

Обзор сервиса Smart Web Security AntiDDoS + WAF + Antibot

Марат Вахитов,
Solution Sale Security,
Yandex Cloud

Святослав Грунский,
Product Manager SWS,
Yandex Cloud

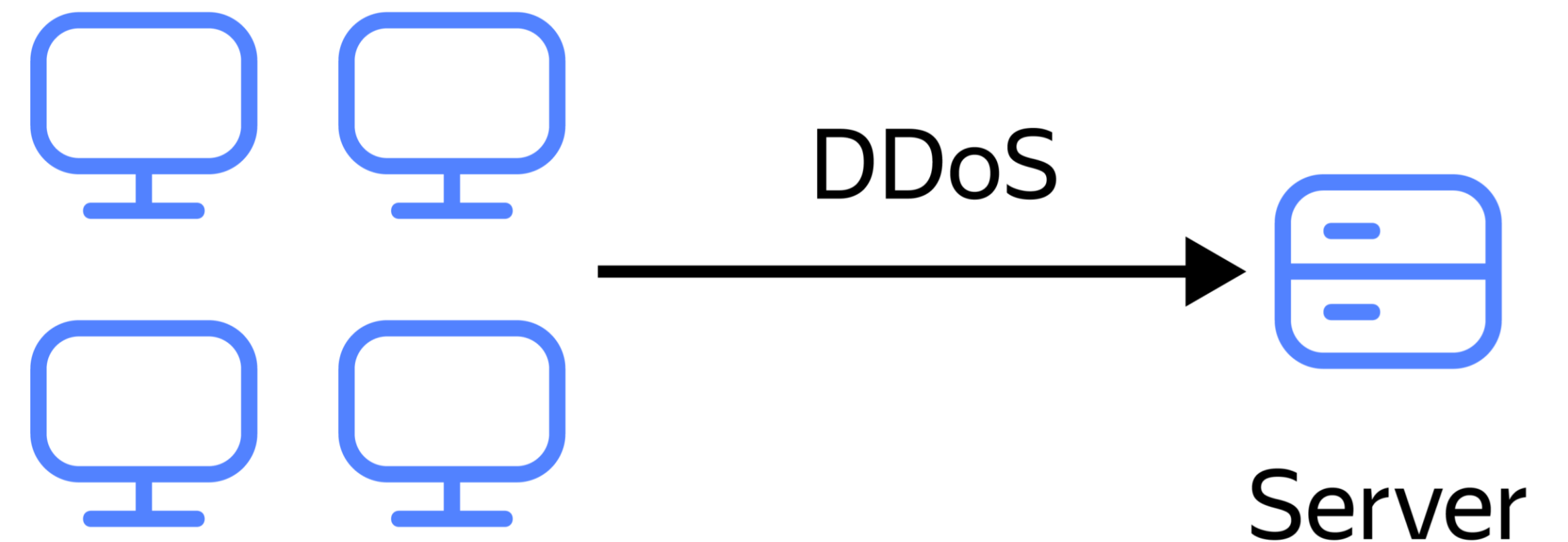
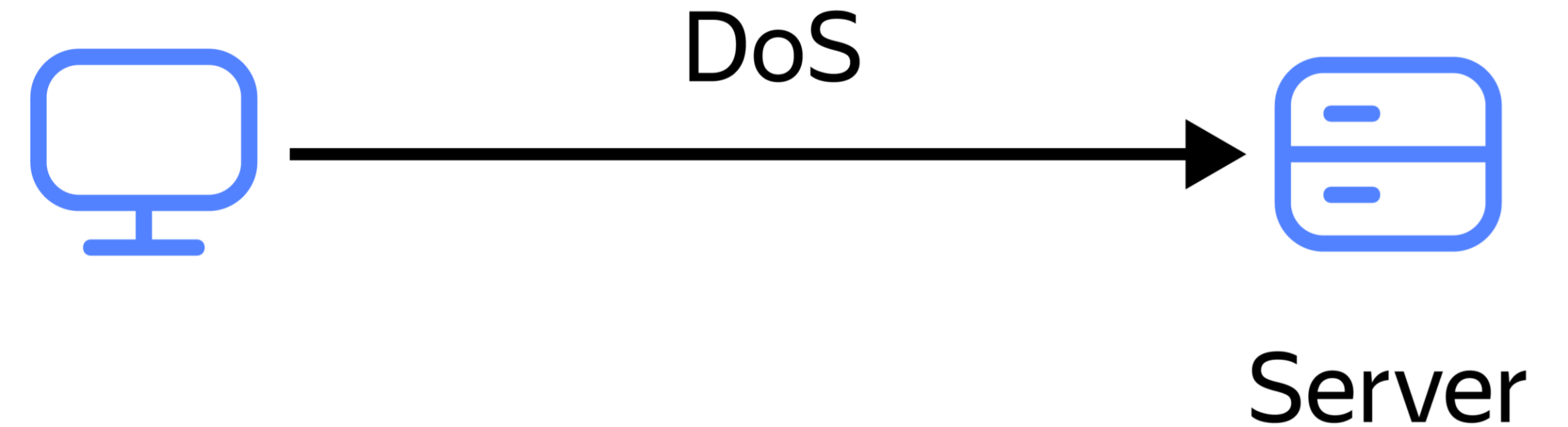
О чём поговорим

1. Что такое AntiDDoS, WAF, Antibot
2. Статистика
3. Smart Web Security
4. Q&A

Что такое DoS-атака

DoS-атака — Denial of Service,
(отказ в обслуживании) —
хакерская атака на вычислительную
систему. Её цель — **сделать ресурс**
недоступным для пользователей

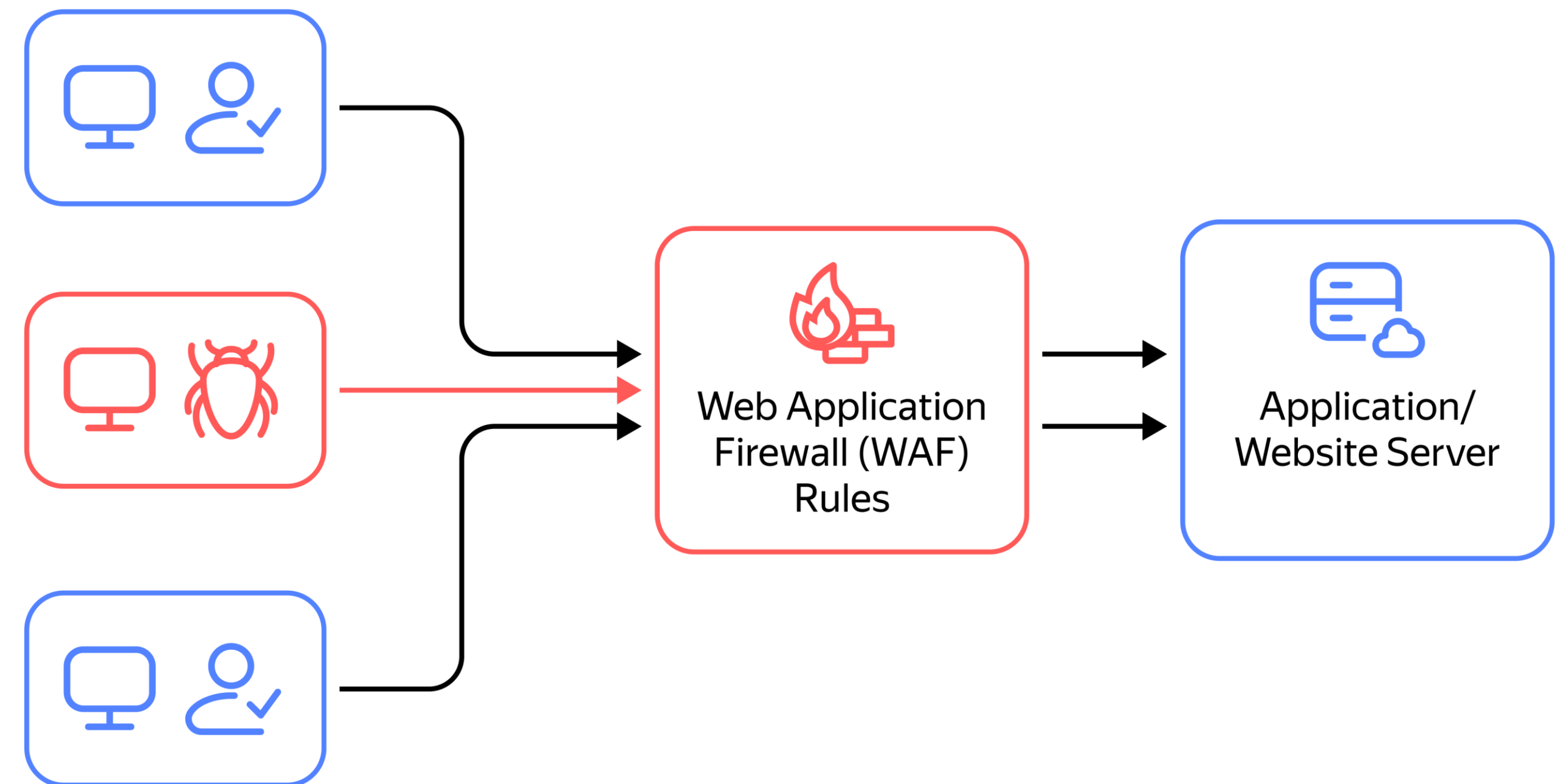
DDoS-атака — атака с множества
источников одновременно.
Различие в масштабе и сложности



