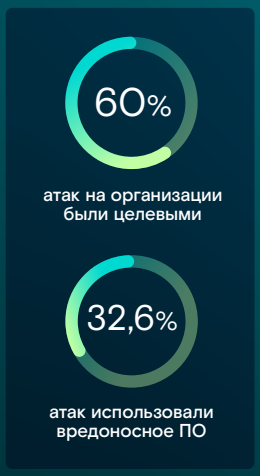
Сервис защиты от продвинутых угроз

Защита от ранее неизвестных киберугроз и сложных целевых атак в реальном времени с помесячной оплатой для организаций любого масштаба

rt-solar.ru
rt.ru

Ростелеком Солар

Проблематика



Данные Solar JSOC и Positive Technologies, 2020 г.

Сегодня злоумышленники все чаще используют продвинутое вредоносное ПО для атаки критически важных сегментов компании. Они изменяют вредоносное ПО и активируют с задержкой во времени, поэтому обнаружить его с помощью стандартных средств защиты невозможно.

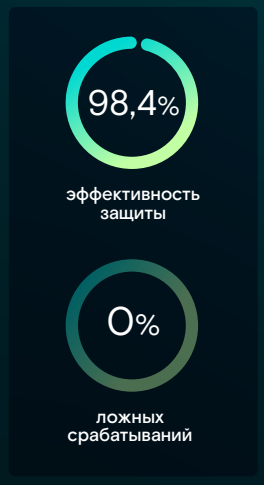
Так, для защиты от сложных угроз применяются песочницы. Они анализируют файлы из входящей почты или веб-трафика и принимают решение — пропустить их дальше или заблокировать.

Но у песочниц есть свои минусы:

- Некоторые песочницы можно обойти, т.к. вредоносные файлы умеют скрывать свое присутствие.
- Анализ угроз замедляет работу сотрудников в среднем на 30 минут.
- Стоимость внедрения собственной песочницы начинается с 10 млн. рублей. Чем больше файлов нужно анализировать, тем дороже.

Эти проблемы можно решить, воспользовавшись сервисом защиты от продвинутых угроз (Sandbox) компании «Ростелеком».

Описание сервиса



Данные NSS Labs, 2019 г.

Сервис Sandbox компании «Ростелеком» — это комплексная защита от продвинутых и ранее неизвестных угроз в реальном времени с помесячной оплатой. В основе сервиса — Check Point Sandblast, лидирующее решение для защиты от продвинутых угроз согласно отчету NSS Labs за 2019 год.

- Обойти защиту Sandbox не получится. Проверка вредоносного кода производится до того, как он попытается скрыть следы своего присутствия.
- Анализ угроз не влияет на работу пользователей и происходит незаметно для них. На этапе проверки доступна безопасная копия анализируемого файла.
- Сервис подключается в течение 5 дней. Ежемесячно оплачивается только количество анализируемых файлов. Эксплуатацией сервиса занимаются специалисты «Ростелеком-Солар».

Решаемые задачи

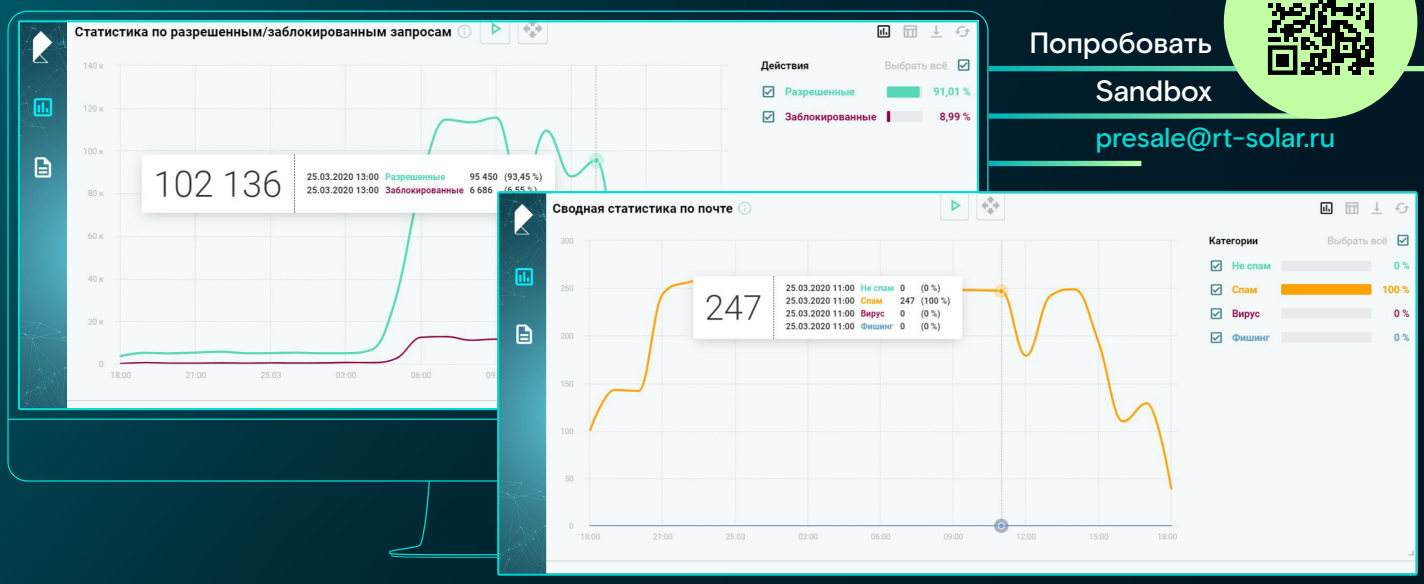
- Защита критически важных сегментов незаметно для бизнес-процессов
- Обнаружение сложно детектируемых угроз в почте и веб-трафике
- Снижение затрат на построение и эксплуатацию системы защиты
- Проверка скрытых угроз в зашифрованном трафике протоколов SSL/TLS

Для кого

Сервис подходит компаниям, которые заинтересованы в эффективной защите критически важных сегментов и повышении общего уровня безопасности.

