ СЛУЖБА
ГЛОНАСС

Правительство
Камчатского края

Правительство
Самарской области

ОТС

РТК-ЦОД

Вы получаете

- SOC-команду вместо ФОТ 6–18 млн ₽ и поиска дефицитных специалистов
- Реагирование по согласованным с вами сценариям
- Оплату только за нужные модули - сервис растёт вместе с вами
- Экспертизу Solar JSOC и базу атак Solar 4RAYS в одном пакете

Гарантии по договору

30^{млн ₽}

Возмещение за ущерб от пропущенный инцидент

* для тарифа JSOC ONE Start

** небольшая часть организаций, которые выбрали Solar SOC и согласились на открытый референс

Как работает

- 01

Сбор информации с инфраструктуры для выявления следов атак (Compromise Assessment)
- 02

Установка EDR-агентов на рабочие станции и серверы

* Подключение системы сбора событий Solar SIEM
- 03

Агенты передают для анализа данные о событиях в облако JSOC, блокируют атаки на рабочих станциях и серверах

* Детектирующий контент JSOC выявляет инциденты, аналитики верифицируют и отправляю оповещение клиенту
- 04

В случае направленной атаки, подключаются эксперты JSOC для оперативного блокирования угрозы

Свяжитесь с вашим менеджером «Солара» или оставьте заявку

Запросить консультацию

* для тарифа JSOC ONE Smart

	JSOC ONE Start	JSOC ONE Smart
Стоимость	от 3 млн Р	от 4,2 млн Р
Технологическое ядро	Solar EDR	Solar EDR + Solar SIEM
Compromise Assessment	на этапе подключения	на этапе подключения
24x7 Выявление и реагирование на инциденты	на конечных точках	реагирование на конечных точках
Реагирование на СЗИ клиента	-	Р
Блокировка запросов к опасным доменам (DNS)	+	+
Учет активов и подключённых систем (Lighthouse)	ограничено конечными точками	+
Раннее оповещение о новых угрозах	для каналов провайдера Ростелеком	для каналов провайдера Ростелеком
Аналитика угроз (TI): оценка рисков и поиск следов атак	+	+
Подключение нетиповых источников	-	лимитировано кол-вом eps
Сопровождение: выделенный сервис-менеджер, аналитик	+	+
Поиск утечек	Р (промо)	Р (промо)

!

Представленная тарифная линейка JSOC ONE содержит платные опции, которые подключаются по запросу

Solar AURA

Комплексный DRP-сервис для мониторинга
внешних цифровых угроз

Solar AURA

Сводим к минимуму финансовые, репутационные и киберриски

[Подробнее на сайте](#)

Вызовы бизнеса

Снижать цифровые риски, а именно:

- Предупреждать атаки
- Выявлять факторы репутационных рисков
- Выявлять факторы финансовых рисков, в т. ч. при взаимодействии с контрагентами
- Осуществлять защиту бренда компании и личных брендов ключевых сотрудников
- Обеспечивать высокий уровень защищенности инфраструктуры

Решение

- Оперативное выявление утечек данных
- Обнаружение и блокировка фишинга от имени компании
- Обнаружение признаков подготовки кибератак в даркнете
- Обнаружение признаков применения эквайринга в противоправных целях
- Отслеживание случаев незаконного использования бренда
- Мониторинг ИТ-активов компании

11 модулей

в одном сервисе

2+ млн

доменных имен и выданных SSL-сертификатов анализируется в сутки

87%

фишинговых ресурсов блокируется менее чем за 24 часа

96%

событий анализируется в автоматическом режиме

Нам доверяют компании из разных отраслей

Ретейл – в том числе Wildberries

Финансы и страхование

Государственные структуры

Промышленность и нефтепереработка

Недвижимость и другие

Подключение

Формат поставки

Облачный сервис

Модули Solar AURA

- Антифишинг
- Бренд компании
- Юрлица
- Утечки
- Личный бренд
- Тренды
- Услуги
- Медиаполе
- Резюме
- Инфраструктура
- Антидроп

Ценообразование

Механика ценообразования: зависит от состава подключаемых модулей и количества объектов (доменов, брендов, IP и т. д.) на мониторинге

- Подписка сроком 1 год и более может быть предоставлена на помодульной основе под конкретные задачи, требований по обязательному минимальному набору компонентов нет
- В рамках одной компании может использоваться несколько подписок с доступом к разным модулям, например, для подразделений PR, ЭБ и ИБ

Как попробовать решение

- Онлайн-демонстрация
- Пилотный проект

ТОПовые преимущества

Широкий функционал

11 модулей в одном сервисе + дополнительные услуги по аналитическому и юридическому сопровождению

Мгновенный мониторинг

Широкое покрытие источников в публичных и закрытых сегментах интернета

Оперативная блокировка фишинга

Минимальное время — 1 мин. 46 сек., 87% ресурсов — менее чем за 24 часа

Сервис под ключ

Подключение до 3 дней, доступность в работе — сервис не требует высокой квалификации специалистов заказчика

Совместная работа и контроль эффективности

Многопользовательский режим, постановка задач, контроль их выполнения и учет затраченного времени

Интеграционные возможности

Добавление событий через API, обработка большого количества запросов и двусторонняя интеграция с решениями других классов



**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Сервис выявления и анализа уязвимостей 1 VM



Оперативное выявление и анализ уязвимостей
от инвентаризации до устранения

Выявление и анализ уязвимостей

Выстраиваем сервис под потребности вашего бизнеса

Подробнее на сайте

Риски бизнеса

- Снизить риск критичных инцидентов и простоев бизнеса
- Уверенно проходить проверки регуляторов и внешние аудиты
- Сдерживать рост затрат на ИБ при дефиците людей и экспертизы

Решение

- End-to-end процесс VM: от инвентаризации до контроля фактического закрытия критичных уязвимостей
- Комплаенс-отчётность и прозрачные метрики по охвату, срокам устранения и уровню защищённости
- Аутсорс-команда по VM за цену одного специалиста с настройкой, администрированием и автоматизацией

Ключевые факты

Предсказуемые затраты на ИБ

Обеспечиваем контроль уязвимостей по цене одного специалиста, с гибкими тарифами по числу IP-адресов

Проверено на системах федерального масштаба

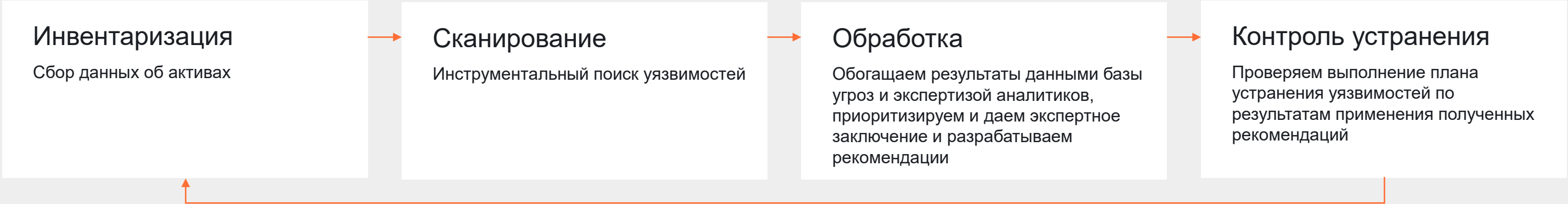
Защищаем крупные государственные и коммерческие инфраструктуры (включая Госуслуги и другие высоконагруженные сервисы)

Быстрый старт без инфраструктурных изменений

Запускаем процесс контроля уязвимостей за 60–90 дней и начинаем выявлять критичные уязвимости уже через 2–5 рабочих дней после подключения

Как работает сервис

ЭТАПЫ



Как это работает

Схема подключения облачного сервиса

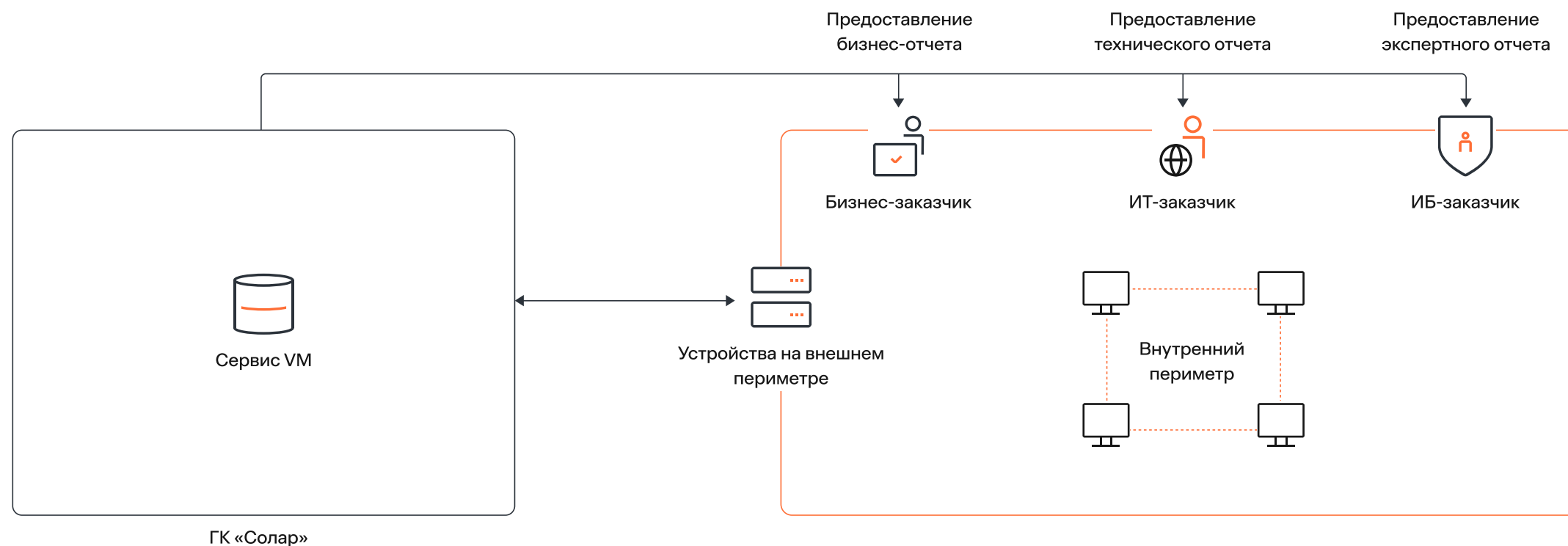
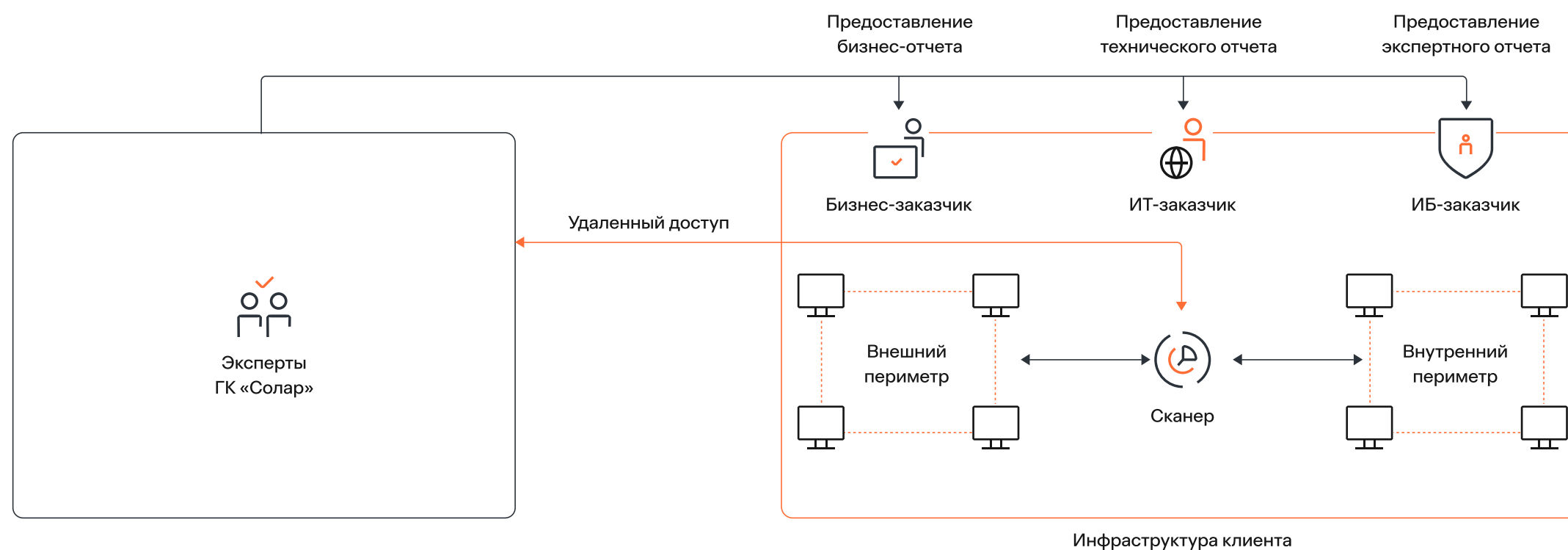