Что такое WAF

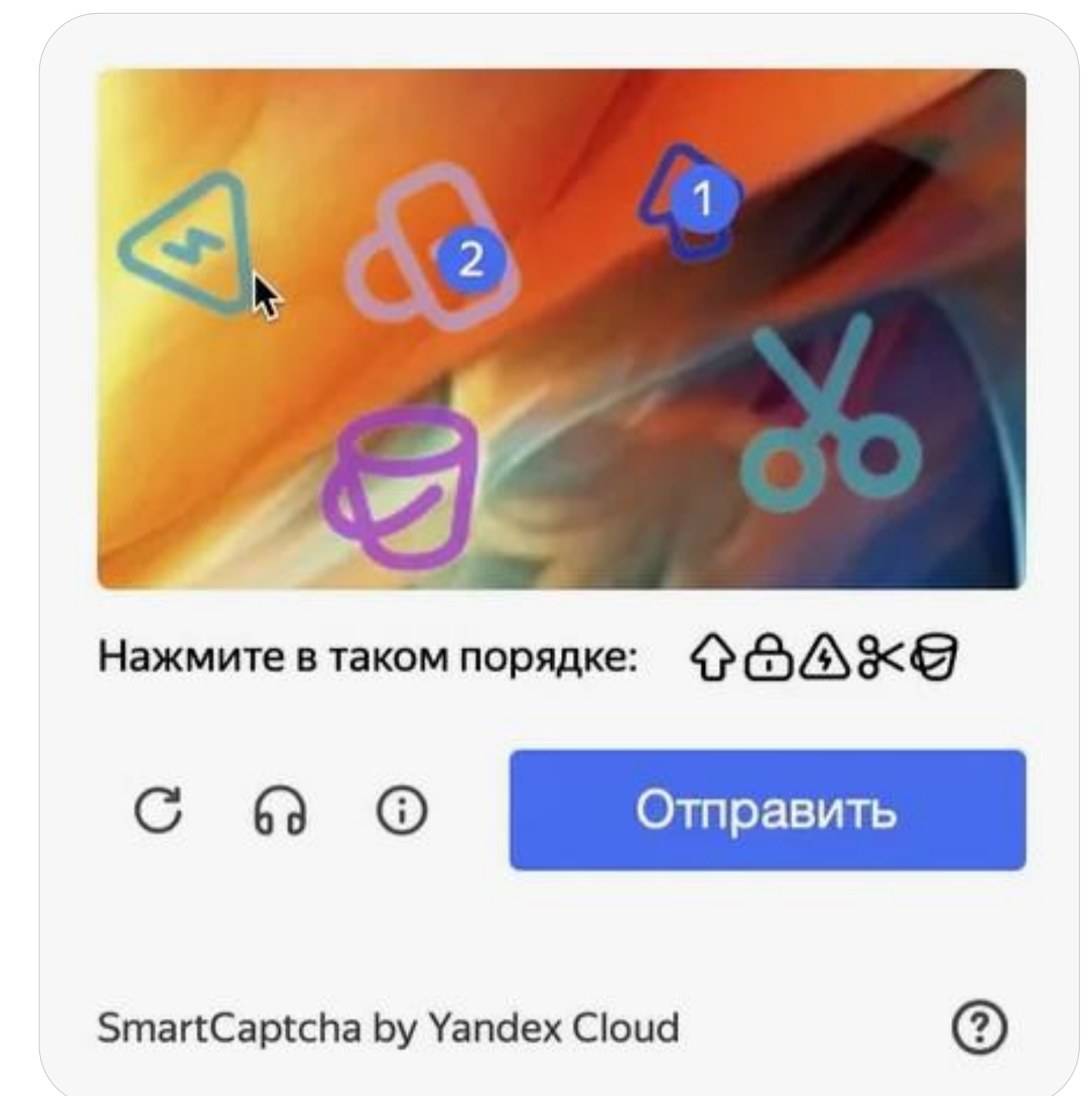
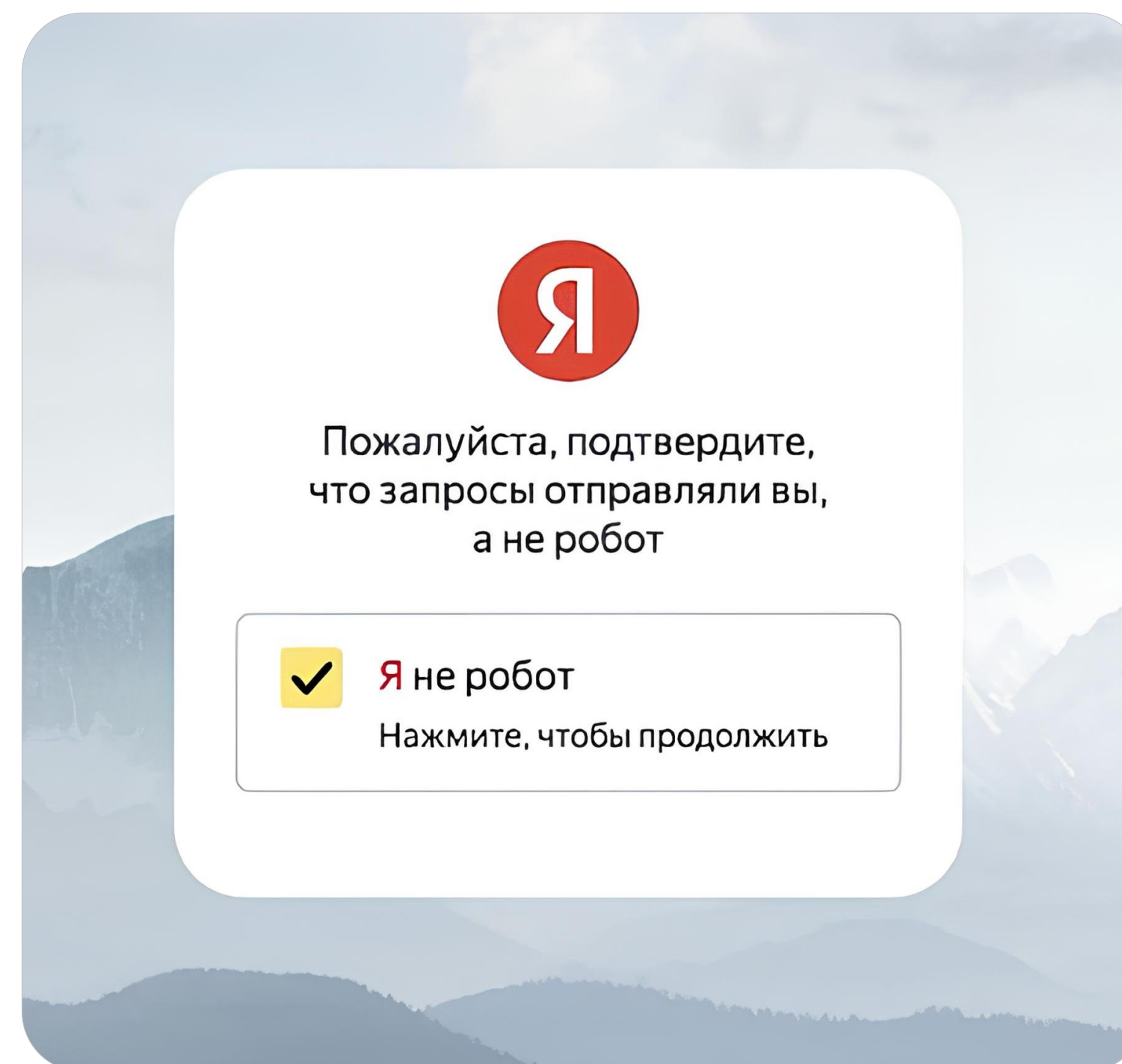
WAF (Web Application Firewall) — специализированное средство защиты веб-приложений