- Государственные органы
- Учреждения здравоохранения
- Промышленность и добыча
- Транспорт и логистика
- Образовательные учреждения
- Финансовые организации
- Энергетическая отрасль
- Онлайн и розничная торговля

Личный кабинет Solar MSS



Попробовать Sandbox

presale@rt-solar.ru

Преимущества

Комплексный подход

Полноценная интеграция с сервисами защиты электронной почты (SEG) и сетевого периметра (UTM) экосистемы Solar MSS

Удобно

Детализированные отчеты об угрозах и анализируемом трафике компании

Защита от обхода

Проверка на уровне CPU блокирует вредоносный код до его выполнения и попытки скрыться

Актуально

Регулярное обновление базы угроз

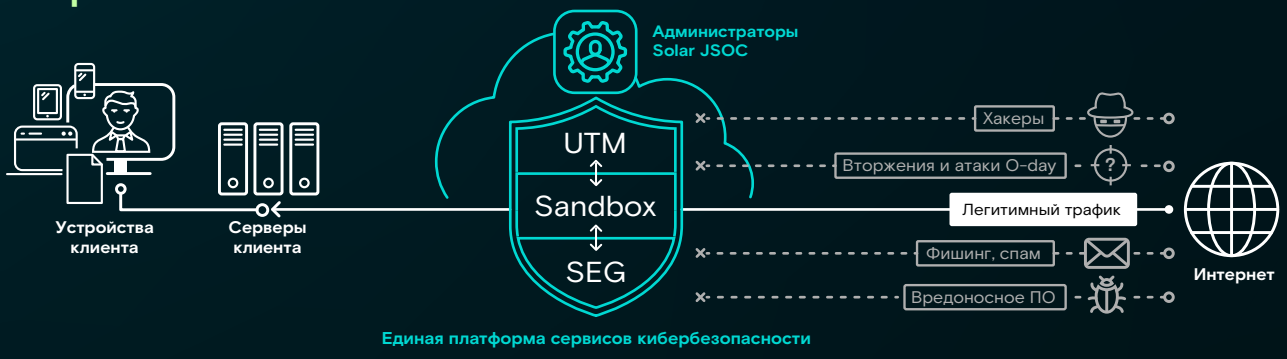
Безопасно для бизнес-процессов

Возможность доступа к безопасной копии файла на этапе анализа его содержимого

Надежно

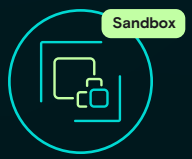
Мгновенное обнаружение ранее неизвестных угроз

Схема работы



Варианты использования

Сервис легко интегрировать с другими решениями экосистемы Solar MSS.



Отдельное решение Sandbox

Интеграция с сервисом защиты электронной почты (SEG)

Интеграция с сервисом защиты от сетевых угроз (UTM)

Выгоды сервисной модели

- Просчитываемые ежемесячные платежи
- Устранение дефицита кадров
- Быстрое подключение
- Контроль работы сервиса 24/7
- Взаимодополняемые сервисы в рамках экосистемы
- Простая масштабируемость
- Личный кабинет с детальными отчетами
- Соответствие законодательству РФ

Сервисы кибербезопасности «Ростелекома»

Solar MSS
управляемые сервисы кибербезопасности

Экосистема управляемых сервисов кибербезопасности для комплексной защиты от массовых киберугроз (MSS)

- Регистрация и анализ событий ИБ (ERA)
- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Защищенная удаленная работа (SRW)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)
- Контентная фильтрация (CF)

Solar JSOC
экспертные сервисы кибербезопасности

Первый и крупнейший в России коммерческий центр мониторинга и реагирования на киберинциденты (SOC)

- Мониторинг и анализ инцидентов ИБ
- Комплексный контроль защищенности: анализ рисков и обследование инфраструктуры, тестирование на проникновение, Red Teaming и др.
- Реагирование на инциденты и техническое расследование
- Эксплуатация систем ИБ и реагирование на атаки
- Анализ угроз и внешней обстановки
- Построение SOC и его частных процессов*

*В том числе Центров ГосСОПКА

О компании «Ростелеком-Солар»

«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.

№1	800+	70+	24/7	400+	86+ млрд
на рынке сервисов кибербезопасности	экспертов кибербезопасности	клиентов из топ-100 российского бизнеса	обеспечение кибербезопасности	комплексных и сервисных проектов в год	анализируемых событий ИБ в сутки

Ростелеком Солар

presale@rt-solar.ru rt.ru rt-solar.ru +7 (499) 755-07-70

0.11.BL.SB.01