Ростелеком
Солар

Сервисы и решения Solar MSS

Обеспечиваем кибербезопасность по подписке.
Просто, выгодно, надежно.

rt.ru

rt-solar.ru

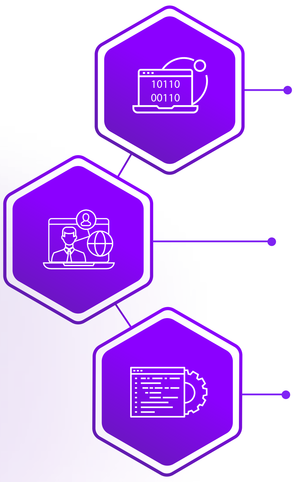
Содержание

Экосистема сервисов кибербезопасности по подписке

Solar MSS — крупнейшая в России экосистема сервисов кибербезопасности

Сервисы защищают от всего спектра угроз и решают комплексные задачи, позволяя компаниям сфокусироваться на основной деятельности. Эксперты «Ростелеком-Солар» осуществляют работы с учетом специфики региона, профиля, масштаба и потребностей каждой компании в режиме 24×7. Разнообразие технологий в составе экосистемы и партнерство с ведущими поставщиками ИБ позволяют предоставлять клиентам широкий выбор вариантов сервисов.

Сервисы Solar MSS объединены в экосистему на трех уровнях.



Технологический

Обмен информацией между сервисами и создание общих политик безопасности

Пользовательский

Единая точка взаимодействия с клиентом и визуализации работы

Аналитический

Оценка эффективности решения комплексных задач

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

Обеспечиваем кибербезопасность по подписке

Просто

От 2 дней
на подключение сервиса

70%
сервисов и решений подключаются без вмешательства в инфраструктуру

Выгодно

Гибкие тарифы
сервисов основаны на клиентском опыте

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

Надежно

Высокий уровень
подготовки экспертов по кибербезопасности

Ответственность
в рамках договорных обязательств, соответствие строгим SLA

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

Узнайте подробнее о сервисе

Онлайн-ресурсы стабильно защищены и остаются доступными круглосуточно

Сервис мониторинга трафика и защиты от DDoS-атак — это круглосуточная защита каналов связи и онлайн-ресурсов от атак для организаций любых регионов по подписке. Сервис нейтрализует даже самые сложные и массированные атаки и обеспечивает круглосуточную доступность интернет-ресурсов пользователям. Обработка трафика производится на территории России. Сервис доступен в рамках канала передачи связи «Ростелеком».

Статистика по угрозам DDoS-атак

В 2,5 раза
стало больше DDoS-атак на российские компании

Более 6 дней
длилась самая долгая из зафиксированных атак

33%
атакуемых — это органы государственной власти

Решаемые задачи

Круглосуточный мониторинг и отражение атаки в автоматическом режиме

Сервис анализирует трафик 24/7, и в случае подозрения на атаку трафик направляется в центр очистки. Это позволяет избежать недоступности ресурсов и остановки рабочих процессов

Доступность онлайн-ресурсов во время обработки трафика

Фильтрация атаки не влияет на доступность инфраструктуры, приложений и сервисов для пользователей. Архитектура сервиса выполнена с учетом механизма его отказоустойчивой реализации

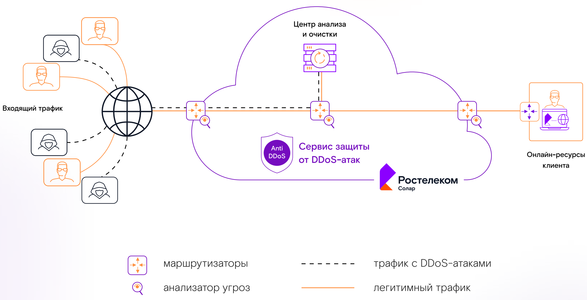
Отражение массированных атак

Сервис фильтрует атаки уровня L3/L4 объемом до 5 Тбит/с, что позволяет отражать массированные атаки, многократно превышающие самые сильные из зафиксированных в России

Защита от DDoS-атак для всех офисов и подведомственных организаций

Собственная защищенная магистральная сеть, охватывающая всю страну, обеспечивает простую масштабируемость при подключении новых офисов

Схема функционирования сервиса



Ключевые преимущества

Минимизация ложных срабатываний

Правила блокирования и мониторинга атак постоянно актуализируются, проводятся специальные исследования, разрабатываются сигнатуры для выявления атак в различных отраслях