Фильтрует и блокирует вредоносный трафик, направленный на веб-приложения и сайты. Он защищает от распространённых атак, таких как SQL-инъекции, XSS, атаки на веб-уязвимости, и предотвращает компрометацию данных и простои ваших сервисов



Что такое Antibot

SmartCaptcha —
сервис для верификации
запросов, который помогает
определить обращения
пользователей
и блокирует роботов



Статистика атак

+108%

Выросло общее **количество**
DDoS-атак в 2024 году,
по сравнению с 2023 годом

+100%

В 2 раза выросла **мощность атак**
на веб-приложения в 2024 году,
по сравнению с 2023 годом

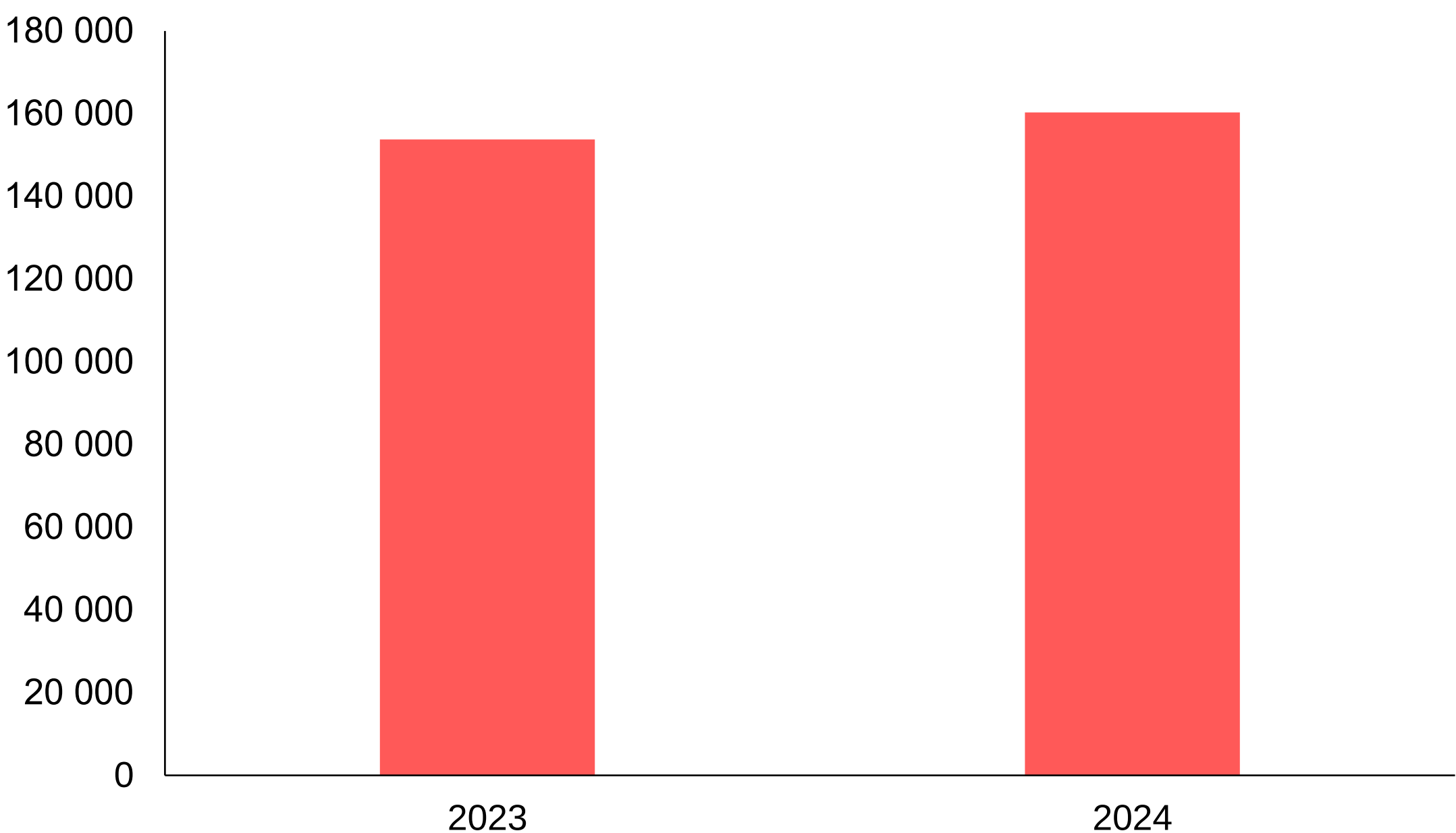
DDoS-атаки на Яндекс

Пиковые значения

75%

имеют пиковый RPS < 150 тыс.

