Servicepipe Web DDoS & Bot Protection

Высокоточная защита веб-сайтов, мобильных приложений и API от DDoS-атак и фулстек-ботов

servicepipe

Продукты на базе собственной технологии Servicepipe Cybert в реестре российского ПО

Фильтрация DDoS и ботов без блокировок по IP

Любые варианты интеграции: облачный, гибридный, локальный

Отказоустойчивая и производительная модульная архитектура платформы фильтрации

Пользовательские правила для настройки гранулярной фильтрации под индивидуальный профиль трафика ресурса

Защита в том числе API мобильных приложений без раскрытия SSL ключей (соответствие PCI DSS)

Обучение браузерному трафику не требуется, мобильному трафику – до 3 суток

Выявление и блокировка как простых, так и продвинутых фулстек-ботов

Бесшовная интеграция с WAF и CDN, а также снижение до -95% инцидентов на WAF, требующих разбора

Пользовательская панель управления защитой

Управление белыми и чёрными локальными списками

Защита без изменений в коде веб-приложения

Опциональная CAPTCHA

Балансировка нагрузки

< 1 мс вынесение вердикта и блокировка бота

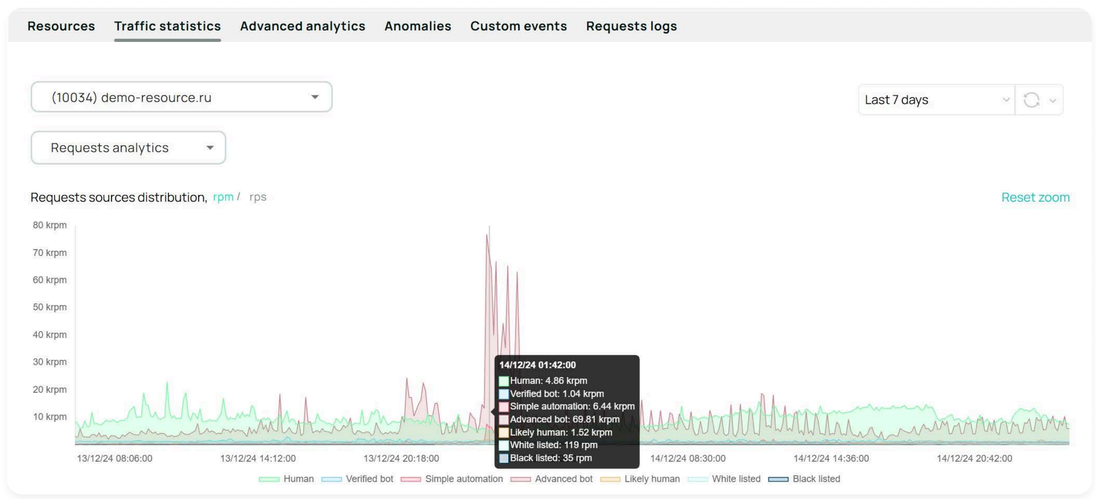
< 0,01 % ложноположительных срабатываний

< 10 минут подключение даже под DDoS-атакой

99,99 % SLA доступность систем фильтрации

24/7 режим работы SOC и NOC

- Бесшовная интеграция со всеми популярными решениями WAF на российском рынке: Вебмониторэкс, Positive Technologies и SolidLab
- Решение полностью автоматизировано — для его работы не требуется штатный специалист, доп. оборудование или широкие сетевые каналы
- Схема защиты без раскрытия SSL не требует анализа логов с веб-сервера



Разметка ботовых запросов в панели управления Servicepipe

О ПРОДУКТАХ ВЕБ-ЗАЩИТЫ SERVICEPIPE

Servicepipe защищает от любых высокочастотных и низкочастотных атак на L7, парсеров, сканеров уязвимостей, утилит для целевых атак (включая zero-day), массовых регистраций и брутфорса, фейковых заявок, SMS-бомберов, атак на бизнес-логику и любой другой нелегитимной автоматизации, включая угрозы из эталонных списков OWASP.