Скорость очистки трафика

Веб-трафик на очистку перенаправляется за максимально короткое время — от 30 секунд до 1 минуты

Трафик доставляется без задержек

Доставка трафика в отсутствие DDoS-атаки до защищаемого ресурса происходит без изменения маршрутизации

Экспертная поддержка

Профилирование атак, консультации по принятию контрмер, а также техническую поддержку осуществляют специалисты «Ростелеком-Солар»

Защита от продвинутых угроз (Sandbox)

Узнайте подробнее о сервисе

Обнаружение ранее неизвестных угроз, обходящих базовые средства защиты, с экспертным сопровождением проектов

Сервис Sandbox — это защита корпоративной сети и сотрудников от ранее неизвестных киберугроз и сложных целевых атак. Анализируя почтовый и веб-трафики, сервис обнаруживает вредоносное ПО в реальном времени. Для использования продвинутой защиты здесь и сейчас не требуется закупки дорогостоящего оборудования и содержания штата профильных специалистов.

Статистика по продвинутым угрозам

На 30%

выросло количество атак, направленных на получение контроля над инфраструктурой

49%

событий информационной безопасности было выявлено с помощью сложных интеллектуальных средств защиты и анализа событий бизнес-систем

450 000

новых вредоносных программ появляется каждый день

Решаемые задачи

Круглосуточная защита сети и почты

Защита сетевого периметра и электронной почты от массовых атак, вирусов, фишинговых рассылок, скрытых и неизвестных угроз

Повышение уровня защищенности

Обеспечение необходимого уровня защищенности от неизвестных и скрытых киберугроз в сети для компании и филиалов

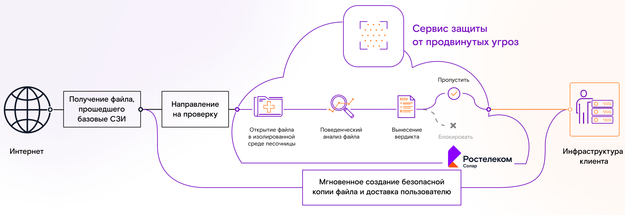
Оптимизация бюджета

Удобные прогнозируемые платежи равными частями, отсутствие капитальных затрат для начала использования сервиса

Сокращение трудозатрат

Снижение нагрузки и высвобождение времени ИБ-специалистов для решения стратегических задач за счет автоматизации процесса защиты сети и почты

Схема функционирования сервиса



Ключевые преимущества

Защита от техник обхода песочниц

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

Создание безопасной копии проверяемого файла без потери времени

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

Подробный анализ вредоносного кода и блокировка опасных объектов

Электронные письма проходят специальную проверку, которая позволяет обнаружить вредоносные объекты и блокировать опасные и подозрительные ссылки

Минимальные затраты на старте

При подключении сервиса не требуется закупка аппаратного решения, лицензий и подписки на обновления, которые необходимы при традиционной интеграции песочницы

Защита от сетевых угроз (UTM)

Узнайте подробнее о сервисе

Межсетевое экранирование, система обнаружения вторжений, контроль веб-трафика под управлением экспертов «Ростелеком-Солар»

Сервис защиты от сетевых угроз позволяет установить барьер между корпоративной сетью и внешними сетями, обеспечивает защищенный выход в интернет и применение единых правил безопасности. Сервис предотвращает сетевые угрозы и позволяет контролировать доступ сотрудников к веб-ресурсам. Анализ сетевой инфраструктуры, формирование правил защиты и их адаптация осуществляются экспертами «Ростелеком-Солар».

Решаемые задачи

Круглосуточная защита корпоративной сети

Внутренняя сеть компании защищена от сетевых сканеров, вирусов, троянов и вредоносного ПО. Предотвращается угроза использования корпоративной сети майнерами, торрент- и бот-сетями

Межсетевое экранирование и контроль приложений

Блокировка атак и фильтрация соединения осуществляется по заданным правилам разграничения доступа, активность которых можно отслеживать, изменять их, отключать и добавлять новые

Предотвращение вторжений

Сервис распознает вредоносную активность внутри сети или со стороны интернета, отслеживает и блокирует атаки в режиме реального времени

Антивирусная фильтрация трафика

Сервис обеспечивает антивирусную проверку веб-трафика без ущерба для производительности и быстродействия сети. Осуществляется мониторинг и блокировка подозрительных файлов