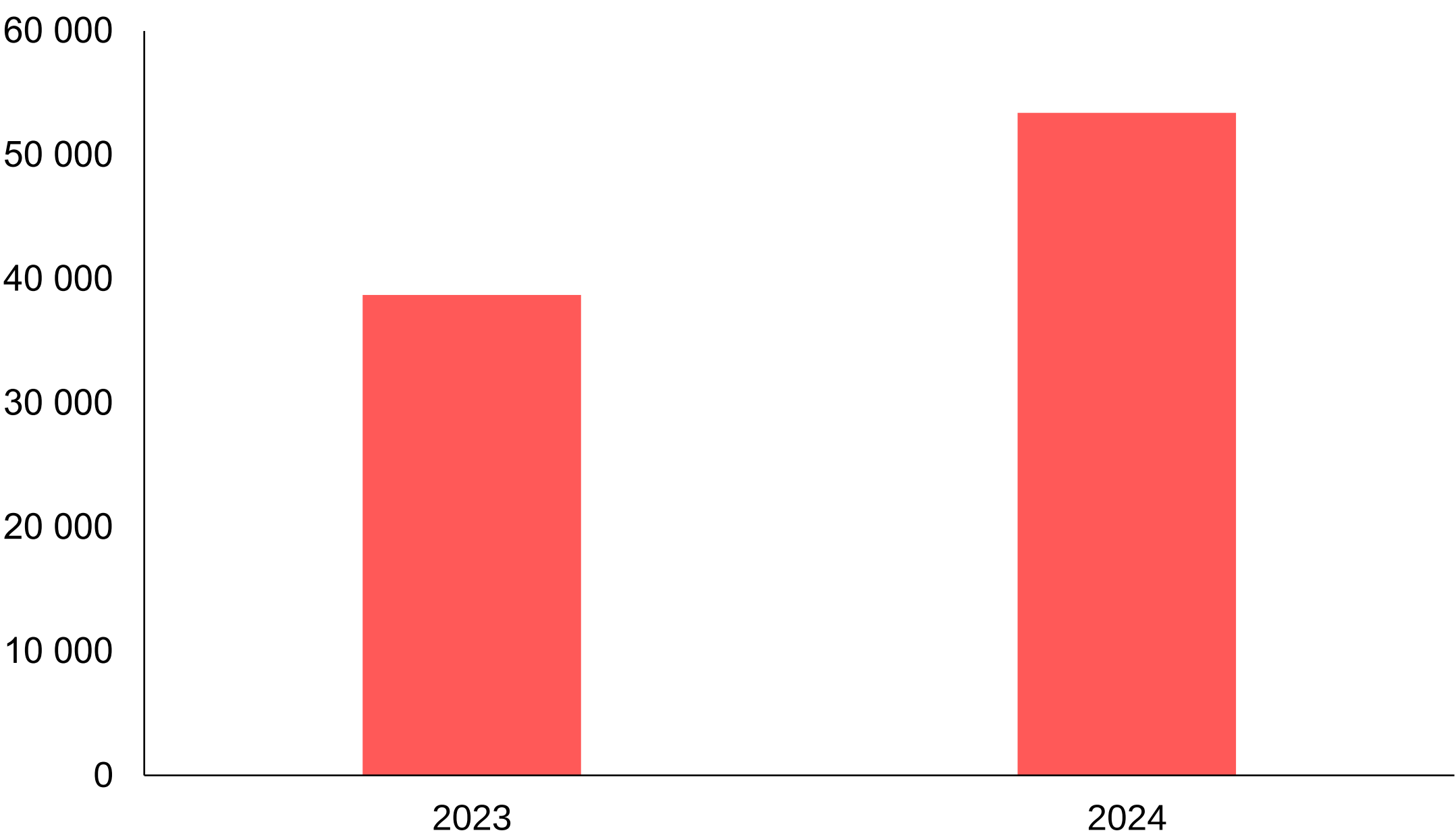
75-й процентиль по пиковым RPS



38%

составил рост медианного значения пиковых RPS

Медианное значение пиковых нагрузок, RPS



DDoS-атаки на Яндекс

Продолжительность

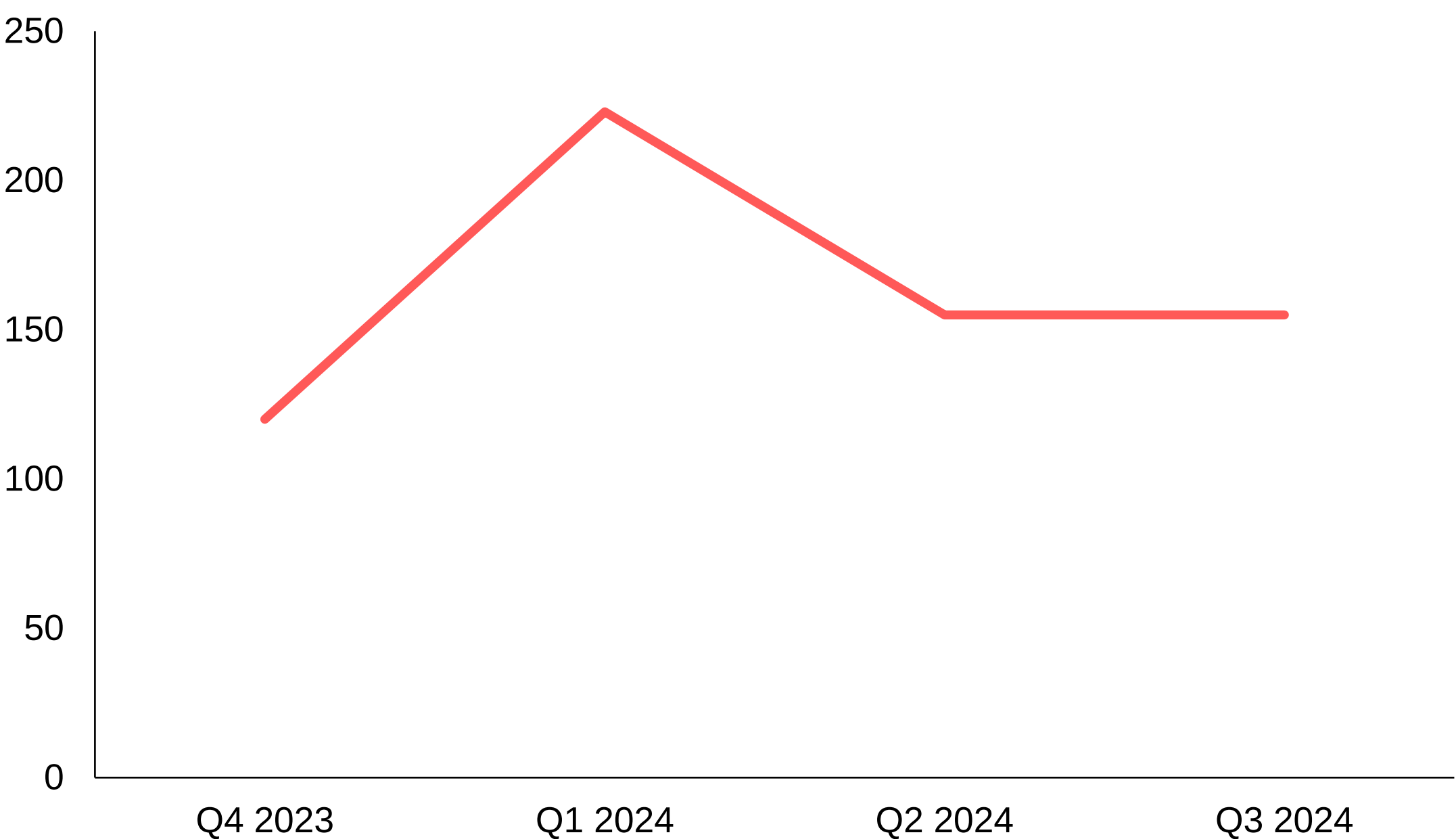
75%

DDoS-атак длятся 2–3 минуты

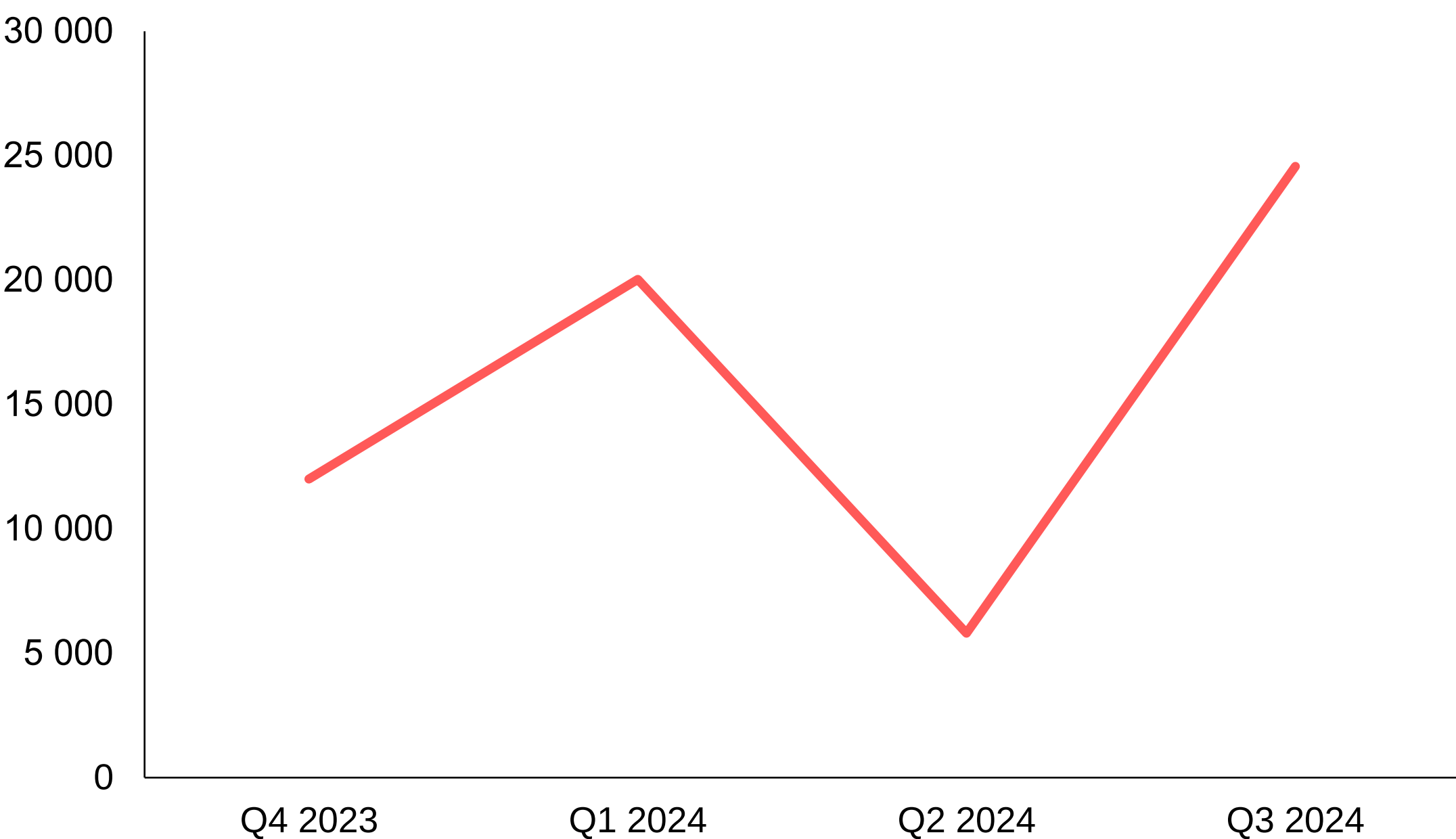
400 минут

продолжалась самая длительная атака

Длительность атаки, с



Максимальная длительность атаки, с





Smart Web Security

Smart Web Security

Сервис для защиты веб-приложений



Возможности

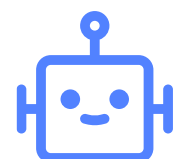
Защита от DDoS-атак

Очистка трафика при помощи ML-моделей и базовых правил фильтрации



Защита от ботов

Поведенческий анализ трафика и отправка подозрительных запросов в сервис SmartCaptcha



Web Application Firewall

Широкое покрытие векторов атак OWASP
Топ-10 за счёт использования нескольких наборов правил и ML-WAF



Ограничение нагрузки на приложение

При помощи продвинутого Rate Limiter возможно задать ограничение на весь трафик или на отдельные параметры запроса



Smart Web Security

Сервис для защиты веб-приложений



Преимущества

Защищает высоконагруженные сервисы при среднем времени анализа запроса 1 мс



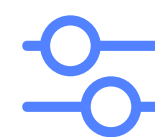
Эффективная очистка и широкое покрытие атак (сигнатуры + ML)



ML-технологии Яндекса для точного обнаружения атак



Гибкая настройка политик безопасности и правил фильтрации трафика



Подключение за 30 минут, простая настройка, мгновенная реакция на атаки



Интеграция с другими сервисами облака и широкие возможности автоматизации



Интеграция в инфраструктуру

1

Нативная
интеграция
с сервисами
Yandex Cloud

2

Защита гибридных
инфраструктур
и ресурсов вне
Yandex Cloud

3

Защита физических
серверов
Yandex BareMetal
или ресурсов в ЦОД

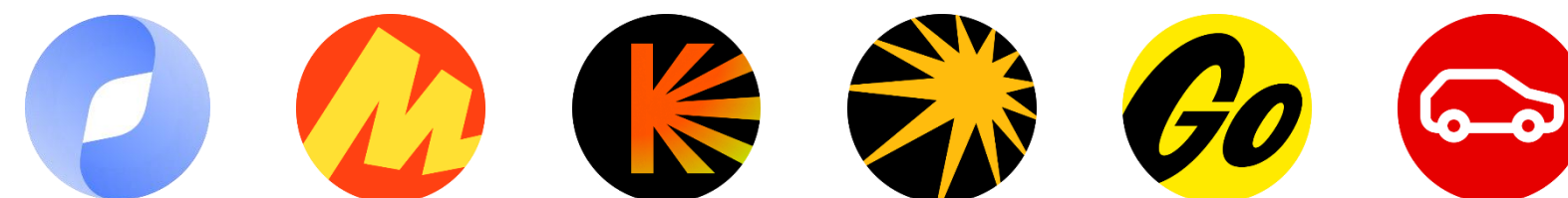
Smart Protection

Анализирует трафик
с помощью алгоритмов
машинного обучения
и поведенческого анализа

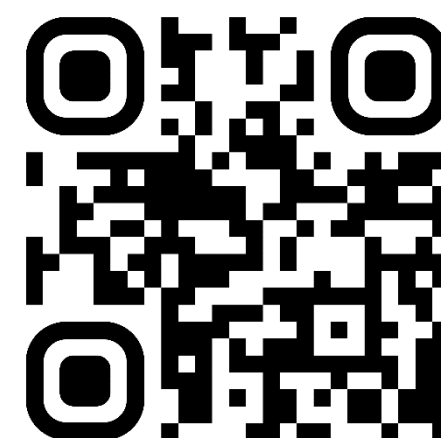
- Блокирует атаки, аномальные и нелегитимные запросы
- Подозрительные запросы отправляет в сервис SmartCaptcha