Схема подключения на сканере клиента



Управлять угрозами просто

- Облачная лицензия на 10–50% дешевле прямой покупки у вендора, необходимые аппаратные мощности входят в стоимость сервиса
- Собственные search-листы с учётом трендов уязвимостей и их применимости в атаках
- Три типа отчётов: бизнес, технический, экспертный — для всех заказчиков в компании (инженеры, CISO, регуляторы)

Подходит для компаний с разной структурой

- Формат сервиса
 - Облачный
 - Облачный сервис для распределенной инфраструктуры
 - Обслуживание на сканере клиента
 - Ретроспективный аудит
- Интеграции с IRP, SOAR, Helpdesk, системами инвентаризации
- WhiteBox- и BlackBox-сканирования

Запросить консультацию

Solar Threat Intelligence Feeds

Сервис поставки потоков данных (фидов) об актуальных угрозах

Непрерывное усиление SOC с помощью уникальных фидов для раннего обнаружения и реагирования

Solar Threat Intelligence Feeds

Поток данных об угрозах, основанный на уникальных знаниях команды Solar 4RAYS и данных от крупнейшего оператора связи ПАО «Ростелеком»

[Подробнее на сайте](#)

Вызовы команды SOC и бизнеса

- SOC перегружен количеством обрабатываемых инцидентов. Выше шанс пропустить критичный инцидент. Риск понести убытки
- SOC получает данные, бесполезные для предотвращения кибератак. Выше шанс пропустить критичный инцидент. Риск понести убытки
- Нехватка контекста угроз для ускорения реагирования на инцидент. Низкая скорость реагирования. Выше потери от последствия атаки

Решение

SOLAR TI FEEDS. Поток данных (фидов) об актуальных угрозах:

- Индикаторы компрометации (IoC): IP-адреса, домены, веб-ссылки, хэш-суммы
- Индикаторы атак (IoA): правила обнаружения Suricata, YARA, Sigma
- Доступ к TI-portal с контекстом по индикаторам компрометации

** Решение включено в единый реестр российского ПО. Реестровая запись [№28356](#) от 06.06.2025*

Ключевые факты

Актуальные угрозы из уникальных источников

- Сведения от сенсоров в сети крупнейшего телеком-оператора «Ростелеком»
- Телеметрия сервисов крупнейшего центра противодействия Solar JSOC и топ-5 в рейтинге MSSP Европы
- Результаты собственной киберразведки и более 300 расследований Solar 4RAYS

Реальные знания о вредоносных кампаниях 24/7

- Ежедневно фиксируются и обрабатываются события
- 200+ млрд событий на сенсорах, 3+ млн алертов, 1+ млн действий хакеров

После автоматической и ручной проверки остаются только сведения о самых опасных и актуальных угрозах

Непрерывное усиление SOC для раннего обнаружения и реагирования на угрозы.

Solar TI Feeds — это собственные источники данных и команда исследователей киберугроз центра исследований Solar 4RAYS

Проверенные знания без фолзов

- Проверяем и обкатываем правила на крупнейшем коммерческом SOC в РФ
- Подтверждаем полезность фидов при проведении собственных расследований
- Даем возможность оценить качество данных на пилотном подключении

[Читать исследования в блоге](#)

Возможности сервиса Solar Threat Intelligence Feeds

Лицензирование и ценообразование



Кастомизация фидов

- Поставка более 20 готовых фидов
- Готовые 4 комплекта под ключевые задачи служб ИБ
- Индивидуальная настройка фильтров, срезов и правил

Интеграция с СЗИ

- SIEM-, SOAR-системы, NGFW, EDR, XDR и т. п.
- TI-платформы

Гибкость состава

Solar TI Feeds позволяет подключать только необходимый состав потоков данных под ваши текущие задачи с возможностью дальнейшего апгрейда и масштабирования

Гибкость подключения

- Подключение через агент
- Подключение напрямую

Быстрый старт пилота

Подготовим предложение за 2–3 дня:

- обсудим задачи
- проведем бюджетную оценку
- и обсудим старт пилота

Протестировать сервис

Security Awareness

Повышение киберграмотности сотрудников

Комплексный подход к формированию навыков противодействия фишингу

Security Awareness обеспечивает комплексный подход к программе повышения уровня осведомленности о киберугрозах и помогает сформировать у сотрудников навык обнаружения фишинговых атак и правильного реагирования на них

[Подробнее на сайте](#)

Какие требования закрывает

- Проведение обучения по вопросам защиты от фишинговых атак
- Проведение имитационных рассылок электронных писем на служебные адреса электронной почты с целью оценки устойчивости пользователей к атакам методами социальной инженерии
- Проведение тренировок по практической отработке пользователями мероприятий по защите информации и формированию навыков по защите информации
- Соблюдение обязательных требований регуляторов

Преимущества

- Экспертный подход, планирование обучения и учебных фишинговых рассылок
- Анализ результатов обучения и фишинговых рассылок
- Подготовка отчетов с рекомендациями
- Кастомизация шаблонов рассылок, обучающие курсы от экспертов

Стоимость зависит

- От модели поставки (MSS, SaaS, On-premise)
- Количества сотрудников

Технологии

[Платформа «Secure-T»](#)[Сервис ГК «Солар»](#)

Ключевые факты

- Российское ПО, сертификация ФСТЭК
- Соответствие законодательству: 152-ФЗ, положение ЦБ РФ 757-П, Приказы ФСТЭК № 117, № 239 (КИИ)
- Своевременное оповещение ИБ-департамента в случае киберинцидента
- Снижение вероятности утечек конфиденциальной информации
- Повышение уровня осведомленности сотрудников о киберугрозах

Как начать использовать Solar SA



Проверить, насколько вероятны угрозы фишинга вне зависимости от мер, принимаемых в компании



Быстро оценить, какое количество сотрудников уязвимы к фишингу:

- переходы по фишинговой ссылке
- заполнение информации в фишинговой форме
- открытие вложения



Получить развернутый аналитический отчет с рекомендациями мер по повышению уровня кибергигиены сотрудников



Провести аудит навыков киберграмотности



Выявить группу высокорисковых пользователей, наиболее уязвимых к фишингу, чьи учетные данные попали в даркнет

К моменту старта проверки должны быть выполнены следующие условия:

- Подготовлен список проверяемых сотрудников для обучения в формате таблицы .xls
- Предоставлен домен для анализа утечек
- Выполнены настройки по добавлению исключений в антиспам-систему и песочницу
- Выделены технические специалисты
- Подписаны договор и авторизационное письмо
- Согласованы содержание и даты учебных фишинговых рассылок

Важно

Домену клиента будет проведено выявление учетных записей, попавших в публичные утечки (совместно с Solar AURA*)

* [Сервис мониторинга внешних цифровых угроз](#)



Защита веб-приложений

Web Application Firewall

Сервис защиты веб-ресурсов от киберугроз
в круглосуточном режиме



Защита веб-приложений (WAF)

Эффективное противодействие атакам на веб-приложения за счет эксплуатации многоступенчатых модулей защиты, включающих профилирование и анализ аномалий трафика

[Подробнее на сайте](#)

Риски бизнеса

- Взлом сайта может привести не только к потере прибыли, но и доверия клиентов, что негативно сказывается на конкурентоспособности бизнеса
- Нарушение безопасности данных пользователей ведет к штрафам, судебным искам и долгому восстановлению доверия
- Злоумышленники тоже учатся и уже сейчас используют ботов и технологии обхода защиты, усложняя обнаружение и блокировку угроз
- Бизнесу важно быстро и безболезненно реагировать на хакерские атаки, без долгих процедур и крупных расходов

Решение

- Автоматическая фильтрация в режиме реального времени, экспертное управление, выявление и блокировка атак без ущерба для работы сервисов
- Защита API, CMS и бизнес-логики с кастомизацией под клиента, маскирование чувствительных данных на уровне WAF, соответствие требованиям 152-ФЗ
- Круглосуточный мониторинг и анализ событий командой Solar MSS, регулярная актуализация и настройка защитных правил под новые угрозы
- Развертывание WAF от двух дней без остановки веб-приложений, минимум действий со стороны клиента, возможность подключения под атакой

Ключевые факты

Многоуровневая защита и экспертная поддержка

Многоуровневая система Solar MSS обнаруживает сложные и нетипичные атаки за счет комбинированного анализа трафика, кастомных экспертных правил и круглосуточного мониторинга

Устойчивость к веб-угрозам

Комплексная защита охватывает уязвимости OWASP Top 10, прикладные DDoS- и бот-атаки, предотвращает утечки данных и обеспечивает профилирование трафика и анализ аномалий

Адаптивность и индивидуальная настройка

Сервис обучается на реальном трафике клиента, что позволяет создать индивидуальный профиль защиты, адаптированный под поведение пользователей и изменения веб-приложения