Схема функционирования сервиса на одной площадке

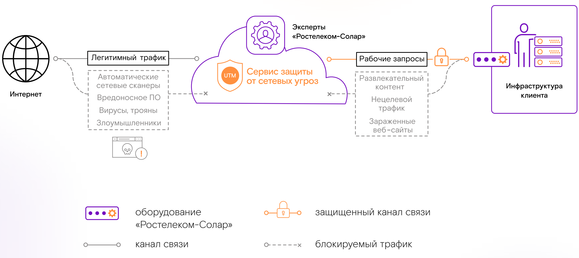
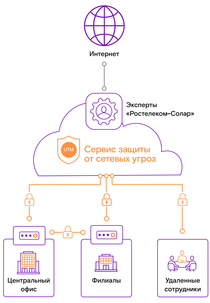


Схема функционирования сервиса на нескольких площадках



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

оборудование «Ростелеком-Солар» · защищенный канал связи · канал связи

Ключевые преимущества

Экспертиза провайдера

Подбор оптимального решения, своевременное обновление конфигурации и аппаратной части, а также техническая поддержка осуществляются специалистами «Ростелеком-Солар»

Контроль пользователей и сетевого трафика

Обеспечивает безопасность ИТ-инфраструктуры и соблюдение корпоративных политик, осуществляя контроль и мониторинг действий пользователей

Безопасный удаленный доступ

Сервис организует защищенный удаленный доступ пользователей к информационным системам организации с применением криптографических алгоритмов

Веб-фильтрация и проверка SSL- и SSH-трафика

Можно разрешить или запретить определенный контент с помощью настройки правил фильтрации контента. Сервис также проверяет SSL- и SSH-трафик на наличие угроз

Защита веб-приложений (WAF)

Узнайте подробнее о сервисе

Противодействие атакам на веб-приложения за счет эксплуатации многоступенчатых модулей защиты

Сервис защиты веб-приложений позволяет обеспечить надежную защиту корпоративных веб-сервисов, одновременно снизив издержки на персонал, оборудование и устранение последствий атак. Использование сервиса помогает клиентам развивать стратегию защиты веб-приложений и отвечать на появление новых угроз и кибератак.

Статистика по угрозам для веб-приложений

№1

веб-атаки — главный инструмент взломов среди профессиональных кибергруппировок

Каждые 39 секунд

совершается кибератака

57%

веб-приложений содержат критические уязвимости

Решаемые задачи

Быстрое и точное выявление основных угроз

ИБ-специалисты получают информацию не обо всех событиях кибербезопасности, а только о действительно важных

Расширенная защита от DDoS-атак уровня приложений

Сервис автоматически выполняет непрерывное профилирование поведения пользователей, что позволяет отслеживать аномалии, включая попытки совершить DDoS-атаки уровня L7

Защита от программ-роботов

Сервис оперативно обнаруживает автоматизированные атаки, нацеленные на кражу уникального контента или размещение несанкционированного контента, без блокировки поисковых ботов

Маскирование конфиденциальных данных

При использовании сервиса можно создавать правила определения чувствительных данных, которые применяются для маскировки секретной информации от третьих лиц

Схема функционирования сервиса

Ключевые преимущества

Оперативная актуализация политик ИБ и сигнатур уязвимостей

Для того чтобы противодействовать известным уязвимостям, осуществляется своевременное обновление политик безопасности и баз сигнатур уязвимостей

Контроль доступа к ресурсам

Позволяет контролировать доступ к защищаемым ресурсам для групп или отдельных пользователей с помощью формирования определенных правил

Минимизация рисков утечки информации

Сервис использует всестороннюю схему защиты для обеспечения максимальной безопасности, позволяет отражать атаки из списка OWASP Top 10 и автоматизированные атаки

Быстрое подключение защиты без значительных затрат

Оперативное подключение сервиса без остановки веб-приложений и без привлечения дополнительных специалистов по кибербезопасности

Шифрование каналов связи (ГОСТ VPN)

Узнайте подробнее о сервисе

Построение и эксплуатация защищенных сетей с использованием сертифицированных средств криптографической защиты информации (СКЗИ)

Сервис шифрования каналов связи защищает информацию при передаче по открытым каналам связи, обеспечивая конфиденциальность и целостность данных. Сервис позволяет организовать защищенное взаимодействие между георасределенными объектами в любом регионе и выполнить требования российского законодательства. В рамках сервиса ГОСТ VPN используются СКЗИ, сертифицированные ФСБ России.

Российское законодательство требует шифрования передаваемых данных в соответствии со стандартами, которые регулирует ФСБ России.

