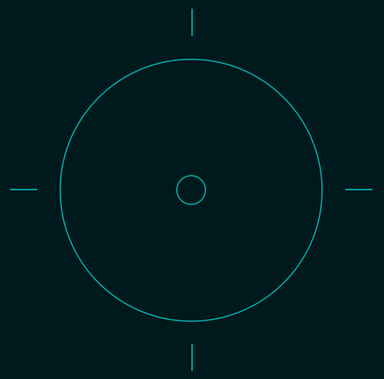
БКС МИР ИНВЕСТИЦИЙ + servicepipe

Выявление кибератак в зашифрованном трафике веб-приложений с непрерывным улучшением точности

История успешной синергии клиента БКС и разработчика Servicepipe при решении задачи защиты от DDoS-атак и вредоносных ботов



Ситуация

servicepipe

БКС МИР ИНВЕСТИЦИЙ

БКС — финансовая группа с 29-летней историей, многолетний лидер Московской биржи по объёму торгов.

Специфика бизнеса и многомиллионная клиентская база требуют стабильной круглосуточной доступности сервисов БКС, так как она напрямую влияет на прибыль компании.

В 2022 году финансовый рынок столкнулся с масштабными DDoS-атаками в десятки миллионов запросов в секунду и ботовыми атаками на системы регистрации и авторизации ключевых приложений. Кибератаки перешли в плоскость веб-приложения и стали нагружать балансировщики, включая веб-серверы.

Масштаб и разнообразие новых атак выявили необходимость в усилении средств защиты. БКС требовалось универсальное решение: эффективная веб-защита, соответствующая требованиям регулятора и адаптируемая к меняющемуся ландшафту киберугроз.

Специфика финансовой отрасли: соответствие требованиям регулятора

servicepipe

БКС МИР ИНВЕСТИЦИЙ

БКС, как инвестиционная компания, должна соблюдать ряд требований финансового регулятора и внутренние требования по обеспечению устойчивости к кибератакам. В частности, не передавать ключи шифрования SSL сторонним компаниям, чтобы исключить возможность доступа злоумышленников при взломе провайдера защиты или анализе клиентских данных третьими лицами.

С 2021 года информационная безопасность финансовых организаций должна соответствовать требованиям ГОСТ Р 57580 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций». Соответствовать требованиям ГОСТ Р 57580 непросто. В стандарте приведено более 400 требований, в том числе «функционал обнаружения вторжений». Антибот Servicepipe удовлетворяет данному требованию, но лишь при условии его размещения внутри инфраструктуры БКС.

Требования БКС к защите от DDoS-атак и ботов

servicepipe

1. Защита веб-ресурсов и мобильного API без раскрытия зашифрованного клиентского трафика
2. Обеспечение круглосуточной доступности для любого количества веб-приложений и брокерских сервисов без изменений в их коде
3. Отражение DDoS-атак в автоматическом режиме без блокировки по IP-адресам
4. Защита от ботов с первого запроса без задержки на анализ логов веб-сервера
5. Стабильная доставка до веб-серверов не менее 1 Гбит/с очищенного трафика
6. Интеграция функционала платформы Servicepipe через API
7. Отсутствие ограничений по количеству защищаемых веб-ресурсов
8. Квалифицированная техподдержка 24/7

> «Главный критерий выбора антибот-решения: высокая точность защиты от ботов без раскрытия ключей SSL, в том числе и для мобильного API».
>
> Никита Зибаев, руководитель центра противодействия внешним атакам БКС

Архитектура IT-решения: локальная интеграция Servicepipe Антибот

servicepipe

Схема локальной интеграции NGINX-модуля Servicepipe Антибот в инфраструктуре БКС

Локальная защита зашифрованного трафика предусматривает интеграцию модуля Servicepipe Антибот для веб-сервера NGINX в инфраструктуре БКС. Схема исключает передачу SSL-сертификата за пределы контура сети в процессе работы алгоритмов определения нежелательной автоматизации для защиты веб-ресурсов на L7.

Архитектура IT-решения: алгоритм локальной защиты

servicepipe

1. На оборудовании заказчика устанавливается модуль решения Servicepipe Антибот для веб-сервера NGINX.

2. Веб-сервер БКС принимает соединение и устанавливает HTTPS-сессию.