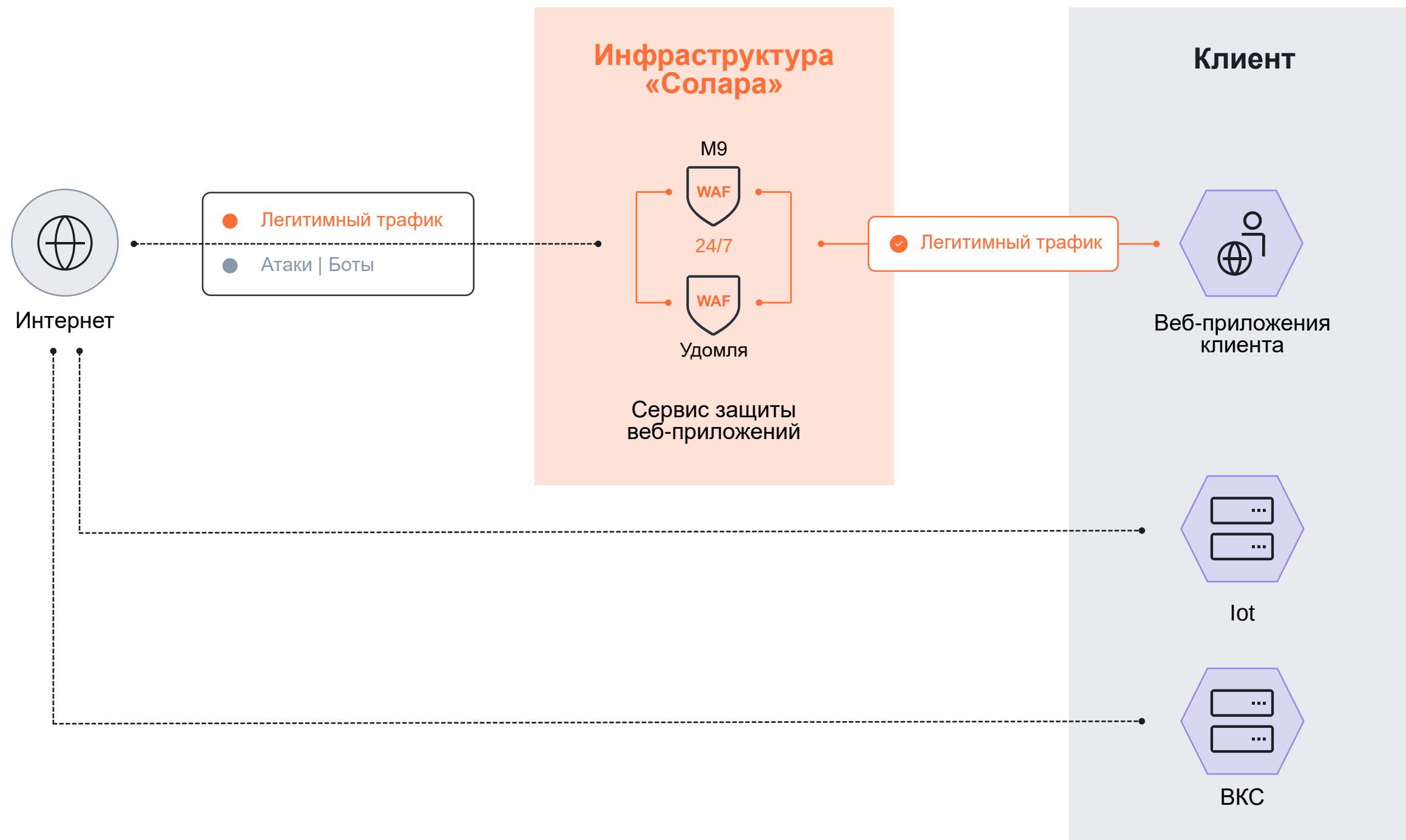
Удобство и экономия для бизнеса

Быстрое подключение без покупки оборудования, передача нагрузки и ответственности экспертной службе «Солара», оплата только по факту пользования, масштабирование под нужды бизнеса, ЛК для управления и контроля

Нам доверяют



Шаги внедрения



Варианты подключения

Стандартное

До 5 дней

- Анализ потребностей заказчика
- Автоматизированное развертывание WAF
- Настройка WAF и личного кабинета заказчика
- Круглосуточный мониторинг, донастройка профилей защиты

Подключение под атакой

3-5 часов

- Оперативное развертывание WAF
- Ручное профилирование защиты, идентификация и блокировка злоумышленника
- Финальная проверка доступности, перевод защиты в штатный режим

Шаги внедрения

Метрики тарификации

- Количество веб-приложений
- Тип веб-приложений: инфоресурс, портал+, ДБО, API, OWA, Share Point
- Максимальное количество запросов к веб-приложению в секунду, RPS
- Необходимый заказчику уровень обслуживания: скорость реакции, глубина сопровождения и дополнительные опции



Сроки контрактования

- Типовое подключение — от 3 дней
- Срок контрактования — от 3 месяцев



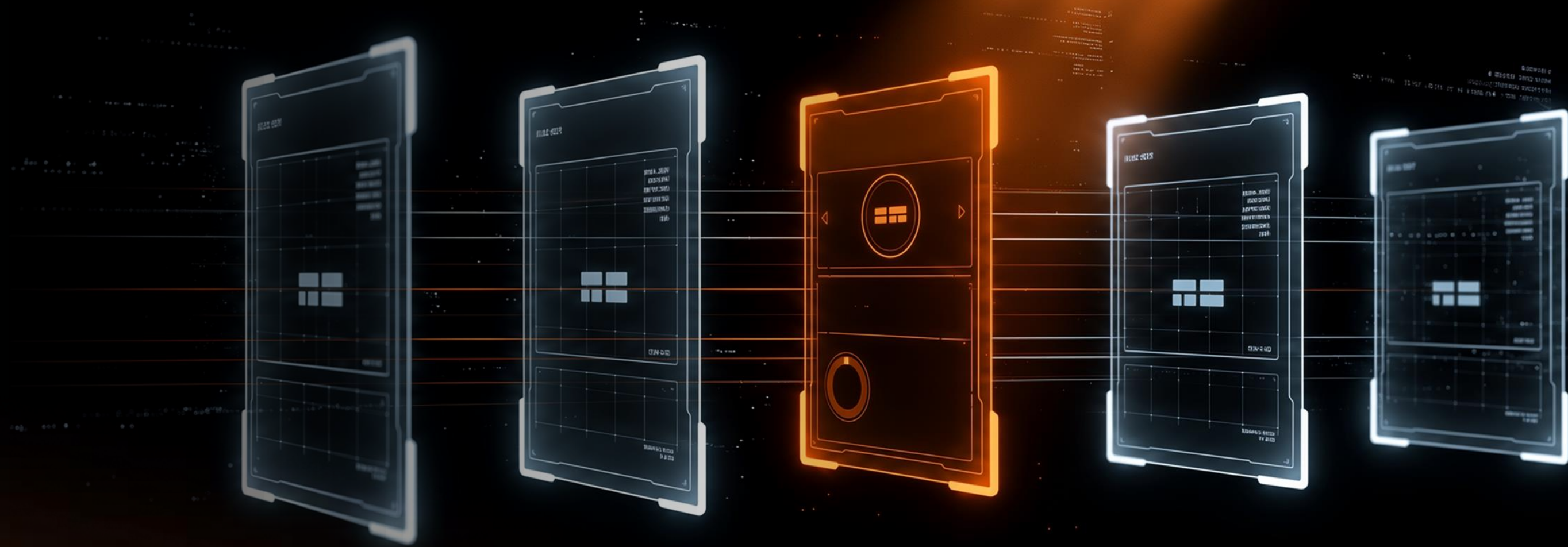
**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Защита от бот-трафика

Antibot



Экспертный сервис по защите от бот-трафика
и распределенных атак отказа в обслуживании
на уровне приложений

Защита от бот-трафика (Antibot)

Эффективное противодействие атакам на веб-приложения за счет эксплуатации многоступенчатых модулей защиты, включающих профилирование и анализ аномалий трафика

[Подробнее на сайте](#)

Риски бизнеса

- Избыточная нагрузка на серверы приложений из-за массовых бот-запросов снижает производительность и вызывает сбои
- Рост объемов бот-трафика снижает точность защиты и увеличивает риск пропуска атак
- Существенные затраты на инфраструктуру и защиту (WAF) из-за необходимости обрабатывать лишний трафик
- Рекламный фрод и искажение аналитики приводят к неэффективному расходу бюджета и потере связи с реальными клиентами

Решение

- Solar Antibot блокирует паразитный трафик еще на входе, обеспечивая стабильную работу сервисов
- Сервис использует автоматическое масштабирование для эффективной фильтрации угроз независимо от нагрузки — до 1 000 000 RPS
- Antibot снижает TCO облачной инфраструктуры и WAF за счет исключения затрат на обработку паразитного бот-трафика
- Сервис очищает данные, блокирует накрутки и защищает инвестиции в рекламу за счет выявления и фильтрации ботов

Ключевые факты

Интеллектуальная фильтрация трафика

Решение использует современные методы: анализ TLS-отпечатков, JavaScript-челленджи, CAPTCHA и машинное обучение, точно выявляя и блокируя паразитный бот-трафик до входа на сервер

Экономия и оптимизация затрат

Не нужно покупать собственное оборудование и лицензии — оплата только за сервис, а умная фильтрация снижает нагрузку на инфраструктуру и расходы на защиту