Решаемые задачи

Защита сетей

Данные надежно зашифрованы и остаются конфиденциальными при передаче между филиалами

Поддержка всех регионов в режиме 24/7

Оперативно подключаем и настраиваем оборудование в любых регионах России

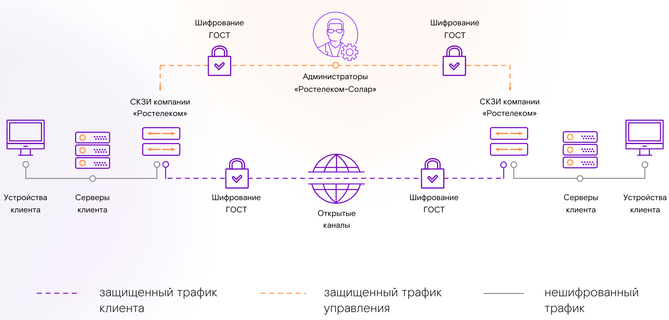
Сохранение работоспособности сети

За работоспособностью следит распределенная команда экспертов, обслуживающая 10 000 криптошлюзов

Оптимизация бюджетов

Сервис экономит ресурсы на закупку и обновление дорогостоящего оборудования

Схема функционирования сервиса на одной площадке



Ключевые преимущества

Знание специфики

Экспертиза и специализация «Ростелеком-Солар» по направлению шифрования каналов связи

Гибкость

Возможность подключения сервиса как отдельно от заключения договора на оказание услуг связи, так и вместе с ним

Удобство

Защита передаваемой информации не только между площадкой клиента и ЦОД оператора, но и между площадками клиента

Свобода выбора

Возможность выбора вендора решения, на котором будет организовано защищенное взаимодействие

Контроль уязвимостей (VM)

Узнайте подробнее о сервисе

Поиск и приоритизация уязвимостей с экспертными рекомендациями по их устранению

Сервис контроля уязвимостей направлен на поиск и учет информационных активов и оценку их уровня защищенности. На основе полученных в результате сканирования данных эксперты приоритизируют полученные данные, разрабатывают план и рекомендации по исправлению обнаруженных уязвимостей и проверяют выполнение данных рекомендаций.

Статистика по уязвимостям

Для 31%

известных уязвимостей доступны рабочие эксплойты

Более 1 миллиона

серверов в РФ до сих пор не защищены от атак типа WannaCry

94%

уникальных уязвимостей имеют уровень критичности выше среднего

Решаемые задачи

Выявление уязвимостей раньше злоумышленников

Приоритизация и своевременное устранение уязвимостей позволяют помешать хакерам проникнуть в ИТ-инфраструктуру и навредить бизнесу

Оценка защищенности решений подрядчиков

Выявление уязвимостей в сетевом периметре, ПО и ОС, которые поставляют подрядчики

Поиск теневых и забытых активов

Сервис помогает найти все активы в ИТ-инфраструктуре, чтобы гарантировать ее защиту

Приоритизация критичных уязвимостей

Эксперты «Ростелеком-Солар» готовят рекомендации по устранению найденных уязвимостей с учетом актуальных угроз кибербезопасности

Ключевые преимущества

Несколько скоринговых моделей оценки

Экспертные рекомендации строятся на основе методики приоритизации, позволяющей определить, какие уязвимости нужно устранить в первую очередь

Подробные рекомендации и контроль выполнения

Сотрудникам ИТ- и ИБ-отделов будет понятно, как именно устранять найденные уязвимости, а руководителям — отслеживать работу исполнителей

Экспертная обработка результатов сканирования

Специалисты «Ростелеком-Солар» приоритизируют все обнаруженные уязвимости и подготовят поэтапный план по их устранению

3 вида отчетов для разного уровня погружения

Отчеты о работе сервиса адаптированы под задачи исполнителей и руководителей и помогают им эффективно контролировать уязвимости

Управление навыками кибербезопасности (SA)

Узнайте подробнее о сервисе

Комплексное обучение сотрудников основам киберграмотности с экспертной поддержкой

Сервис управления навыками кибербезопасности обеспечивает комплексный подход к программе повышения осведомленности о киберугрозах и помогает сформировать у сотрудников навык обнаружения фишинговых атак и правильного реагирования на них. В ходе обучения клиенты получают техническую поддержку и консультации, а также подробный и понятный отчет о прогрессе обучения и тренировок сотрудников. Процесс обучения полностью сопровождается экспертами и состоит из обучающих курсов, тестов и практических тренировок.