3. Развёрнутый на нём NGINX-модуль получает необходимые для анализа на прикладном уровне данные о запросе и сверяется с локальным кешем. В случае отсутствия вердикта, модуль направляет их на проверку в центр принятия решений Servicepipe. Получив вердикт, NGINX-модуль сохраняет его в кеше и выдаёт серверу директиву пропустить или заблокировать данный запрос.

Непрерывное усиление защиты: обучение легитимному трафику

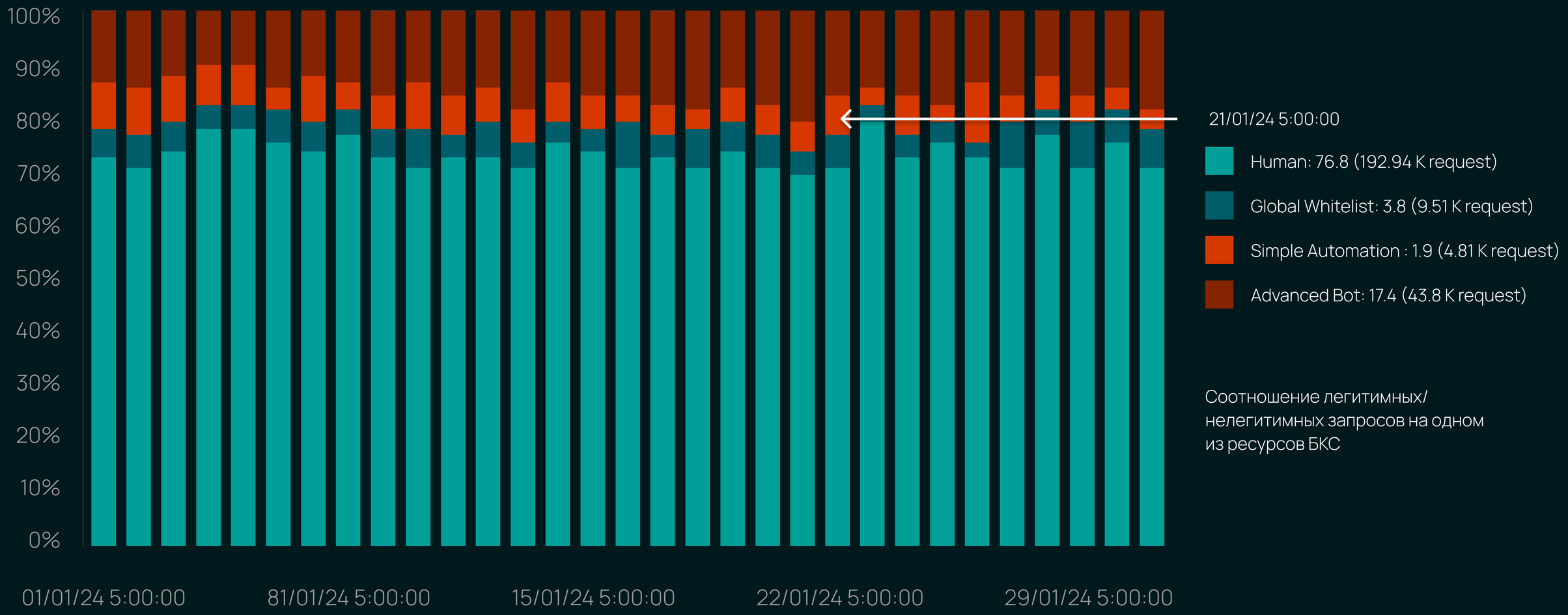
servicepipe

Из-за VPN, анонимайзеров и работы с корпоративных ПК, которыми пользуются клиенты и сотрудники БКС, возможны ложноположительные срабатывания системы фильтрации. Чтобы минимизировать количество ошибок, необходимо непрерывное обучение система фильтрации профилям легитимного трафика на защищаемым ресурсах. Чтобы модель для обучения становилась шире, БКС умышленно заводят необходимые сервисы под защиту отдельными веб-ресурсами. Антибот непрерывно дообучается профилям легитимного трафика по каждому из них.

