Сервис защиты от DDoS-атак

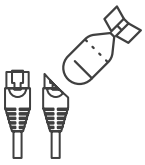
Постоянная доступность сетевой инфраструктуры, веб-приложений и онлайн-сервисов

- rt-solar.ru
- rt.ru

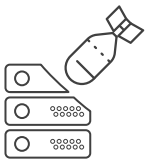
Ростелеком
Солар

Что такое DDoS-атаки

DDoS-атака — распределенная атака, направленная на нарушение доступности интернет-ресурсов за счет отправки вредоносных запросов, превышающих производительность оборудования. Для отправки этих запросов используются бот-сети из зараженных интернет-устройств или эксплуатируются уязвимости устройств глобальной сети.



Атаки на канал



Атаки на серверы
и сетевое оборудование

Атаки на приложения
и сервисы

Нарушение доступности может стать отправной точкой для развития комбинированной атаки, нацеленной на кражу конфиденциальной информации и персональных данных, заражение хостов или выведение из строя оборудования.

Дешевизна и распространенность инструментов для организации атак — причина роста количества DDoS-атак. Чаще всего атакуют представителей электронной коммерции и игровой индустрии.

95%
Рост количества атак

64%
Доля атак на сегмент
игровой индустрии

16%
Доля атак на сегмент
электронной коммерции

Источник: «Отчет о DDoS-атаках на российские компании в 2018 году», ПАО «Ростелеком»

Финансовые риски

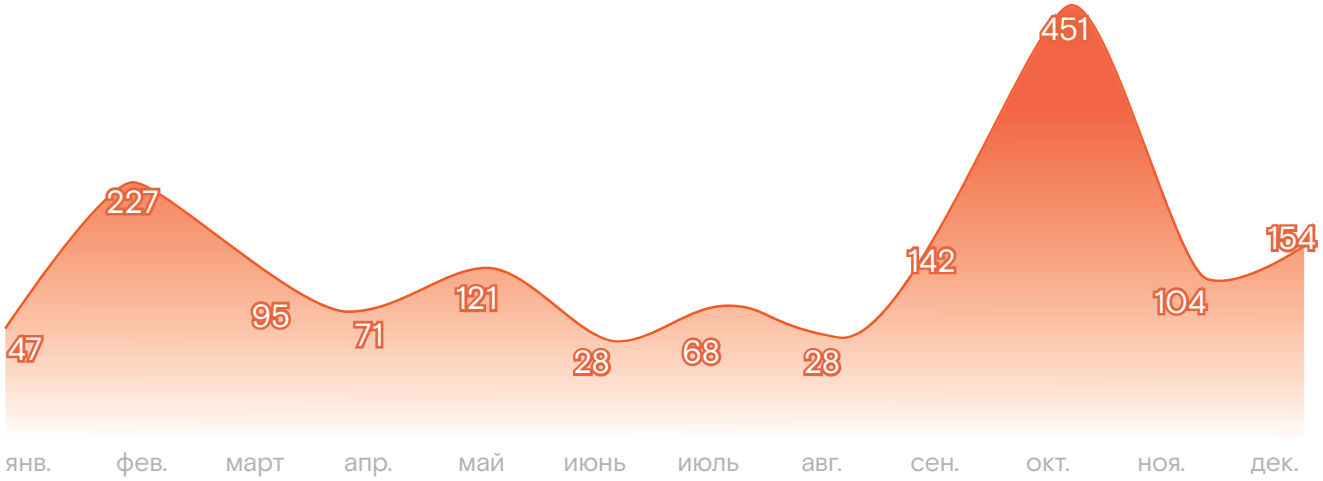
- Расторжение контрактов рекламодателями
- Потеря вложений на продвижение сайта
- Срыв сделок, отмена аукционов торговых площадок

Репутационные риски

- Падение биржевых индексов компании
- Снижение стоимости бренда
- Недоступность публичной корпоративной информации

Технологические риски

- Простой производства
- Потеря сотрудниками доступа к корпоративным приложениям



Интенсивность DDoS-атак в 2018 г. (Гбит/с), данные ПАО «Ростелеком»

Уникальность

360°

Сервис Anti-DDoS компании «Ростелеком-Солар» — это эшелонированная оборона от DDoS-атак. Он защищает **каналы, сетевую инфраструктуру** и **веб-ресурсы** компании.