Построен на собственной
технологии Яндекса «Антиробот»

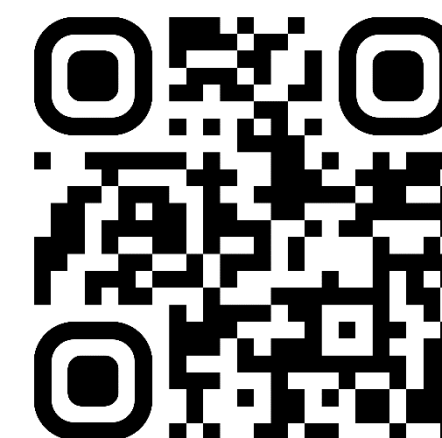
- Защищает уже более 100 сервисов, включая:



- Подробнее про технологию:



[clck.ru/
3BXvUQ](https://clck.ru/3BXvUQ)



[clck.ru/
3BXvcQ](https://clck.ru/3BXvcQ)

Yandex Ruleset

Собственный набор правил от команды экспертов Яндекса

Не требует первоначальной настройки и снижает уровень ложноположительных срабатываний

arch yc yc-sws Smart Web Security / Профили WAF / Создание профиля WAF

Создание профиля WAF

Имя * ?

Описание

Метки

Добавить метку

Наборы правил

Выберите один или несколько наборов правил, которые будут применяться для анализа и действий с запросами. Настроить выбранные наборы можно после создания профиля WAF.

Набор / Вендор	Версия	Количество правил ?	Описание	Выбран
Yandex Ruleset PREVIEW Yandex	0.1.0	167	Набор разработан сообществом инженеров и аналитиков информационной безопасности Яндекса и состоит из ... тестируется на реальном трафике сервисов Yandex.	☒
Yandex Malicious Score PREVIEW Yandex	latest	6	Набор разработан инженерами и аналитиками Яндекса для выявления вредоносных запросов с помощью технологий машинного обучения. Это позволяет выявлять неизвестные угрозы и оперативно адаптироваться к новым типам атак, обеспечивая защиту в реальном времени. Набор проходит тестирование и показывает высокую эффективность при низком уровне ложных срабатываний.	☒
OWASP Core Ruleset OWASP	4.8.0 ▾	264	Набор разработан открытым сообществом OWASP и состоит из правил, которые предназначены для обнаружения вредоносных действий, включая загрузку вредоносных файлов, потенциальные атаки SQL Injection, попытки отказа в обслуживании, попытки инъекции кода и многое другое.	☒

Условие срабатывания профиля ?

При каком условии выносится вердикт о вредоносном запросе.

☒ Вердикт получен хотя бы в одном выбранном наборе

☐ Вердикт получен в каждом выбранном наборе

Приоритет применения правил ?

Укажите порядок, в котором будут анализироваться и применяться правила из выбранных наборов. Для изменения порядка перетащите имя набора.