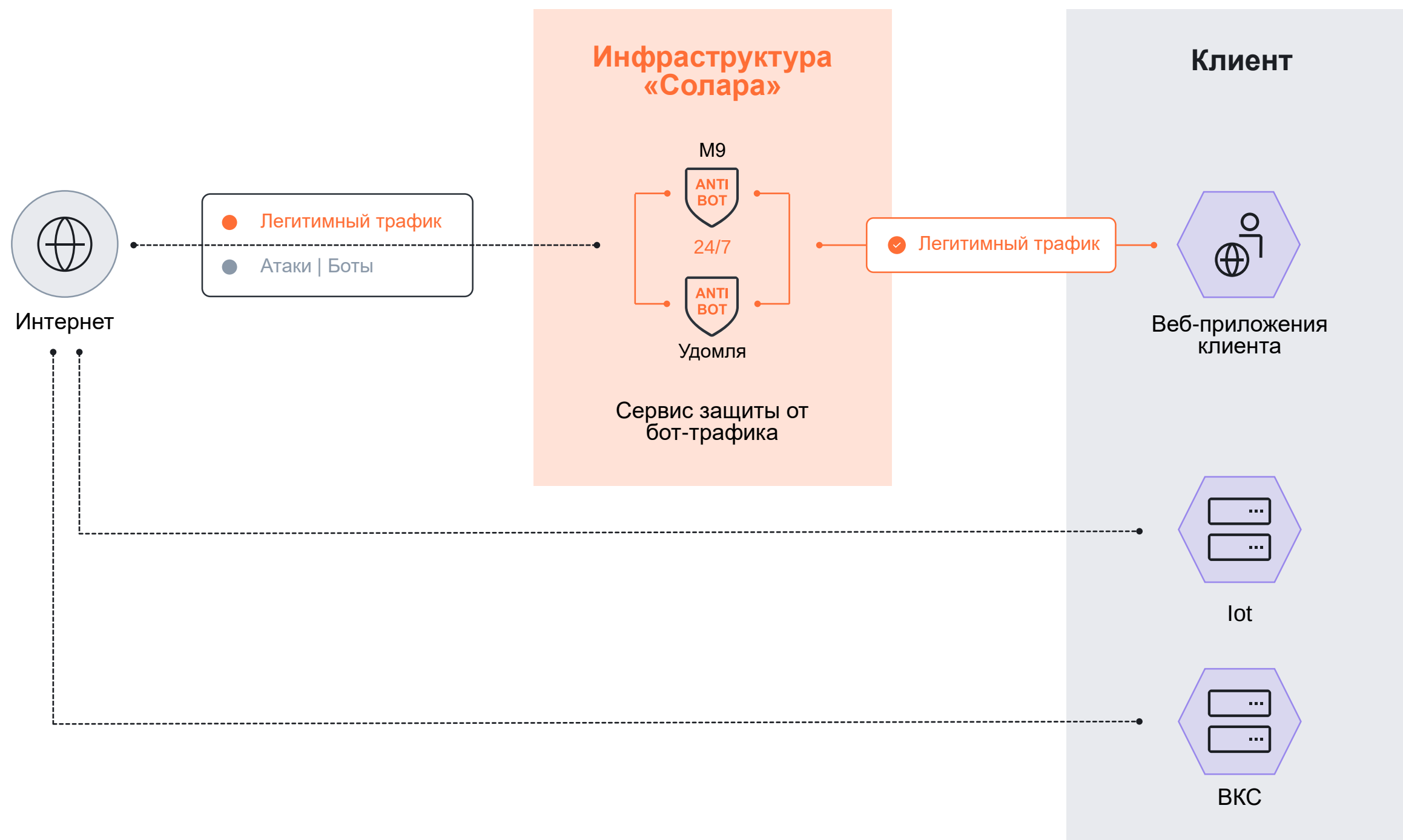
Адаптивность и индивидуальная настройка

Сервис подключается за 3 дня через смену DNS-записи, не требует сложной интеграции и дополнительного оборудования, полностью работает в облаке

Прозрачное управление и экспертная поддержка

Управление защитой осуществляется через удобный онлайн-кабинет, а команда специалистов ГК «Солар» постоянно контролирует эффективность и настраивает сервис под актуальные угрозы

Шаги внедрения



Варианты подключения

Стандартное

До 5 дней

- Анализ потребностей заказчика
- Автоматизированное развертывание сервиса
- Настройка Antibot и личного кабинета заказчика
- Круглосуточный мониторинг, донастройка профилей защиты

Подключение под атакой

3-5 часов

- Оперативное развертывание сервиса
- Ручное профилирование защиты, идентификация и блокировка злоумышленника
- Финальная проверка доступности, перевод защиты в штатный режим

Шаги внедрения

Метрики тарификации

- Количество FQDN — число сайтов/веб-приложений
- Величина полосы веб-трафика, Мбит/с (не равна емкости канала ШПД)



Сроки контрактования

- Типовое подключение: от 1 недели
- Срок контрактования: от 3 месяцев

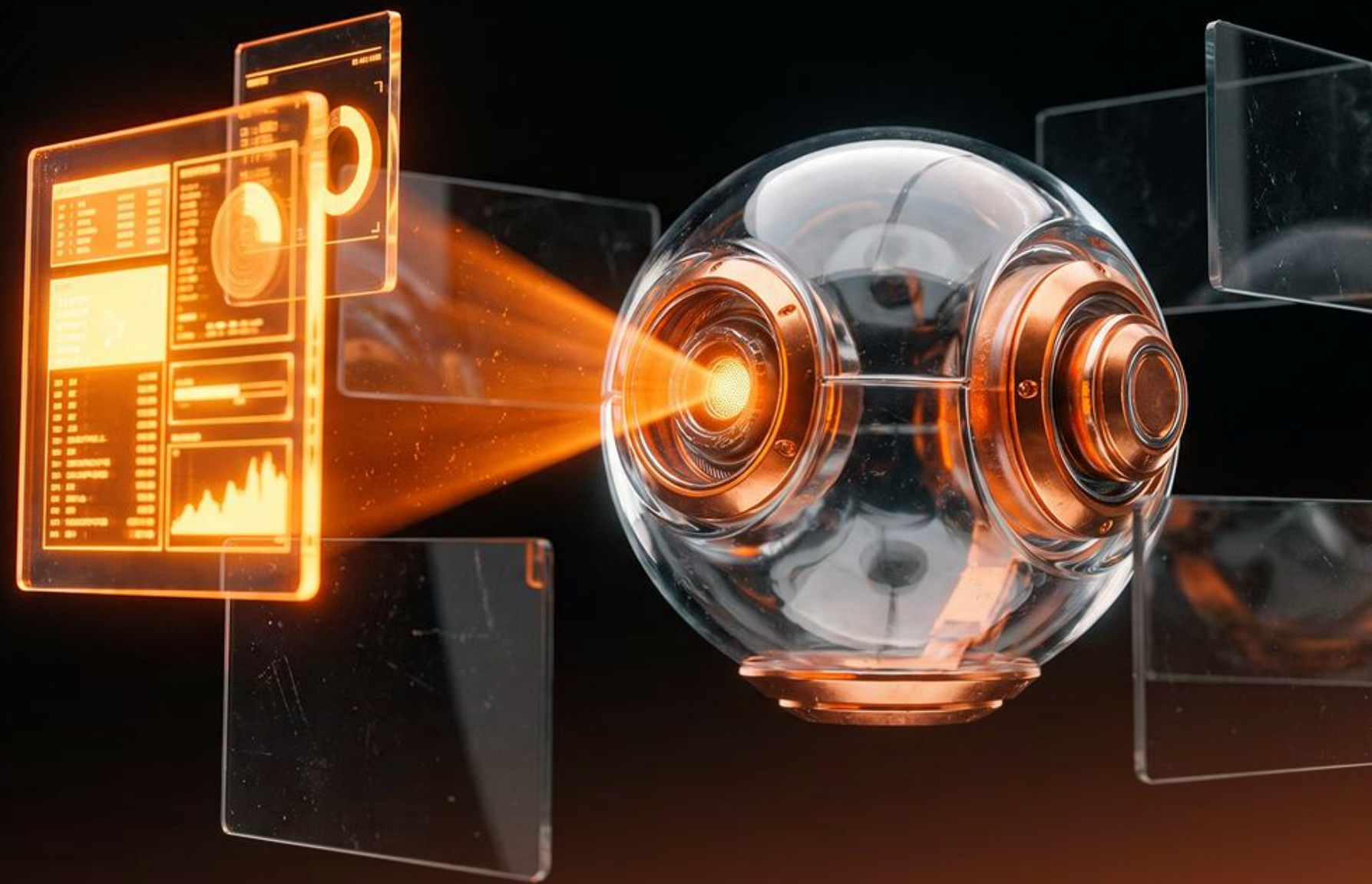


**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Мониторинг трафика и защита от DDoS-атак



Круглосуточная защита каналов связи
и онлайн-ресурсов от DDoS-атак

Мониторинг трафика и защита от DDoS-атак

Нейтрализуем даже самые сложные и массированные атаки уровня L3/L4 и обеспечиваем круглосуточную доступность интернет-ресурсов пользователям

[Подробнее на сайте](#)

Риски бизнеса

- Непредсказуемые DDoS-атаки приводят к недоступности сервисов, простоям бизнес-процессов и потере клиентов
- Сложности с поиском и удержанием опытных специалистов по кибербезопасности
- Значительные расходы на инфраструктуру и ИБ-службу
- Рост мощности и сложность атак требует уникальных технических решений

Решение

- Автоматическая фильтрация и блокировка атак за 1 минуту, круглосуточная стабильность сервисов
- Экспертное сопровождение и управление защитой, техническая поддержка 24/7
- Сервисная модель оплаты по факту использования, без вложений в оборудование и лицензии
- Защита до 5 ТБ трафика, эшелонированная гибридная архитектура, развертывание за 5 часов под атакой

Ключевые факты

Самая большая инсталляция Anti-DDoS в России

Самая большая магистральная сеть в стране — более 500 тыс. км. Гарантируем подключение и защиту любых ваших организаций и филиалов в РФ

Отражение сверхмощных мультивекторных атак

Сервис способен выдерживать любые атаки мощностью, многократно превышающей зафиксированные на текущий момент в России

Выявление угроз на ранней стадии

Эшелонированная гибридная защита позволяет отбивать атаки до их подхода к инфраструктуре заказчика, используя маршрутизаторы на сети «Ростелеком» и трансграничные маршрутизаторы

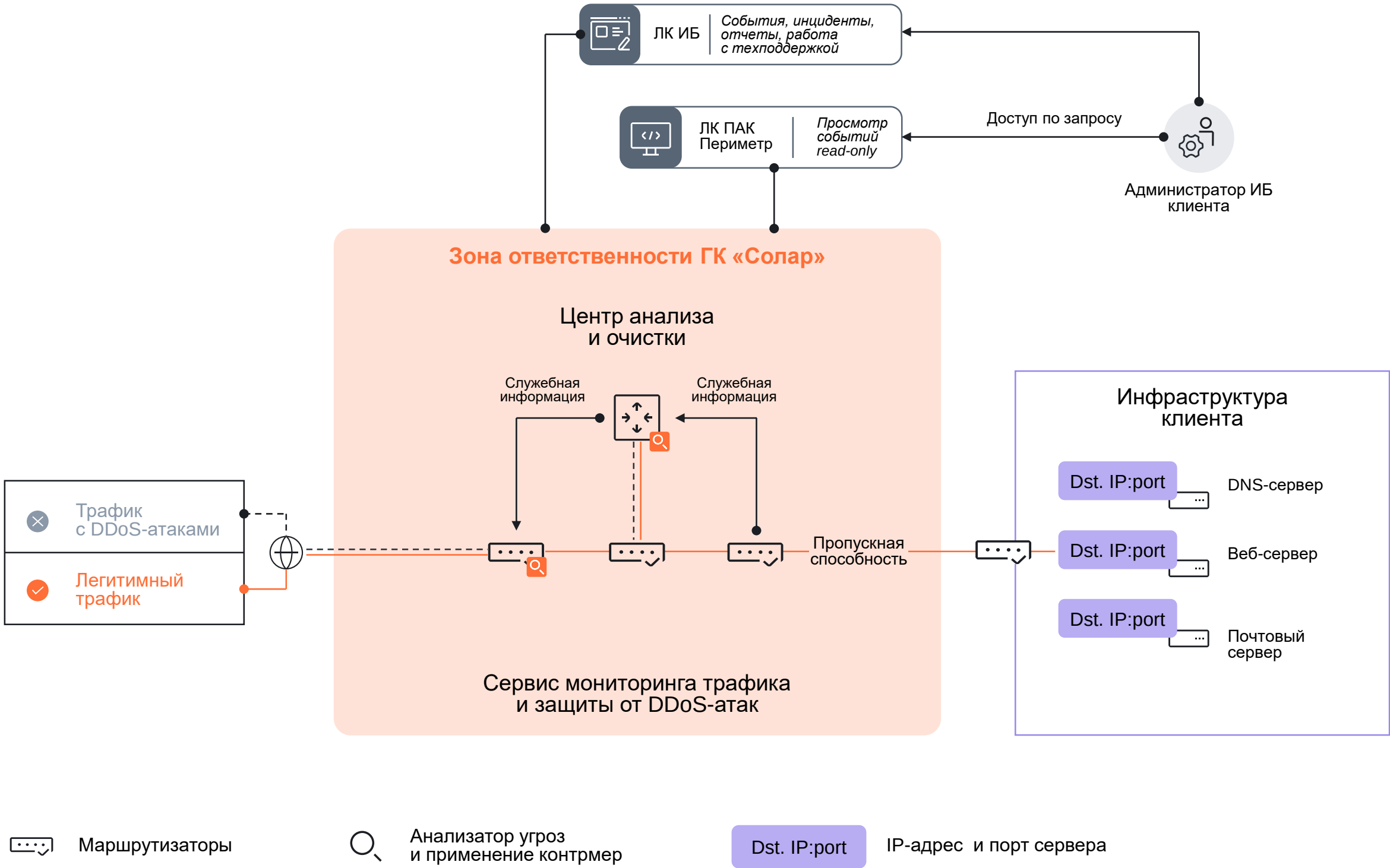
Постоянное усовершенствование политик фильтрации