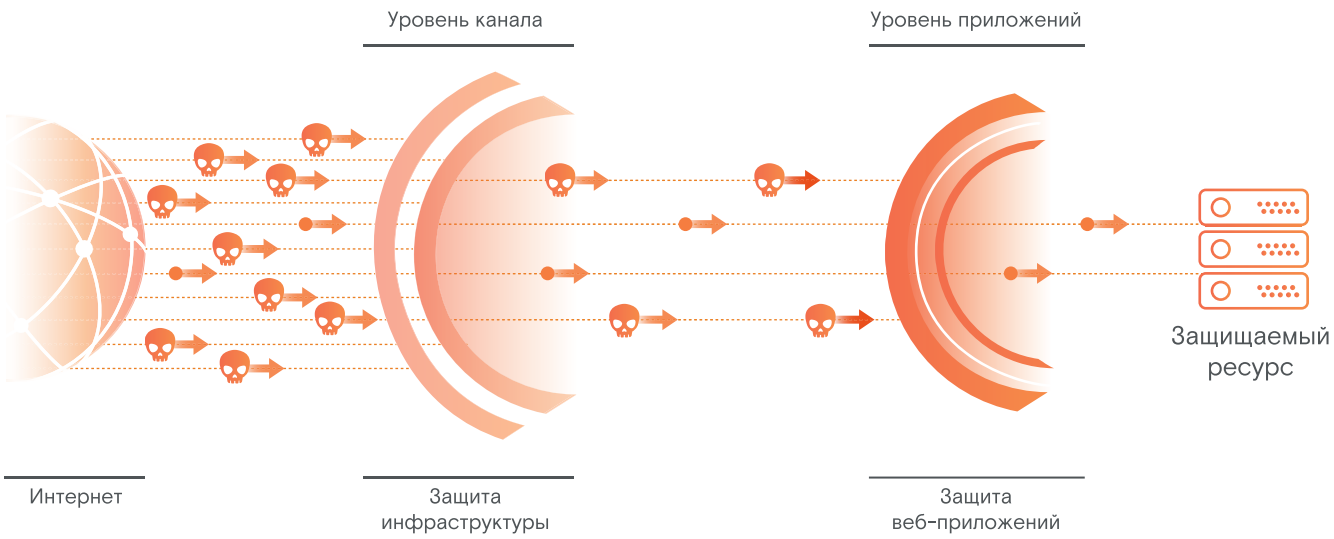
Фильтрация атак осуществляется многоступенчато, на всех уровнях модели OSI — от уровня канала до бизнес-логики приложения.

Доступность всех интернет-сервисов и приложений

Защита распределенной интернет-инфраструктуры на уровнях L3-L4 модели OSI

Защита веб-сайта компании, в том числе от атак уровня приложений

Схема работы



Ключевые особенности

Доставка трафика в отсутствие атаки до защищаемого ресурса **без изменения маршрутизации**

WAF Сервис защиты веб-приложений

Отсутствие дополнительных платежей за количество и максимальную полосу атак

- Возможность предоставления **чистого канала** — **защита** от DDoS-атак **всех интернет-приложений клиента**
- Защита от атак на IP-адрес ресурса (Direct to Origin) **без дополнительных затрат на выделенный канал**
- Фильтрация атак уровня **L3-L4** полосой **5+ Тбит/с** и атак уровня **L7** — полосой **300+ Гбит/с**
- Возможность предоставления CDN — **ускорение веб-сайта**
- Опыт защиты крупных проектов **(Олимпиада в Сочи)**
- **Простая масштабируемость** для подключения новых офисов
- Обработка трафика **на территории России**

+ Благодаря георасределенной платформе сервис доступен организациям со сложной инфраструктурой, подключенной к **любым интернет-провайдерам.**

Нас выбрали

Более 250 крупных российских компаний выбрали защиту компании «Ростелеком-Солар»
Среди них — государственные организации, банки, страховые компании, телеком-провайдеры, представители электронной коммерции и игровые сервисы.

Преимущества сервисной модели

Экономия и эффективность

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

Устранение дефицита кадров
Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов.

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

Профессиональная команда
Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли.

Технологичность и надежность

Доступность
Защита и мониторинг 24 часа в сутки без перерывов и выходных.

Надежность
Эксплуатация распределенной отказоустойчивой инфраструктуры.

Гибкость
Простая масштабируемость и быстрое изменение параметров услуги.

Скорость
Быстрое подключение к сервисам и оперативное реагирование на инциденты.

Соблюдение законодательства

Соответствие требованиям
Выполнение требований законодательства и регуляторов РФ.

Подходящие средства защиты
Эксплуатация сертифицированных решений лидирующих вендоров.

Лицензии регуляторов
Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России.

Отслеживание изменений
Меры защиты всегда соответствуют всем новым законам и регламентам.

Узнать подробнее или заказать сервис

presale@rt-solar.ru

Сервисы кибербезопасности «Ростелеком-Солар»

Solar MSS — кибербезопасность как сервис

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Защита от DDoS-атак (Anti-DDoS)

ЕПСК*

- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Управление мобильными устройствами (EMM)

Solar JSOC — сервисы мониторинга и реагирования

- Мониторинг, реагирование и анализ инцидентов ИБ
- Контроль защищенности и управление уязвимостями
- Техническое расследование инцидентов
- Эксплуатация систем ИБ и реагирование на атаки
- Подготовка аналитики для бизнеса и поддержки принятия решения
- Сервисы ГосСОПКА

*Единая платформа сервисов кибербезопасности

О компании

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

Ростелеком Солар

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70

S.9.07.BR.ADD.02