SERVICEPIPE CYBERT

Интеллектуальная система тонкой фильтрации трафика для защиты веб-приложений от DDoS-атак, ботов (включая продвинутых) и целевых угроз

- Поддержка WebSocket, gRPC, IPv6, HTTP/2 и ГОСТ-сертификатов
- Пользовательские правила фильтрации
- Непрерывное дообучение под контролем экспертной команды аналитиков
- Оперативное реагирование 24/7 команды техподдержки

ЧТО ГАРАНТИРУЕТ ВЫСОКУЮ ТОЧНОСТЬ ЗАЩИТЫ

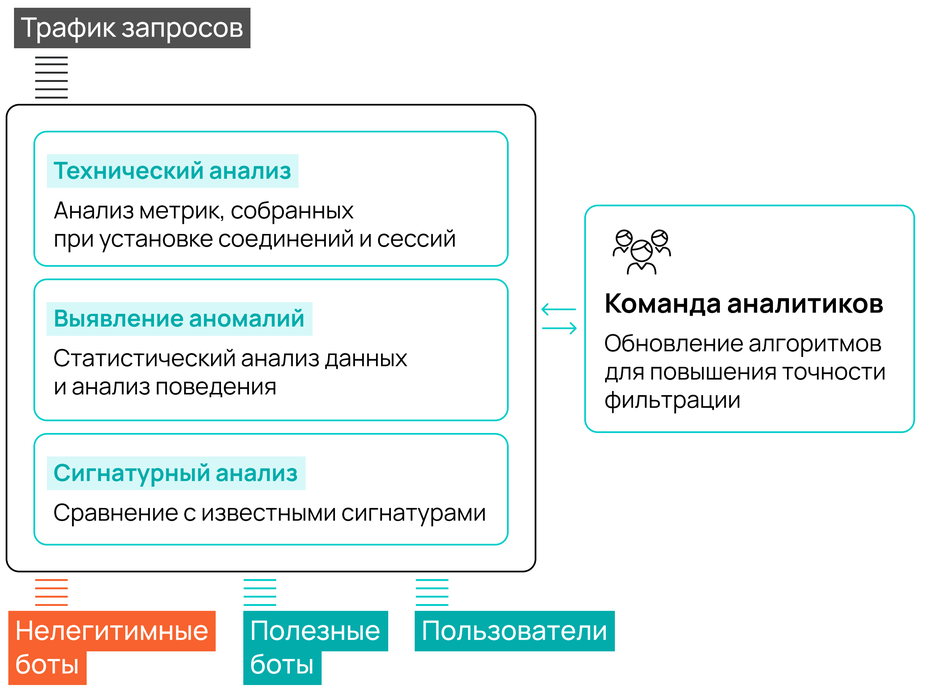
МНОГОФАКТОРНЫЙ АНАЛИЗ

Вердикт «бот/человек» выносится на основе многофакторного позапросного анализа трафика в реальном времени. Анализируются технические и статистические параметры запроса, сигнатуры и поведенческие факторы:

- Входящий трафик непрерывно анализируется на наличие статистических аномалий
- При получении очередного запроса проводится базовый технический анализ его источника
- Если запрос из данного источника является не первым в наблюдаемом интервале времени, вычисляются поведенческие факторы пользователя, последовательность действий пользователя сравнивается с заданной легитимной моделью
- Запрос сопоставляется с сигнатурами, актуальными для ресурса в данный момент, при этом могут учитываться факторы — как совпадение, так и «близость»
- Полученная информация комбинируется в вектор факторов, на основе которого вычисляется легитимность запроса
- Для повышения точности осуществляется контроль со стороны команды аналитиков

ПОЗАПРОСНАЯ ФИЛЬТРАЦИЯ

Мы выявляем и блокируем любую нежелательную автоматизацию с самого первого вредоносного запроса, не блокируем по IP-адресам и мгновенно детектируем даже низкочастотные атаки, которые сложно обнаружить статистическими методами.



Пилот — лучшее доказательство нашей эффективности

welcome@servicepipe.ru +7 (495) 374-62-65