Регулярно анализируем и обновляем политики фильтрации. На основе обширного опыта и клиентской базы создаем свои фиды и черные списки для эффективной блокировки угроз

Нам доверяют



Шаги внедрения



Варианты подключения

Стандартное

До 5 дней

- Консультация и расчет
- Подключение и настройка
- Запуск и эксплуатация

Подключение под атакой

3-5 часов

- Консультация и расчет
- Подключение и настройка
- Запуск и эксплуатация

Шаги внедрения

Метрики тарификации

Количество профилей защиты

Выберите подходящий тип сервиса в зависимости от количества профилей (объектов) защиты — сервисов, каналов и филиалов

Уровень поддержки

Определите необходимый уровень обслуживания: скорость реакции, глубина сопровождения и дополнительные опции



Сроки контрактования

- Типовое подключение — от 1 недели
- Срок контрактования — от 3 месяцев



**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Защищенный доступ к веб-ресурсам ГОСТ TLS

Внедрение и поддержка защищенного взаимодействия с веб-ресурсом заказчика с использованием российской и зарубежной криптозащиты

Защищенный доступ к веб-ресурсам (ГОСТ TLS)

Внедрение и поддержка защищенного взаимодействия с веб-ресурсом заказчика с использованием российской и зарубежной криптозащиты

[Подробнее на сайте](#)

Риски бизнеса

- Ужесточение нормативов использования отечественной криптографии для веб-сайтов КИИ, ПДн и госорганов
- Зарубежные сертификаты уязвимы к санкционным ограничениям и геополитическим рискам
- Из-за незащищенного взаимодействия пользователей с сайтом вы несете репутационные и финансовые потери
- Сложность внедрения ГОСТ – требуется сертифицированное оборудование СКЗИ КС1 и квалифицированные специалисты

Решение

- Полное соответствие требованиям ФСБ России, ФСТЭК России и нормам 152-ФЗ и 187-ФЗ
- Запасной канал доступа – ГОСТ TLS работает параллельно с RSA, исключая риски блокировки
- Управление сертификатами силами Solar MSS – получение, установка и ротация ГОСТ-сертификатов специалистами провайдера
- Внедрение под ключ – Solar MSS обеспечивает настройку, мониторинг и эксплуатацию 24/7

Ключевые факты

Гибридная криптография RSA+ГОСТ

Одновременная поддержка западных и российских сертификатов обеспечивает доступность для всех браузеров

Три варианта реализации

Облако ГК «Солар», ЦОД, on-premise у заказчика – под любые требования безопасности и инфраструктуры

Сертифицированное ФСБ России

В сервисе используется оптимальный для защиты веб-трафика класс криптографической защиты – не ниже КС1

24/7 администрирование

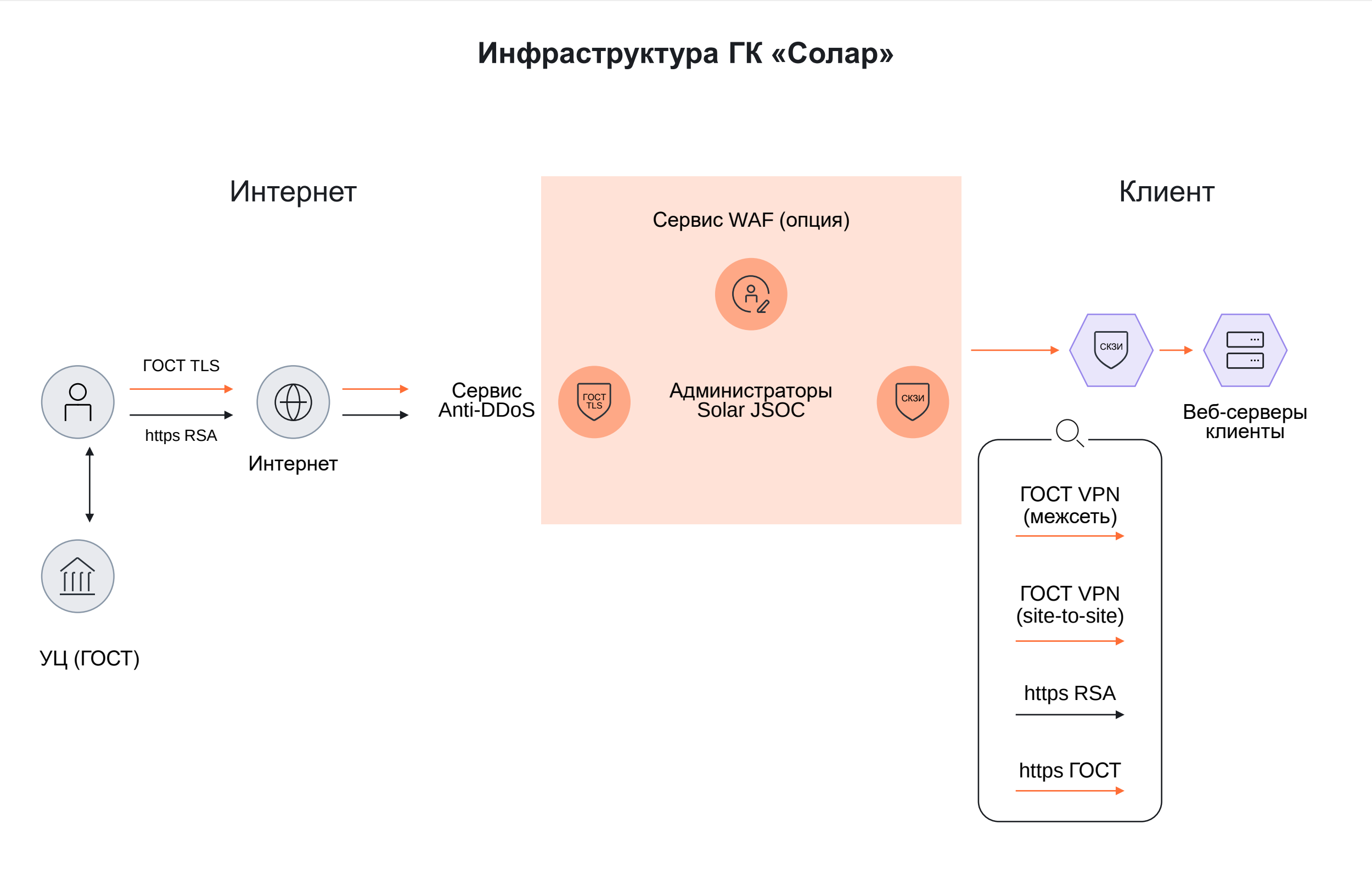
Полный цикл эксплуатации – Solar MSS осуществляет круглосуточный мониторинг, ротацию сертификатов и реагирование на инциденты

Технологии

Предоставляемые в составе сервиса СКЗИ поддерживают:

- актуальные российские криптоалгоритмы ГОСТ 28147-89, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
- Различные версии протокола TLS 1.1 и 1.2

Схема реализации сервиса на инфраструктуре ГК «Солар»



Варианты предоставления сервиса

- 1. ГОСТ VPN (межсеть)
- 2. ГОСТ VPN (site-to-site)
- 3. https RSA / ГОСТ

Метрики тарификации

- Сценарий реализации: инфраструктура ГК «Солар», внешний ЦОД, on-prem у заказчика
- Максимальное количество запросов к веб-ресурсу в секунду, RPS
- Тип защиты канала до веб-ресурса

Сроки контрактования

- Типовое подключение — от 1 месяца (зависит от объема работ)
- Срок контрактования — от 1 года

Запросить консультацию

Шифрование каналов связи ГОСТ VPN

Построение и эксплуатация защищенных сетей
с использованием сертифицированных СКЗИ



Шифрование каналов связи (ГОСТ VPN)

Построение и эксплуатация защищенных сетей между геораспределёнными объектами с использованием российских криптографических алгоритмов

[Подробнее на сайте](#)

Риски бизнеса

- Перехват и утечка конфиденциальной информации при передаче по открытым каналам связи
- Несоответствие требованиям регуляторов к защите информации государственных информационных систем (ГИС), персональных данных (ПДн) и КИИ
- Высокие капитальные затраты на закупку и обслуживание оборудования защиты
- Дефицит квалифицированных специалистов по криптографической защите и сложность масштабирования

Решение

- Надежное шифрование данных ГОСТ-алгоритмами с сертификацией ФСБ России
- Полное соответствие требованиям ФСБ России, ФСТЭК России и нормам 152-ФЗ и 187-ФЗ
- Сервисная модель оплаты без приобретения оборудования и лицензий
- Профессиональная круглосуточная поддержка и быстрое масштабирование сети

Ключевые факты

Соответствие требованиям регуляторов

Использование сертифицированных СКЗИ на всем жизненном цикле

Защищенный контур управления

Аттестация по высшему классу защиты — УЗ-1 и К1

Быстрое подключение и масштабирование

Оперативное реагирование на изменения в бизнесе — подключение новых филиалов

Оплата только потребляемого сервиса

Снижает капитальные затраты, переводит расходы в операционные, делает их предсказуемыми

Нам доверяют

[Истории внедрений](#)

Шаги внедрения

Варианты подключения

Оператор связи — ПАО «Ростелеком»

Подключение сервиса к существующим каналам связи или создание новых, защищенных сервисом