1. OWASP Core Ruleset

2. Yandex Ruleset

3. Yandex Malicious Score

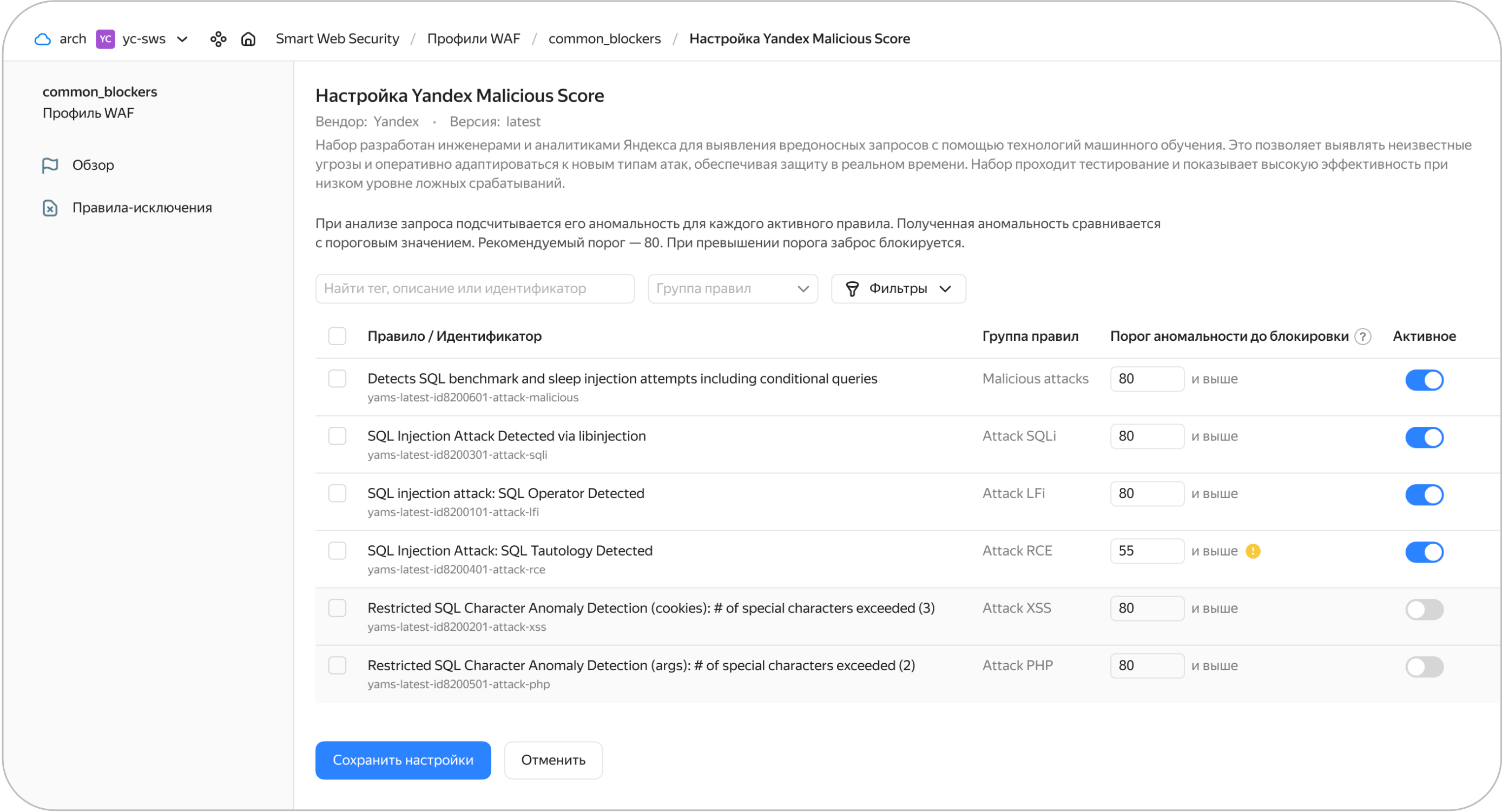
Создать

Отменить

14

ML WAF

Выявляет и блокирует атаки, которые не покрываются сигнатурным методом. Модуль разработан на основе собственных ML-моделей Яндекса. Даёт более точный результат, чем аналогичные решения западных вендоров, при средней скорости анализа запроса менее 1 мс.



Предустановленные списки



Наборы регулярно обновляемых IP-адресов от Yandex Cloud



Помогают автоматически блокировать потенциально опасный трафик

Yandex Cloud

Все сервисы

Поиск

Smart Web Security

Профили безопасности

Профили WAF NEW

Профили ARL NEW

Ещё

Cloud Shell

Избранное

Уведомления

Центр поддержки

architects sw sws-demo Smart Web Security / Списки

Создать список

Списки

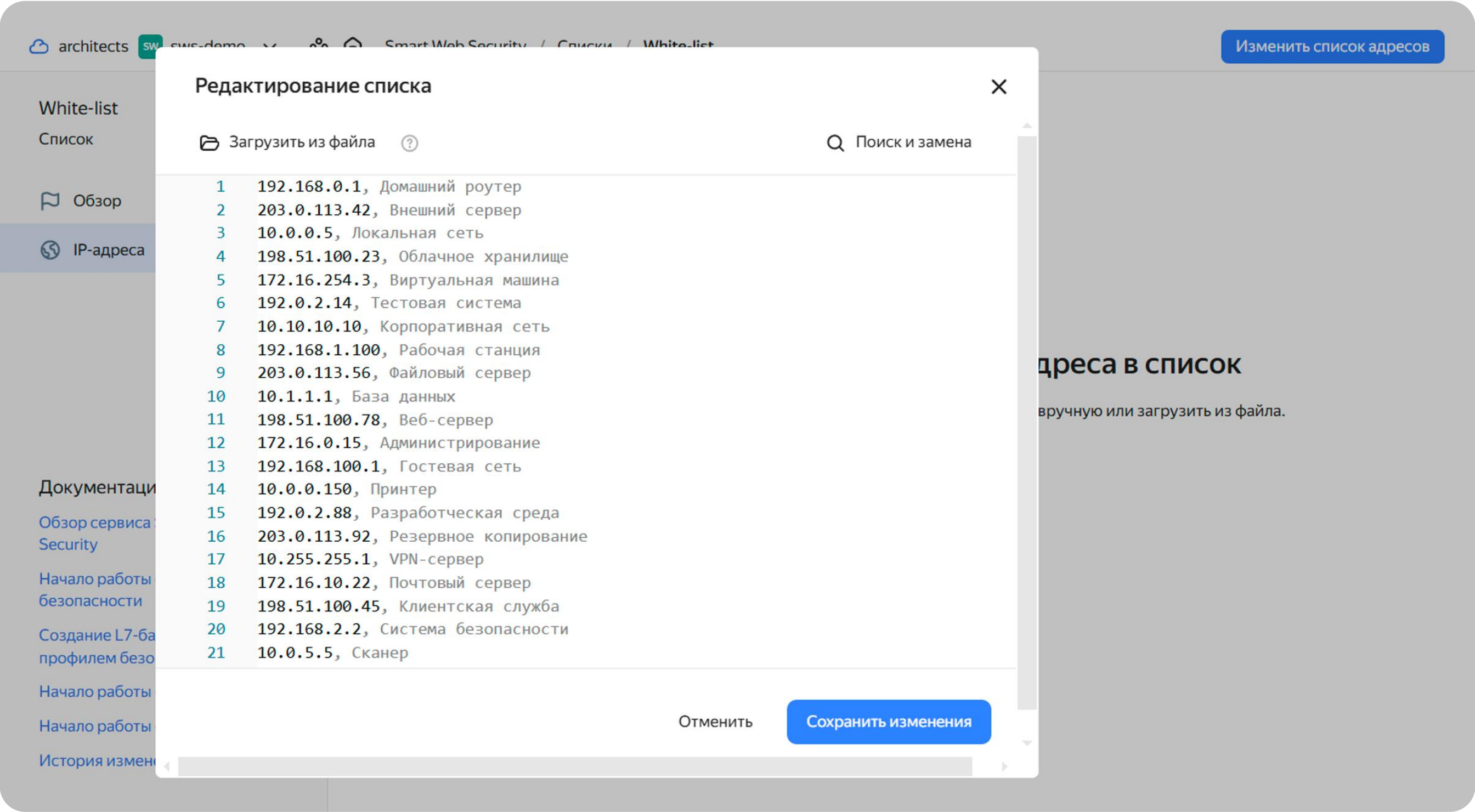
Пользовательские 1 Yandex Cloud 8

Фильтр по имени или описанию

Имя и описание	Тип	Профили безопасности	Профили WAF	Профили ARL	Метки	Идентификатор	
is_proxy The IP address belongs to proxy-providers	IP	—	—	—	—	fevtu1sah9ic7tksq8o0	
is_hosting The IP address belongs to hosting-providers	IP	—	—	—	—	feve23jtdvtboh13akju	
is_ml_vpn The IP address belongs to the vpn-providers (ml predicted)	IP	—	—	—	—	fevdr0noc7ohsjje3n9d	
is_anonymous The IP address belongs to the anonymous networks	IP	—	—	—	—	fevthha4t58cngiu2std	
is_vpn The IP address belongs to the vpn-providers	IP	—	—	—	—	fevs0u4cm9o02kiktop3	