> «Мы считаем, что обучение легитимному трафику в рамках большого количества разных ресурсов происходит значительно лучше. Поэтому мы отдельно завели под защиту значительное количество наших сайтов, сервисов, даже чаты и бэклог-трекеры».
>
> Михаил Драгунов, главный специалист центра противодействия внешним атакам БКС

Непрерывное усиление защиты: обучение легитимному трафику

servicepipe

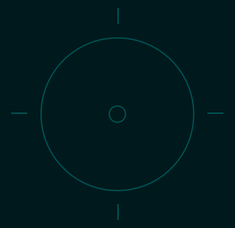


Соотношение легитимных/ нелегитимных запросов на одном из ресурсов БКС

Непрерывное усиление защиты: борьба с единичными блокировками

servicepipe

БКС не оставляет без внимания ни одну ложноположительную блокировку клиента. Совместно с Servicepipe выстроен процесс оперативного разрешения ситуаций блокировок клиентов.



«Мы выстроили автоматизированный процесс учёта обращений клиентов, при котором Антибот непрерывно дообучается профилям легитимного трафика по всем защищаемым ресурсам. Оперативная связь с нами — важнейшая задача для техподдержки Антибота. Ни у кого в России нет такого сочетания экспертности и отзывчивости, как у Servicepipe».

Михаил Драгунов, главный специалист центра противодействия внешним атакам БКС

Результат:
Высокая точность защиты

servicepipe

- Антибот интегрирован в инфраструктуру как NGINX-модуль, не требуя передачи зашифрованного трафика в сторону Servicepipe
- Все веб-ресурсы БКС (включая мобильные API) находятся под постоянной защитой от DDoS-атак и ботов на L7
- Антибот непрерывно обучается профилю трафика всех веб-ресурсов БКС для минимизации ложноположительных срабатываний
- Количество инцидентов для разбора WAF упало на 95% (с 20 млн до 1 млн вредоносных запросов в месяц)

Результат:
Высокая точность защиты

servicepipe

«Анализ и выявление ботов в решении Servicepipe Антибот работает не по логам (когда первый запрос всегда пропускается). Антибот отсекает даже первый запрос, если он вредоносный. Решение умеет точечно выявлять по URL: где система недообучена, где странный трафик, где ошибки по причине новых релизов, изменений в бизнес-логике и разработчиков, забывших о них предупредить. Крайне важна оказалась возможность создавать и управлять большим количество ресурсов. Также вы оперативно обогащаете нас списками ботнетов и вредоносных подсетей. С помощью пользовательских правил мы создаём свои политики обработки запросов».

Михаил Драгунов, главный специалист центра противодействия внешним атакам БКС

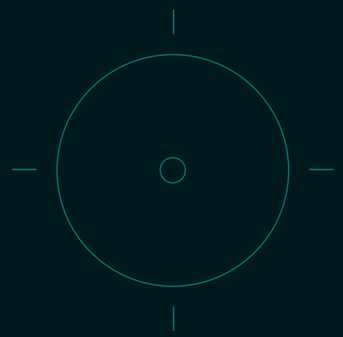
«Считаем, что Антибот Servicepipe даже более точен, чем решения зарубежных лидеров класса Bot Management».

Никита Зибаев, руководитель центра противодействия внешним атакам БКС

Результат:
Высокая доступность сервисов

servicepipe

Доступность сервисов БКС критична и напрямую влияет на прибыль компании.



Благодаря отсутствию простоев из-за DDoS-атак на инфраструктуру и приложения БКС удалось избежать значительных убытков.