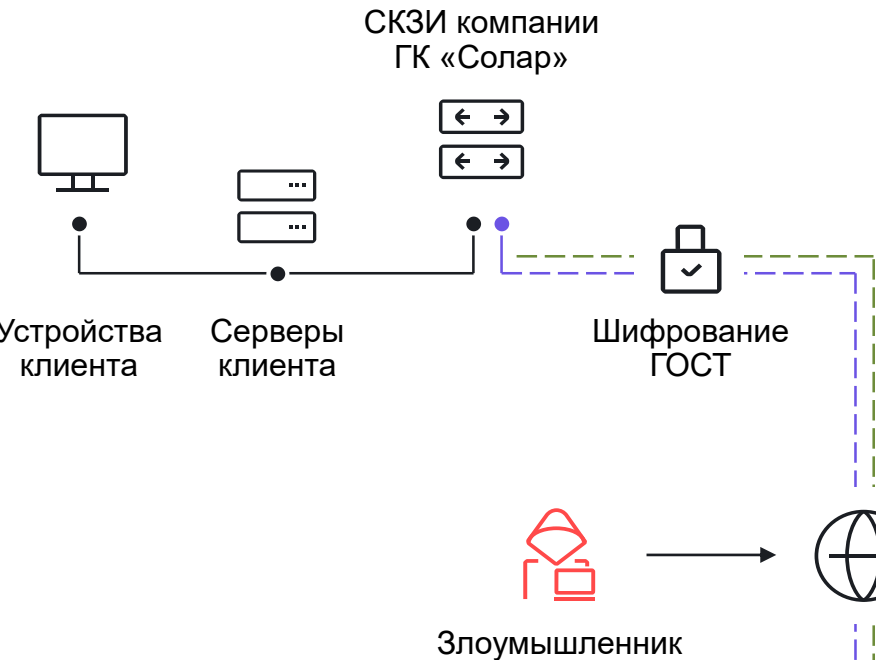
Другие операторы связи

Оказание сервиса на каналах стороннего оператора

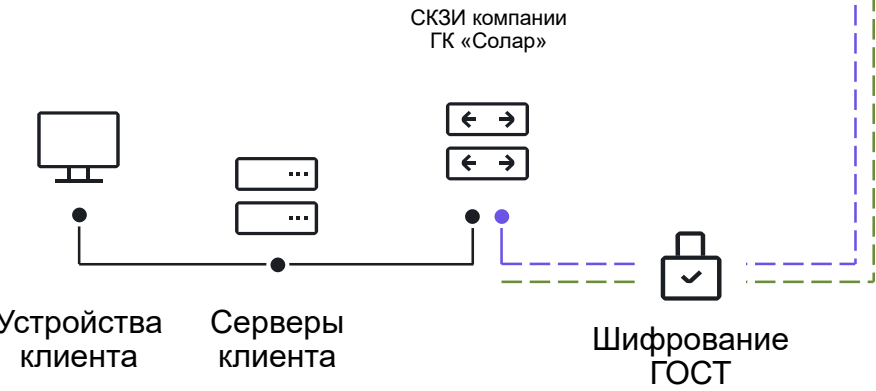
Варианты предоставления сервиса

- 1. Защита с помощью оборудования сервис-провайдера
- 2. Администрирование оборудования клиента

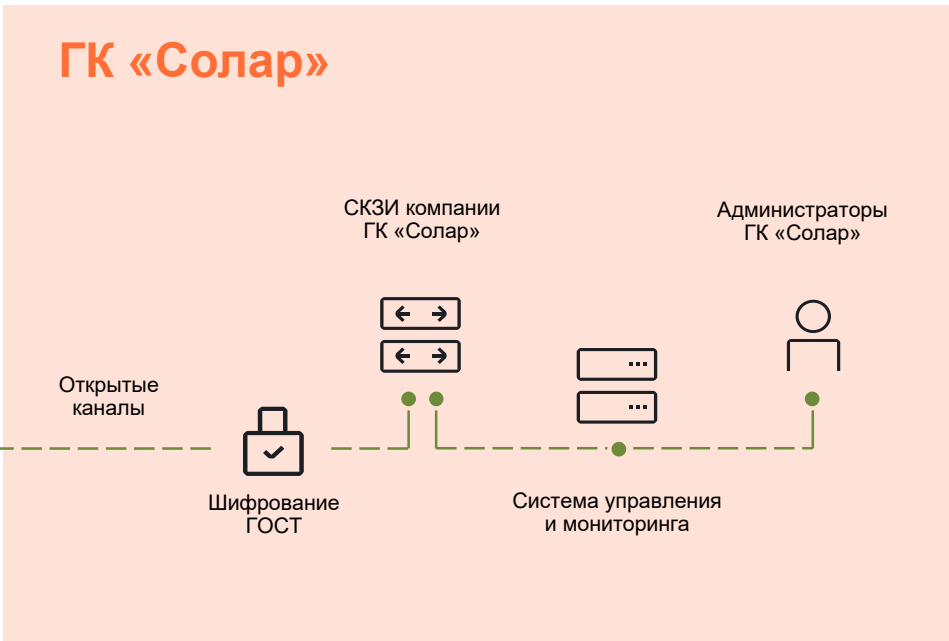
Центральный офис клиента



Филиал клиента



Платформа ГОСТ VPN Аттестованный сегмент



- Нешифрованный трафик
- - - Защищенный трафик клиента
- - - Защищенный трафик управления

Шаги внедрения

Метрики лицензирования

- Перечень объектов с пропускной способностью каналов
- Требования по резервированию
- Дополнительные пожелания: динамическая маршрутизация, межсетевое экранирование и т. д.



Сроки контрактования

- По подписке на 12–36 месяцев
- Включены: вендорская ТП и обновление версий СКЗИ
- Администрированием и учетом СКЗИ занимаются эксперты ГК «Солар»



**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Сервис защиты от сетевых угроз Unified Threat Management (UTM)

Построение и эксплуатация защищенных сетей
с использованием сертифицированных СКЗИ

Сервис защиты от сетевых угроз (UTM)

Защищенный выход в интернет под контролем экспертов центра противодействия кибератакам ГК «Солар» по подписке

[Подробнее на сайте](#)

Риски бизнеса

- Защитить внутреннюю сеть компании от сетевых сканеров, вирусов, троянов и вредоносного ПО
- Гибко подстраивать защиту под потребности бизнеса: корректировать количество офисов, ширину каналов связи и т.п.
- Не тратить время и деньги на выбор и установку дорогостоящих средств защиты (NGFW и т.п.)

Решение

- Надежные средства защиты под управлением экспертов отрасли
- Оплата только потребляемого сервиса, возможность корректировки параметров
- Готовое решение по сервисной модели

Ключевые факты

Экономическая эффективность

Сервисная модель позволяет производить оплату ежемесячно, снижая капитальные затраты.

Централизация

Единая точка выхода в интернет обеспечивает централизованную защиту всей инфраструктуры без развертывания отдельных средств защиты в каждом офисе.

Эксплуатация сервиса в режиме 24/7

Обеспечение бесперебойного предоставления полного цикла сервиса

Нам доверяют



Калмыцкий
государственный университет
имени Б.Б. Гордовикова



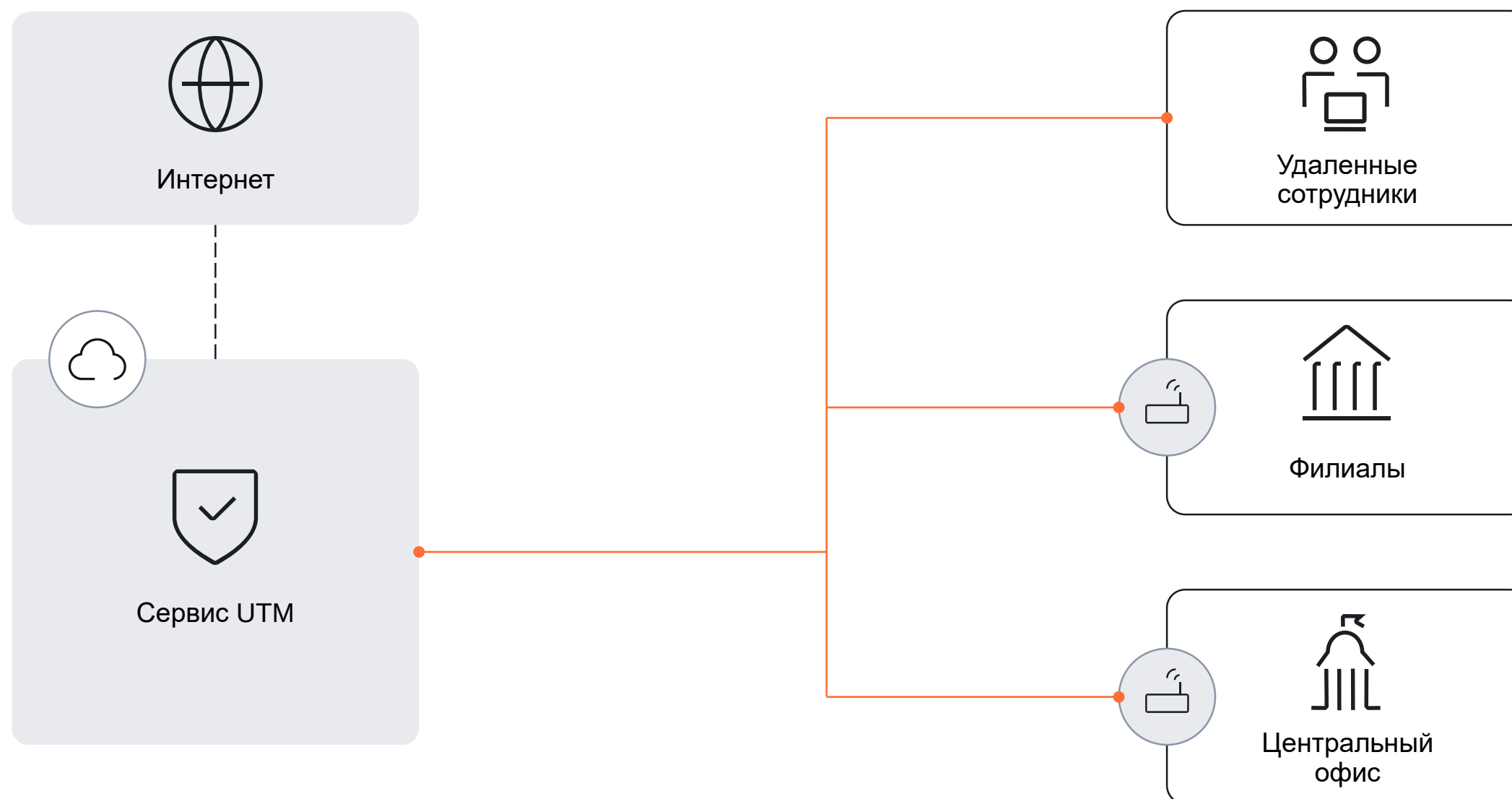
Как это работает

— Выделенный канал ПАО «Ростелеком»
или защищенный туннель через интернет

— — — Централизованный выход в интернет



Оборудование ГК «Солар»
(только для подключения через интернет)



Реализовать защиту просто

- Между ресурсами компании и любым интернет-провайдером разместим оборудование ГК «Солар».
- Для выделенных каналов связи ПАО «Ростелеком» установка оборудования не требуется.
- Создается единая точка выхода в интернет для всех площадок, а площадки образуют защищенную корпоративную сеть.