Статистика по угрозам для веб-приложений

75%

сложных атак, реализуемых злоумышленниками, начинается с фишинга

39%

вредоносного ПО попадает в компанию через e-mail

74%

сотрудников переходят по ссылке или скачивают вредоносное вложение

Решаемые задачи

Обучение основам киберграмотности

Персонал знает, как безопасно себя вести в цифровом пространстве

Предотвращение фишинга

У сотрудников развиты устойчивые навыки реагирования на фишинговые атаки

Повышение осведомленности о цифровых угрозах

Персонал знаком с актуальными векторами кибератак и инструментами киберпреступников

Снижение вероятности утечек конфиденциальной информации

Сотрудники не попадаются на фишинговые атаки, злоумышленники не получают доступ к данным компании

Схема функционирования сервиса

Ключевые преимущества

Актуальные материалы

Для подготовки курсов и тренировочных рассылок используются актуальные сценарии фишинговых атак

Эффективное обучение

Сотрудники проходят интерактивное обучение с практическим закреплением знаний

Индивидуальный подход

В рамках сервиса доступны различные тематики курсов и возможна разработка новых

Поддержка экспертов

Оказываем техническую поддержку и сопровождение на протяжении всего процесса обучения

Защита электронной почты (SEG)

Узнайте подробнее о сервисе

Безопасная электронная почта с экспертной поддержкой по подписке

Сервис защиты электронной почты фильтрует нелегитимные письма, содержащие фишинг, спам и вредоносное ПО. Безопасные письма доставляются на устройства пользователей. Все технические работы – на нашей стороне. Вся необходимая для работы сервиса инфраструктура размещается на вычислительных мощностях «Ростелеком-Солар».

Статистика по фишингу и спаму

75%

сработавших сложных кибератак реализуются через фишинг

84%

входящих писем содержат спам

Решаемые задачи

Минимизация рисков атак с использованием электронной почты

Письма, содержащие фишинг и вредоносное ПО блокируются на этапе доставки, поэтому сотрудники не контактируют с опасными ссылками и вложениями

Избавление от спама в почтовом ящике

Спам-сообщения фильтруются с помощью комплекса алгоритмов и попадают карантин, чтобы не отвлекать сотрудников от работы

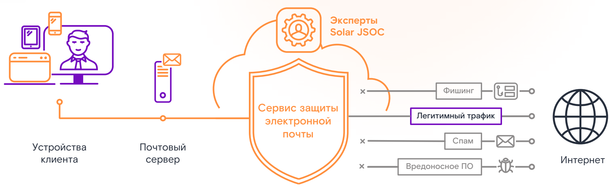
Защита сотрудников от вирусов и вредоносного ПО

Сервис распознает 99,9% типов вирусов и позволяет сотрудникам получать только безопасные письма

Оптимизация рабочего времени

ИТ- и ИБ-специалисты освобождаются от рутинных задач, связанных с обслуживанием защиты почты, и могут уделить время развитию бизнеса

Схема функционирования сервиса



Ключевые преимущества

Экспертная настройка

Благодаря тонко настроенным правилам фильтрации сотрудникам приходят только легитимные письма

Быстрая обработка

Алгоритмы защиты электронной почты обрабатывают входящие письма за десятки миллисекунд

Устойчивость к нагрузкам

Сервис работает даже при большой загрузке, проверяя до 1 000 000 писем в час

Круглосуточная поддержка

Техподдержка всегда на связи для решения вопросов или корректировки сервиса под изменившиеся бизнес-требования

Защита от фишинга и шифровальщиков

Узнать подробнее о решении

Комплексная защита с проверкой угроз на сетевом уровне

Решение позволяет блокировать фишинг и шифровальщики до попадания на компьютеры сотрудников и предотвращать попытки распространения в сети компании. Встроенные процессы обучения сотрудников реагированию на действия киберпреступников дополняют защитные средства и сводят к минимуму угрозы безопасности компании.