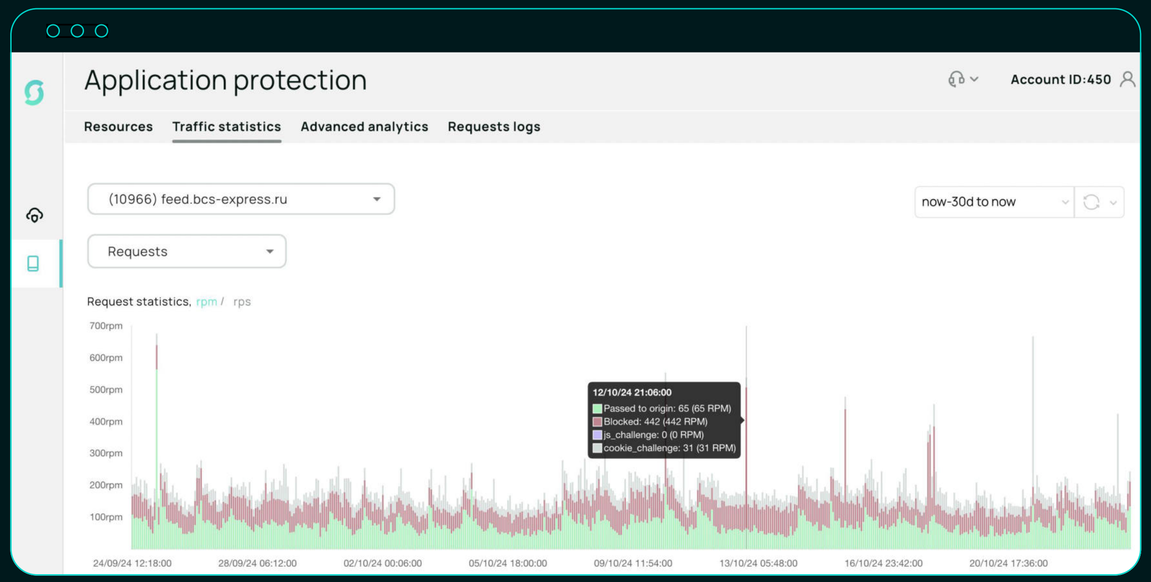
Результат:
Высокая доступность сервисов

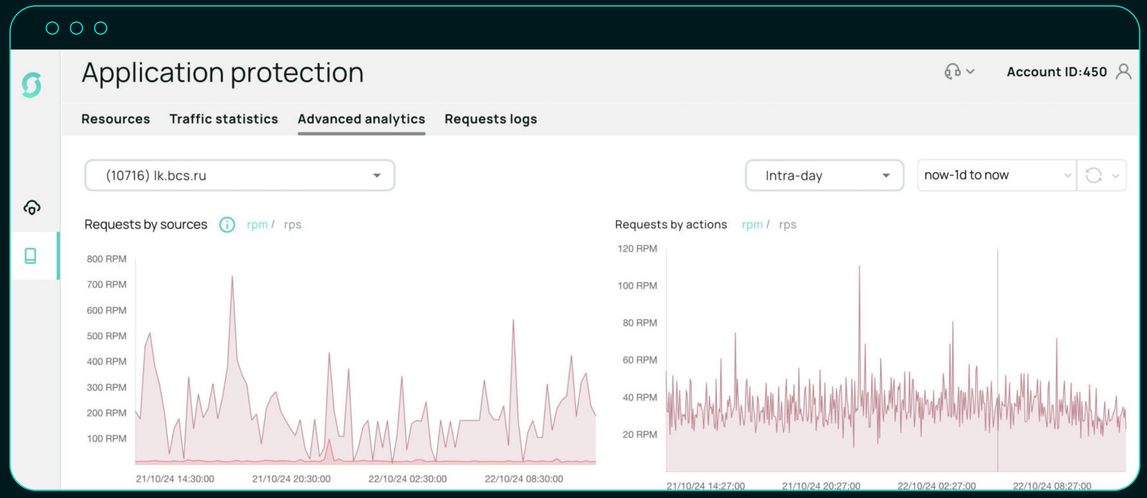
servicepipe

- Множество веб-ресурсов БКС заведены под защиту непрерывно обучающегося Антибота
- 1,5+ Гбит/с в месяц — объём очищенного трафика для сервисов БКС
- −95% инцидентов для разбора WAF — количество вредоносных запросов в месяц упало с 20 млн до 1 млн

Статистика по блокировкам в интерфейсе Антибота

servicepipe





Преимущества Servicepipe

servicepipe

1. Защита от DDoS-атак и ботов без раскрытия клиентского трафика, в том числе для мобильного API
2. Возможность интеграции веб-защиты, соответствующей требованиям регулятора
3. Поддержка защиты для любого количество веб-ресурсов
4. Фильтрация любых нелегитимных запросов без блокировки пользователей
5. Гибкие настройки фильтрации с помощью пользовательских правил
6. Панель управления со статистикой и отчётами в реальном времени
7. Уведомления о DDoS-атаках в чате с техподдержкой
8. Функциональная доработка алгоритмов Антибота по запросу

> «Благодаря нашей удачной синергии с БКС мы уже более двух лет усиливаем алгоритмы Антибота, непрерывно дообучаясь на многочисленных веб-ресурсах и сложном трафике заказчика».
>
> Михаил Хлебунов, директор по продуктам Servicepipe

БКС МИР ИНВЕСТИЦИЙ + servicepipe

Сотрудничество БКС и Servicepipe
в информационной безопасности — это непрерывное
совместное совершенствование алгоритмов
выявления и фильтрации нежелательного трафика в условиях
большого количества атак на финансовую сферу