Пользовательские списки

Доступно создание собственных чёрных и белых списков вручную или загрузка уже готовых файлов в форматах TXT или CSV



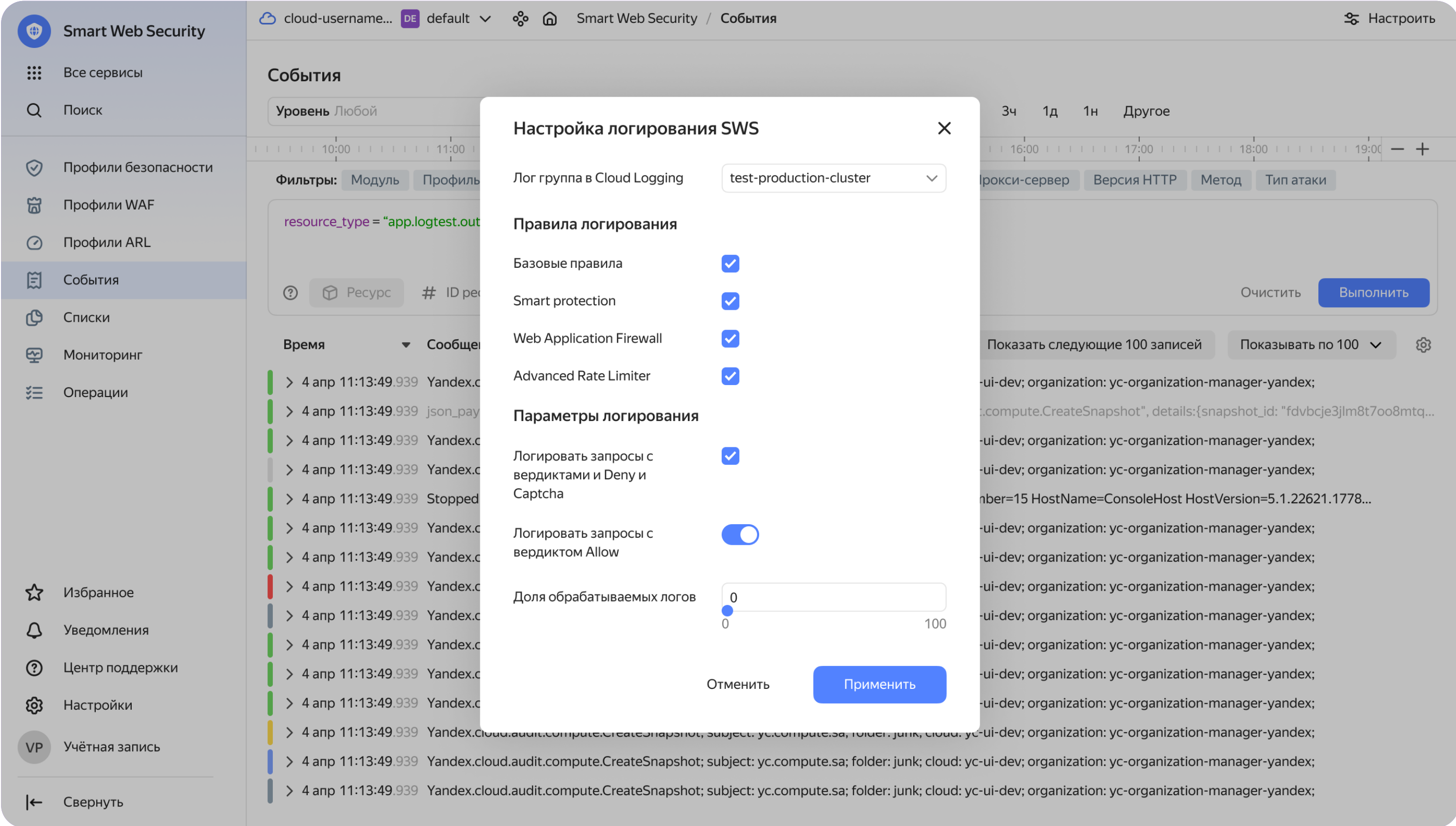
Единый интерфейс для логов

Просматривайте логи с результатом анализа запросов и выданным вердиктом в отдельной вкладке

Логи можно фильтровать по параметрам и значениям

По типу правила: базовые правила, правила Smart Protection, правила WAF, правила ARL