Статистика по фишингу и шифровальщикам

76%

доля атак с использованием фишинга

Каждые 11 секунд

компании заражают шифровальщиками

Решаемые задачи

Защита от любых типов фишинга и шифровальщиков

Комплексная защита почтового канала и периметра сети, дополненная проверкой подозрительных файлов в изолированной среде, помогает предотвратить действия киберпреступников

Индивидуальная адаптация политик, систем и процессов защиты

Средства защиты настраиваются с учетом особенностей инфраструктуры организации, существующих процессов и сценариев реагирования

Обучение сотрудников методам выявления и реагирования на фишинг

Регулярное повышение осведомленности и тренинги позволяют сотрудникам компании распознавать фишинг, не переходить по подозрительным ссылкам и не загружать вредоносное ПО

Снижение затрат на построение и эксплуатацию системы защиты

Совокупная стоимость владения комплексным решением ниже, чем при традиционной интеграции оборудования и последующей технической поддержке

Ключевые преимущества

Экспертиза «Ростелеком-Солар»

Наши специалисты полностью эксплуатируют решение по защите от фишинга и шифровальщиков, включая настройку политик и разработку правил блокирования новых массовых и таргетированных атак

Единая точка доступа

Для контроля работы решения доступны виджеты и отчеты, позволяющие получить актуальные данные в любое удобное время

Регулирование объема защиты

В рамках решения возможно выбрать необходимый уровень защиты в зависимости от бизнес-требований организации

Круглосуточная техническая поддержка

Выделенные линии технической поддержки и дежурная смена экспертов помогают решать вопросы пользователей в режиме 24/7

Защита онлайн-ресурсов

Узнать подробнее о решении

Бесперебойная доступность и защита онлайн-ресурсов компании

Решение для защиты онлайна — это комплексная многоступенчатая защита веб-ресурсов компаний от взломов и DDoS-атак, которая гарантирует безопасность и бесперебойную доступность ресурсов клиентам. Решение предоставляется по подписке и не требует капитальных затрат на закупку, внедрение и эксплуатацию оборудования, а также содержание штата ИБ-специалистов.

Статистика по угрозам для онлайн-ресурсов

77%

критических киберинцидентов в 1 квартале 2022 г. было связано с атаками на онлайн-ресурсы российских организаций

Решаемые задачи

Обеспечение доступности всех онлайн-сервисов и приложений

Решение позволяет избежать недоступности веб-ресурсов и приложений, поскольку анализ трафика и реагирование осуществляются круглосуточно

Защита веб-ресурсов компании от взломов и DDoS-атак

Во время сложных DDoS-атак на веб-ресурс или попытках взлома срабатывает межсетевой экран уровня приложений, который пропускает через себя весь трафик, а при обнаружении вредоносных запросов фильтрует его

Защита инфраструктуры и обеспечение непрерывности бизнес-процессов

В случае атаки на канал или ИТ-инфраструктуру решение производит очистку веб-трафика, при этом легитимные запросы пользователей пропускаются, тем самым обеспечивается непрерывность рабочих процессов

Снижение затрат на построение и эксплуатацию системы защиты

Совокупная стоимость владения комплексным решением ниже, чем при традиционной интеграции оборудования и последующей технической поддержке

Ключевые преимущества

Комплексный подход к решению актуальной задачи

Для защиты онлайн-сервисов и приложений и обеспечения их круглосуточной доступности легитимным пользователям достаточно подключить один продукт, который позволит реализовать данную задачу

Защита веб-ресурсов и приложений на всех уровнях

Решение защищает каналы и ИТ-инфраструктуру, где расположены онлайн-ресурсы, от DDoS-атак уровней L3/L4 и L7

Эксплуатация решения на стороне экспертов

Специалисты «Ростелеком-Солар» полностью эксплуатируют решение для защиты онлайна, включая его адаптацию под специфические веб-ресурсы компании, настройку правил защиты, своевременное обновление политик

Круглосуточная техническая поддержка

Выделенные линии технической поддержки и дежурная смена экспертов помогают решать вопросы пользователей круглосуточно в режиме 24/7

Преимущества сервисной модели

Доступность

Круглосуточный мониторинг и защита во всех часовых поясах без ограничений

Экономия

Отсутствие расходов на оборудование и персонал, перевод капитальных издержек в операционные

Надежность

Бесперебойная работа всех сервисов за счет резервирования данных и отказоустойчивости ЦОД

Экспертность

Эксплуатация и поддержка сервисов профессионалами с учетом актуального ландшафта и профиля киберугроз

Гибкость

Быстрое подключение сервисов с оплатой за понятный результат, масштабируемость на все офисы

Комплаенс

Лицензии ФСТЭК России, ФСБ России, взаимодействие с ГосСОПКА, сертифицированные решения

Подключить защиту просто

Вы оставляете заявку

Наши специалисты связываются с вами для обсуждения деталей

Вы получаете защиту, адаптированную под ваши задачи

Получите бесплатную экспертную консультацию

mss.rt-solar.ru

solar@rt-solar.ru