Подходит для компаний с разной структурой

- Одна площадка, десятки или даже сотни
- Есть удаленные сотрудники или нет
- Есть сотрудники, отвечающие за безопасность на площадках, или нет

Запросить консультацию

Расследование и реагирование на инциденты (DFIR)

Помощь от команды Solar 4RAYS
в отражении атак любой сложности



Помощь в отражении атак любой сложности

Противодействие и предотвращение

Кейсы расследований Solar 4RAYS

Вызовы бизнеса

- **Рост числа атак**
Атакуют все отрасли.
Скорость отражения атак влияет на масштаб ущерба от последствий атаки
- **Прямой ущерб от атак**
Атаки шифровальщиков, утечки данных, уничтожение инфраструктуры приводят к остановке бизнеса, штрафам, оттоку клиентов
- **Финансовые потери от простоя после атак**
Если задеты бизнес-процессы, то компания недополучает прибыль из расчета:

Цена простоя = [t простоя] × [затраты^{в мин.}]

Решение

Расследование и реагирование на инциденты (DFIR)

Когда привлекать команду реагирования:

- Множественные срабатывания систем защиты информации
- Потеря доступа к информационным ресурсам
- Появление неучтенных административных записей
- Заражение ВПО*
- Целенаправленные атаки
- Хищение данных
- Компрометация учетных данных
- И другие

Ключевые факты

Экспертиза отражения атак

300+ расследований атак различной сложности
+10 лет опыта

Всегда актуальные знания об угрозах

Доступ к крупнейшей в РФ базе знаний киберугроз Центра исследований Solar 4RAYS

Техническое сопровождение

Возможность подключения Solar JSOC к инфраструктуре.
Подготовка к отсечению доступа злоумышленнику

Наш опыт

Финансы

Телеком

Госсектор

Транспорт

Промышленность

ИТ

Медицина

Нефтегаз

Другие

Как работает расследование и реагирование на инциденты (DFIR)

Порядок проведения работ

- 01

Первичная оценка ситуации

Сбор данных для первичной оценки степени компрометации инфраструктуры и компетенций злоумышленника
- 02

Разработка плана действий

- Уточнение области атаки и профиля злоумышленника
 - Включение дополнительного логирования событий и/или подключение инфраструктуры к сервису «Мониторинг и анализ инцидентов» Solar JSOC
- 03

Устранение первичных последствий атаки

- Изоляция скомпрометированных ресурсов
 - Сбор данных — снятие дампов памяти, копирование содержимого носителей, выгрузка логов — для дальнейшего анализа и уточнения последствий атак
- 04

Восстановление бизнес-процессов

Координирование активностей по устранению последствий атаки и возобновлению штатного режима работы компании
- 05

Устранение первичных последствий атаки

- Описание хронологии проведения атаки, предпринятых по ее локализации и нейтрализации последствий шагов
 - Предоставление рекомендаций по недопущению повторения сценария кибератаки

Ключевые задачи и цели работ

Локализация инцидента и возврат контроля

- Выявление скомпрометированных ресурсов и каналов управления ими
- Изоляция нарушителя с целью предотвратить компрометацию незатронутых инцидентом систем
- Выдворение нарушителя из инфраструктуры, удаление следов его инструментария

Подготовка к восстановлению ИТ-инфраструктуры

Сбор необходимых для проведения расследования данных, помощь специалистам заказчика

Предотвращение повторения инцидента

Формулирование рекомендаций по недопущению повторных инцидентов

Форматы реагирования на инциденты

Исследование и реагирование на инциденты (DFIR)

- Разовое соглашение
- Старт работ с момента обращения — в порядке очереди
 - Постоплата

Подписка на реагирование на инциденты (RETAINER)

- Подписка на 1-2 года от 250 часов*
- Старт работ с момента обращения — не более 2 часов
 - Обмен неиспользованных часов на 6 услуг, сервисов
 - Цена ниже до 30%, предоплата 100%

* Например, 250 часов хватит для расследования 2 базовых инцидентов

Запросить консультацию

Выявление следов компрометации (Compromise Assessment)

Обнаружение признаков присутствия злоумышленников
в инфраструктуре до наступления последствий



Выявление следов компрометации

Обнаружение признаков присутствия злоумышленников в инфраструктуре до наступления последствий

Кейсы расследований Solar 4RAYS

Вызовы бизнеса

- **Рост числа атак**
Атакуют все отрасли. Скорость отражения атак влияет на масштаб ущерба от последствий атаки
- **Прямой ущерб от атак**
Атаки шифровальщиков, утечки данных, уничтожение инфраструктуры приводят к остановке бизнеса, штрафам, оттоку клиентов
- **Финансовые потери от простоя после атак**
Если задеты бизнес-процессы, то компания недополучает прибыль из расчета:

Цена простоя = [t простоя] × [затраты^{в мин.}]

Решение

Выявление следов компрометации (Compromise Assessment)

Когда привлекать команду реагирования:

- Множественные срабатывания систем защиты информации
- Появление неизвестных процессов, аномалии в сетевом трафике
- Подтвержденный инцидент в смежных инфраструктурах (ДЗО, подрядчик и т. д.) или в частях инфраструктуры, не имеющих сетевой связности с основной (сайт на внешнем хостинге и т. д.)
- Периодическая проверка с целью раннего выявления атак

Также в случае поглощения нового актива в рамках M&A-сделок

Ключевые факты

Экспертиза отражения атак

300+ расследований атак различной сложности +10 лет опыта

Всегда актуальные знания об угрозах

Доступ к крупнейшей в РФ базе знаний киберугроз Центра исследований Solar 4RAYS

Техническое сопровождение

Возможность подключения Solar JSOC к инфраструктуре. Подготовка к отсечению доступа злоумышленнику

Наш опыт

Финансы

Телеком

Госсектор

Транспорт

Промышленность

ИТ

Медицина

Нефтегаз

Другие

Как работает Compromise Assessment

Порядок проведения работ

- 01

Оценка доступности и релевантности инструментов и данных, необходимых для успешных работ

- Политики и регламенты в том числе доменные политики, политики управления доступом и т. п.
 - Топология сети, системные и прикладные журналы
 - Файлы реестров, дампы памяти, временные файлы, жесткие диски и т. п.
- 02

Сбор данных для анализа

- Исследование доступных инструментов и данных (см. этап 1)
 - Реверс-анализ ВПО — функционал, уникальность ВПО, методы сокрытия и обхода средств защиты
 - Ретроспективный анализ хостов, на которых были обнаружены индикаторы компрометации
- 03

Разработка рекомендаций

Гипотеза о компрометации подтвердилась:

Рекомендации по выдворению нарушителя и устранению следов компрометации

Гипотеза о компрометации не подтвердилась:

Рекомендации по повышению устойчивости инфраструктуры заказчика к инцидентам

Что вы получите

Проверку гипотезы о компрометации инфраструктуры

Выявление признаков нападения и следов прошедших атак

Предотвращение развития атаки в случае подтверждения гипотезы

Определение масштаба компрометации и разработка мер по защите инфраструктуры

Аналитический отчет для руководителей и инженеров

Заключение о состоянии инфраструктуры и рекомендации по ее укреплению

Форматы реагирования на инциденты

Выявление следов компрометации (Compromise Assessment)

- Разовое соглашение
- Старт работ с момента обращения — в порядке очереди
 - Постоплата

Подписка на реагирование на инциденты (RETAINER)

- Подписка на 1-2 года от 250 часов*
- Старт работ с момента обращения — не более 2 часов
 - Обмен неиспользованных часов на 6 услуг, сервисов
 - Цена ниже до 30%, предоплата 100%

* Например, 250 часов хватит для расследования 2 базовых инцидентов

Запросить консультацию

Подписка на реагирование на инциденты (Retainer)

- Реагирование на инциденты 24/7
- Экспертиза от Solar 4RAYS



Подписка на реагирование на инциденты (Retainer)

Безопасность без пауз: реагирование на инциденты 24/7

Кейсы расследований Solar 4RAYS

Вызовы бизнеса

- **Рост числа атак**
Атакуют все отрасли. Скорость отражения атак влияет на масштаб ущерба от последствий атаки
- **Непредсказуемость атак. Дефицит персонала**
Сложность планирования бюджета на привлечение внешних команд и дополнительных ресурсов
- **Финансовые потери от простоя после атак**
Если задеты бизнес-процессы, то компания недополучает прибыль из расчета:

Цена простоя = [t простоя] × [затраты^{в мин.}]

Решение

Подписка (RETAINER)

от 250 часов

Предоплаченного объема работ команды реагирования

Срок подписки

1 и 2 года

6 услуг, сервисов

Доступных взамен неиспользованных часов подписки

Ключевые факты

Экспертиза отражения атак

300+ расследований, 10+ лет опыта. Выявляем следы хакеров до наступления последствий атаки

Спокойствие с выгодой

Цена ниже* до 30%. Доступ к другим сервисам и услугам взамен непотраченных часов

* Относительно других форматов приобретения сервиса по реагированию на инциденты

Скорость реагирования

Документы уже подписаны, есть SLA и команда знает инфраструктуру для быстрого старта работ

Наш опыт

Финансы

Телеком

Госсектор

Транспорт

Промышленность

ИТ

Медицина

Нефтегаз

Другие

Возможности подписки на реагирование на инциденты (Retainer)

Порядок проведения работ

- 01

Выбрать вариант подписки

Например, 250 часов хватит для расследования 2 базовых инцидентов
- 02

Выбрать состав подписки. Подписать соглашение

В соглашении будут указаны основные и дополнительные работы, которые можно будет провести в рамках подписки
- 03

Погрузить в детали команду реагирования

Знакомство с командой защиты заказчика и с защищаемой инфраструктурой
- 04

Привлечь команду Solar 4Rays к работам до конца действия подписки

- Увеличение часов на период подписки с шагом в 50 часов
 - При продлении подписки доступен перенос до 15% неиспользованных часов*
- 05

Продление подписки по договоренности

На срок 1, 2 года от 250 часов

* В случае продления подписки на реагирования на момент действия текущей подписки

Доступные работы в рамках подписки

Основные

- Расследование и реагирование на инциденты (DFIR)
- Локализация инцидента и возврат контроля
 - Помощь в восстановлении бизнес-процессов
 - Повышение устойчивости к инцидентам

Дополнительные

- Выявление следов компрометации (Compromise Assessment)
- Информирование о компрометации подрядчиков и самого заказчика в течение года
- Анализ ВПО или сетевого трафика

Варианты подписки

- 1 год – 250, 375, 500 часов и более
- 2 года – 500, 625, 750 часов и более

Уменьшите риски от последствий атак

Высокая скорость реагирования за счет предварительного знакомства с инфраструктурой и SLA

Сэкономите ИБ-бюджет

Стоимость расследований ниже относительно других форматов приобретения сервиса

Инвестируете в устойчивость бизнес-процессов

Прогнозируемые расходы на расследование инцидентов и своевременное отражение атаки

Запросить консультацию

Тестирование на проникновение инфраструктуры



Экспертные услуги

Тестирование на проникновение (пентест)

Детальное исследование, включающее поиск критичных уязвимостей и моделирование действий злоумышленника, для оценки защищенности организации