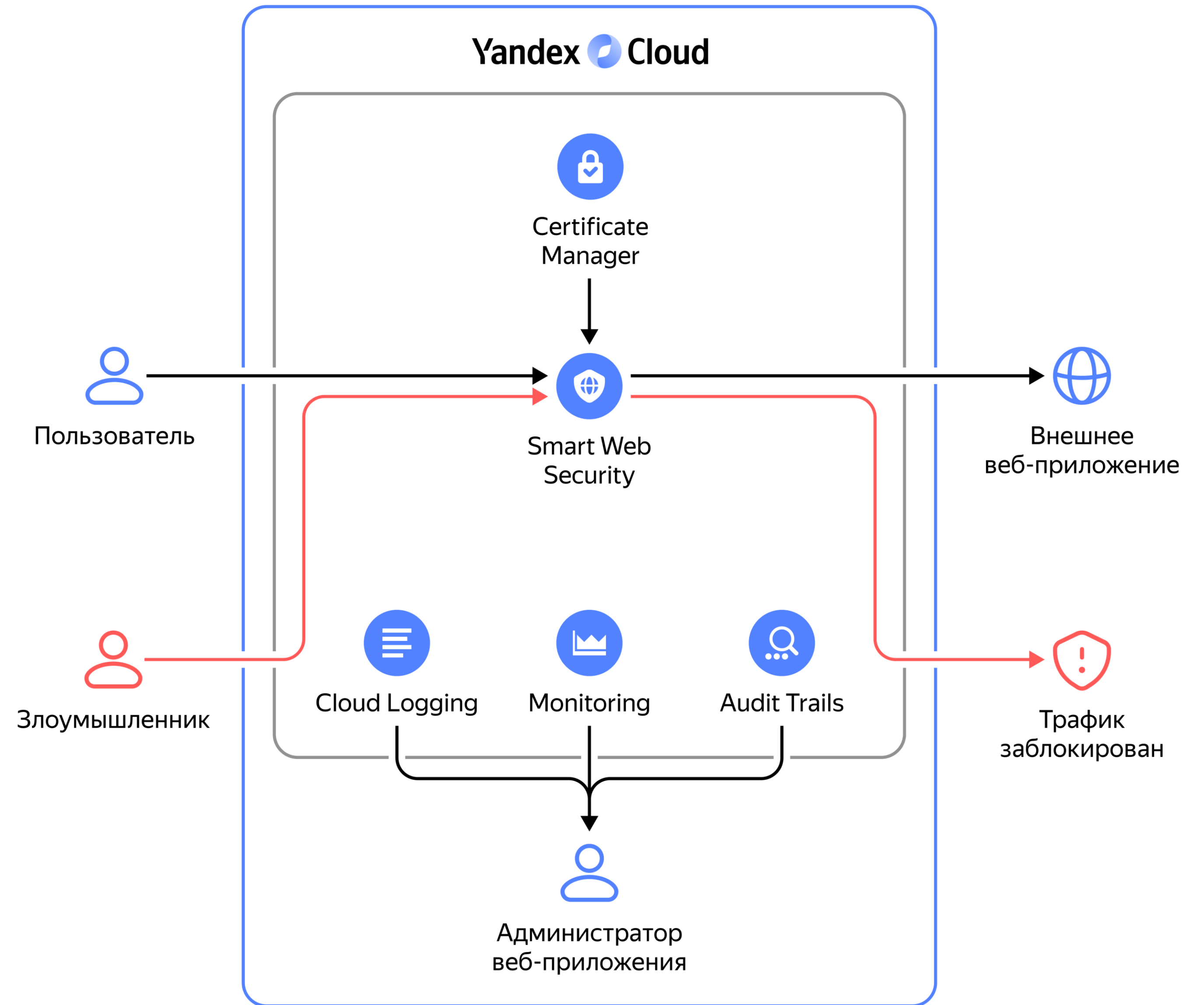
По правилам в режиме Dry Run



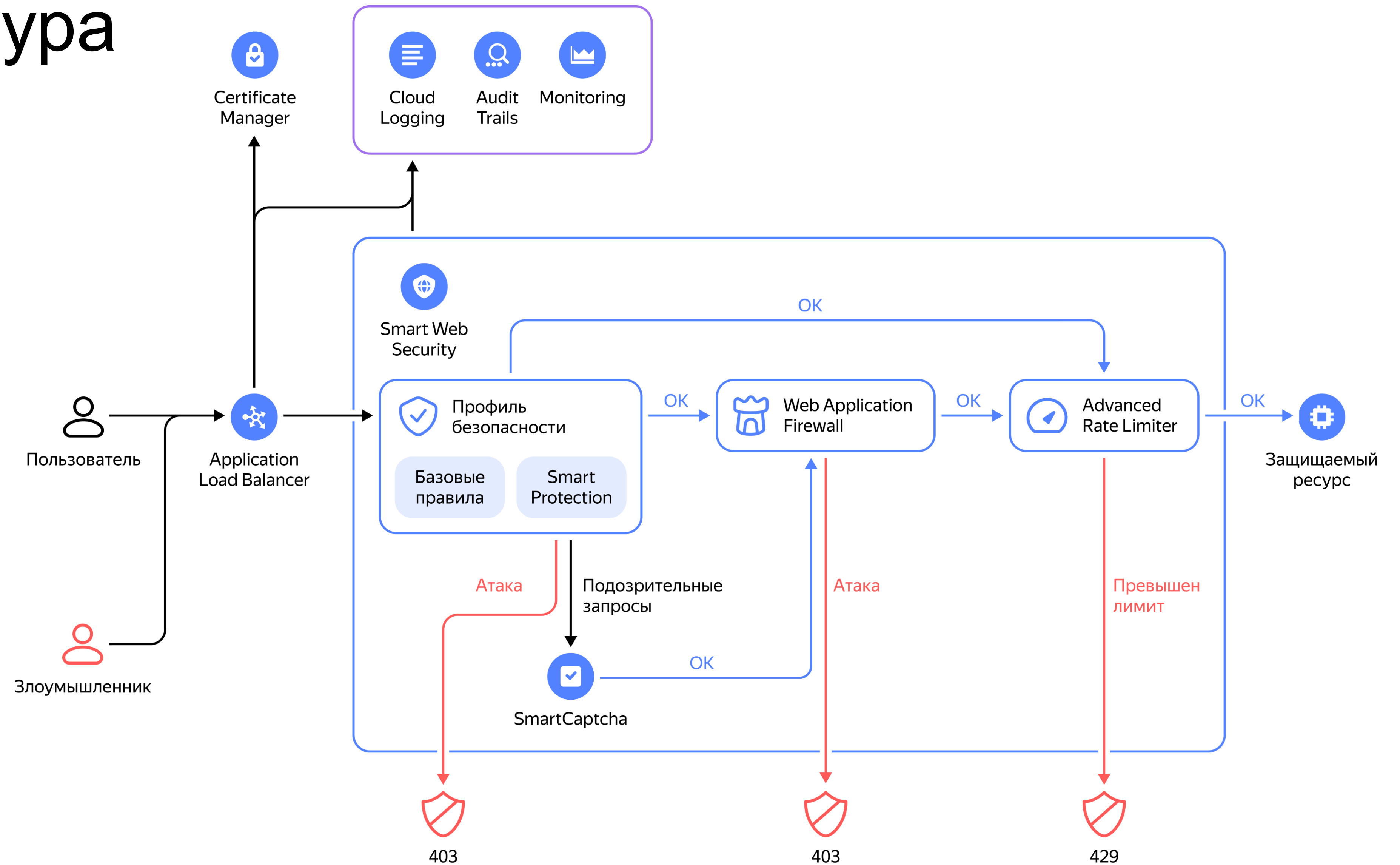
Единая защита для гибридных инфраструктур

Preview

Используйте сервис
для защиты вашей
инфраструктуры,
даже если она размещена
на собственных серверах
или в других публичных
облаках



Архитектура сервиса



Smart Web Security для ювелирного e-commerce

Задача: защита сайта ювелирного завода от киберугроз, снижение рисков даунтайма и роста затрат

Решение: подключили Smart Web Security для защиты от ботов, DDoS- и веб-атак. Доработали архитектуру и подключили Yandex Application Load Balancer

Результаты: обеспечили работу сервисов компании вне зависимости от атак на инфра-структуру. Снизили риск финансовых потерь и оттока клиентов

1

месяц

на внедрение
Smart Web Security

0

часов

на поддержку
сервиса в облаке

250 тыс. рублей

затраты на сервис в месяц



Как быстро развернуть защиту от киберугроз

Задача: развернуть в облаке системы CRM и PIM и обеспечить защиту от угроз ИБ

Решение: размещение систем в Yandex Cloud и подключение Yandex Smart Web Security для предотвращения DDoS-атак уровня приложений и атак OWASP Top-10

Результаты: масштабируемые вычислительные ресурсы, оптимизация затрат на развёртывание и обслуживание инфраструктуры и высокая доступность сервисов вне зависимости от атак на инфраструктуру

4 часа

на развёртывание
решения в облаке

0

часов

на поддержку инфра-
структуры в облаке

2

системы

развернули
в облаке



Application Load Balancer



Compute Cloud



Managed Service for MySQL®



Yandex Smart Web Security

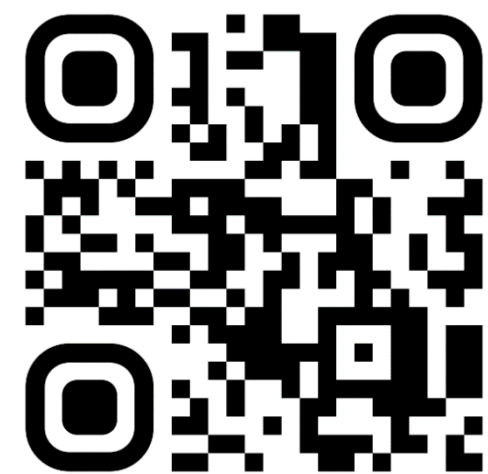
Тарификация

Из чего складывается стоимость

Стоимость зависит от способа тарификации:

- По подписке — подходит для больших объёмов входящего трафика
- По количеству запросов — подходит для небольшого объёма входящего трафика

Start	Pro	Business	Enterprise
от 50 000 ₽ / мес	от 158 000 ₽ / мес	от 255 000 ₽ / мес	
✓ Для малого бизнеса ✓ Объём трафика: до 100 млн запросов в месяц	✓ Для среднего и быстрорастущего бизнеса ✓ Объём трафика: до 500 млн запросов в месяц	✓ Для крупного бизнеса с высоконагруженными системами ✓ Объём трафика: до 1 млрд запросов в месяц	✓ Для корпораций и критически важных инфраструктур ✓ Рассчитывается индивидуально, исходя из вашего запроса и требований



Правила тарификации:
yandex.cloud/ru/docs/smartwebsecurity/pricing

Спасибо!



Марат Вахитов,
Solution Sale Security,
Yandex Cloud