[Подробнее на сайте](#)

Вызовы бизнеса

- Рост и развитие угроз кибербезопасности
- Необходимость соответствия требованиям законодательства РФ по ИБ
- Увеличение штрафов за утечку персональных данных – 3% от годовой выручки компании или 500 млн руб.
- Смена команды информационной безопасности
- Повышение осведомленности сотрудников в вопросах ИБ

Решение

- Выполнение требований регуляторов
- Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты
- Определение глубины возможного проникновения злоумышленника и рисков для критически важных данных и процессов
- Получение представления о векторах атак и наиболее вероятных путях проникновения киберпреступников

> 20 лет

На рынке ИБ

> 3290

Реализованных проектов

Сертификация

Подтверждение квалификации на международном уровне (OSCP+, OSWE, OSWP, CEN, CRT0, OSEP, OSCE, BSCP, CompTIA_Pentest+)

Портфолио

Среди клиентов – крупнейшие в РФ банки, ИТ-компании, медиахолдинги, ритейлеры федерального значения и промышленные компании

Соответствие законам РФ

Лицензия ФСТЭК на деятельность по ТЗКИ

Нам доверяют



Реализация проектов

Виды работ

- Тестирование внутренней инфраструктуры
- Тестирование внешнего периметра
- Анализ беспроводных сетей
- Социальная инженерия
- Нагрузочное DDoS-тестирование
- Тестирование CI/CD-конвейеров
- Тестирование K8s-кластера
- Тестирование частного облака
- Тестирование SOC: Red Team, Purple Team

Возможен комплексный анализ защищенности инфраструктуры

Этапы пентеста ИТ-инфраструктуры

1. Сбор информации
2. Анализ инфраструктуры на наличие уязвимостей
3. Проведение тестирования, проверка возможности реализации сценариев на практике
4. Анализ результатов, формирование детального отчета и рекомендаций

Содержание отчета

- Список обнаруженных уязвимостей с указанием критичности и описанием способов эксплуатации
- Описание векторов атак — реализованных и потенциальных
- Рекомендации по устранению уязвимостей и повышению уровня защищенности инфраструктуры

Преимущества

- Реализация проектов для компаний из различных отраслей
- Собственные программные разработки
- Рекомендации от сертифицированной команды с опытом свыше 20 лет и более 2900 проведенных работ

Ценообразование

Стоимость рассчитывается для каждого заказчика индивидуально на основе трудозатрат, необходимых для его проведения.

Трудозатраты оцениваются на основе данных, предоставленных заказчиком в опросном листе:

- Детализация задач клиента
- Подробное описание инфраструктуры
- Ожидаемые сроки реализации проекта (от 14 дней в зависимости от объема работ)

**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Анализ защищенности приложений

Экспертные услуги



Анализ защищенности приложений

Поиск максимального количества эксплуатируемых уязвимостей, недостатков клиентской и серверной частей любых типов приложений

Подробнее на сайте

Вызовы бизнеса

- Рост числа уязвимостей элементов информационной системы, приводящие к утечкам данных, вмешательству в бизнес-процессы и проведению несанкционированных действий
- Приложения, взаимодействующие с другими компонентами системы, которые в случае атаки ставят под угрозу не только обрабатываемые данные, но и ИТ-инфраструктуру компании
- Увеличение штрафов за утечку персональных данных – 3% от годовой выручки компании или 500 млн руб.

Решение

- Оценка защищенности информационных систем, обеспечение защищенности приложений и стабильности бизнес-процессов
- Выявление уязвимых компонентов приложений, сокращение рисков и предотвращение угроз ИБ
- Определение возможных путей развития атаки на ИТ-инфраструктуру

> 20 лет

На рынке ИБ

> 3290

Реализованных проектов

Сертификация

Подтверждение квалификации на международном уровне (OSCP+, OSWE, OSWP, CEN, CRT0, OSEP, OSCE, BSCP, CompTIA_Pentest+)

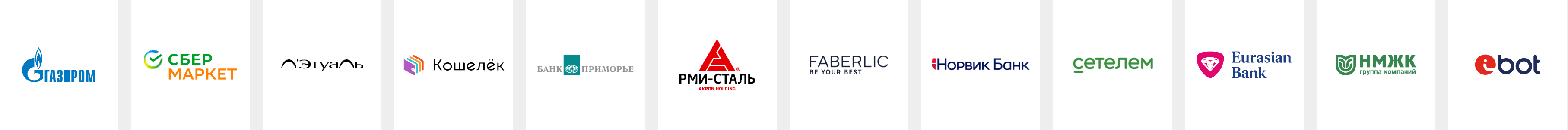
Портфолио

Среди клиентов – крупнейшие в РФ банки, ИТ-компании, медиахолдинги, ритейлеры федерального значения и промышленные компании

Соответствие законам РФ

Лицензия ФСТЭК на деятельность по ТЗКИ

Нам доверяют



Реализация проектов для всего спектра приложений

Виды работ

- Анализ веб-приложений
- Анализ мобильных приложений
- Анализ десктоп-приложений
- Анализ бизнес-приложений (CRM, ERP и др.)
- Анализ операционных систем (ОС)
- Анализ средств защиты информации (СЗИ)
- Анализ кода

Когда проводить анализ защищенности

- при первичной установке информационной системы
- при публикации новой версии используемой ИС
- при внесении существенных изменений в систему
- по прошествии длительного периода времени с последней проверки

Этапы работы по анализу защищенности

1. Сбор информации, ознакомление с функциональностью системы, анализ архитектуры, состава и характеристик программных средств и компонентов
2. Поиск уязвимостей и выявление угроз безопасности
3. Разработка сценариев, определение потенциальных векторов атак с дальнейшим развитием на инфраструктуру
4. Проверка возможности реализации сценариев на практике
5. Формирование детального отчета с результатами и рекомендаций

Преимущества

- Выявление проблемных областей на всех уровнях архитектуры приложения и определение возможных путей развития атаки.
- Перепроверка после исправления недочетов
- Рекомендации от сертифицированной команды с опытом свыше 20 лет и более 2900 проведенных работ

Ценообразование

Стоимость рассчитывается для каждого заказчика индивидуально на основе трудозатрат, необходимых для его проведения.

Трудозатраты оцениваются на основе данных, предоставленных заказчиком в опросном листе:

- Определение типа информационной системы (веб, десктоп, мобильное приложение);
- Подробное описание системы и методов анализа;
- Ожидаемые сроки реализации проекта (от 7 дней в зависимости от объема работ).

**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию



Услуги



Управленческий консалтинг

Комплекс услуг по организации системы ИБ, соответствующей реальным потребностям заказчика, актуальным вызовам внешней среды и требованиям законодательства



Стратегия информационной безопасности

Навигатор в мире кибербезопасности

Риски бизнеса

- Изменение бизнес-стратегии или сферы деятельности Компании
- Середина цикла реализации стратегии ИБ
- Внутренний конфликт между подразделениями ИТ и КБ, или внутри КБ, где нужно распределить обязанности
- Необходимость обоснованного распределения функций и обязанностей
- ИТ «перетягивает» одеяло на себя / выход из-под контроля службы ИТ и становление самостоятельной функцией

Решение

- Синхронизация целей и задач КБ со стратегическими целями Компании
- Оценка стратегических рисков и их финансового ущерба
- Анализ выполнения текущих задач и планов КБ и их актуализация
- Диагностика процессов, компетенций и модели управления КБ
- Архитектурный дизайн технологического ландшафта КБ
- Проектирование целевого состояния и дорожная карта развития КБ

Ключевые факты

Уникальный опыт

Консультирование ТОП компаний из RAEX-600

Экспертиза ген. архитектора и сервис проф. консалтинга

Сплав технарей и бизнес-консультантов

Подход к клиентам на высшем уровне

Интервью с топ-менеджерами ведущих компаний страны

Лучшие практики в основе методологии

- ГОСТ Р 57580
- ГОСТ Р ИСО/МЭК 2700x
- ГОСТ Р ИСО/МЭК 27002
- Требования регуляторов
- FFIEC
- NIST Cybersecurity Framework
- ISO/SAE 21434
- CIS 18 Critical Security Controls
- Solar CRF
- Иные стандарты (по запросу)

Нам доверяют



Основные шаги создания стратегии кибербезопасности



Построение и консалтинг SOC

Запуск и развитие собственного центра
противодействия кибератакам в сопровождении
архитектора комплексной безопасности



Построение и консалтинг SOC

Запуск и развитие собственного центра противодействия кибератакам в сопровождении архитектора комплексной безопасности

[Подробнее на сайте](#)

Вызовы бизнеса

- Большинство SOC не реализуют максимум своих возможностей
- Построение SOC с нуля — амбициозный процесс, в котором ИБ-отдел компании неизбежно сталкивается с чередой серьезных задач
- Отсутствие / недостаточный уровень мониторинга событий ИБ во время построения SOC

Решение

- Оценка зрелости SOC позволяет определить точки роста и раскрыть потенциал центра
- Архитектор комплексной безопасности — надежный партнер с широким многолетним опытом и выверенной в успешных проектах методологией
- Временное подключение к мониторингу Solar JSOC уже через 1–2 месяца после старта проекта

10+ лет

Эксплуатации крупнейшего коммерческого SOC в России

Вендоронезависимость

И максимальный охват технологий SOC

Опыт проектов

По построению и модернизации SOC федерального масштаба

Всегда актуальные знания

О техниках, тактиках и инструментах злоумышленников благодаря Solar 4RAYS

Об услуге

Верхнеуровневый состав услуг

- [Оценка зрелости SOC](#)
- Разработка концепции создания/модернизации центра
- Поставка лицензий и оборудования
- Проектирование и внедрение SIEM, NTA, EDR, IRP, проведение испытаний
- Разработка документов, содержащих описание процессов, положение о SOC и регламент деятельности центра ГосСОПКА, должностные инструкции, метрики/KPI, наборы плейбуков
- Автоматизация плейбуков
- Визуализация метрик и KPI
- Подбор и обучение персонала
- Дальнейшее масштабирование

Лицензирование

- Оценка зрелости: фиксированные тарифы*
- Концепция: фиксированные тарифы*
- Создание/модернизация: в зависимости от состава услуг / технических подсистем, масштабов SOC (на основе калькуляторов*), необходимости поставки лицензий
- Визуализация метрик/KPI: в зависимости от количества процессов и источников событий, необходимости поставки лицензий и выполнения работ по внедрению
- Обучение (как этап проекта создания/модернизации): в зависимости от количества обучающихся и места проведения

* Стоимость может отличаться в зависимости от масштабов существующего или планируемого SOC и количества выездов командированных сотрудников исполнителя на площадку заказчика. За информацией о фиксированных тарифах и калькулятором можно обращаться к Виталию Сиянову: v.siyanov@rt-solar.ru

Как попробовать решение

- Презентация услуг
- Демо (только для визуализации)
- [Оценка зрелости SOC](#) (платная услуга)
- Киберучения (платная услуга)

**Свяжитесь с вашим менеджером «Солара»
или оставьте заявку по QR-коду**

Запросить консультацию

