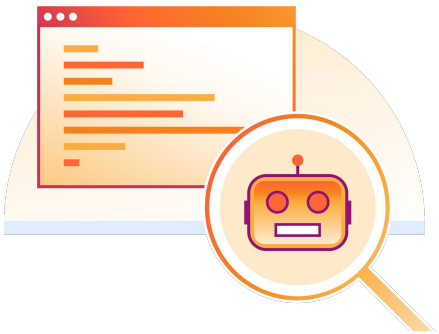
Cloudflare Bot Management (Управление ботами)

Блокируйте вредоносных ботов и управляйте ИИ-ботами без использования CAPTCHA.



Боты маскируются в вашем трафике. Вредоносные боты вредят доходам и удобству пользователей.

30 % трафика приложений в Интернете является автоматизированным трафиком[1]. Традиционные средства защиты, такие как эвристический алгоритм на основе географии и IP-адреса, а также запросы CAPTCHA, легко обходят современные боты. Это сильно расстраивает реальных пользователей.

Благодаря мониторингу **~20 %** веб-страниц, никто не распознает больше программ-обходчиков на базе ИИ и поисковых ботов, чем Cloudflare[2].

Cloudflare Bot Management помогает организациям управлять трафиком программ-обходчиков на базе ИИ и ботов, поступающим на веб- и мобильные приложения без использования CAPTCHA. Разрешите проверенным ботам и совместимым с ИИ программам-обходчикам доступ к приложениям, одновременно блокируя несовместимых и вредоносных ИИ ботов. Это ключевая возможность в нашем портфеле сервисов для защиты приложений.

Преимущества продукта

- Защита от мошенничества, финансовых потерь и ущерба бренду
- Обеспечьте лучшее качество работы веб-приложений и мобильных приложений
- Обеспечьте независимость от нежелательных программ-обходчиков на базе ИИ и поисковых ботов

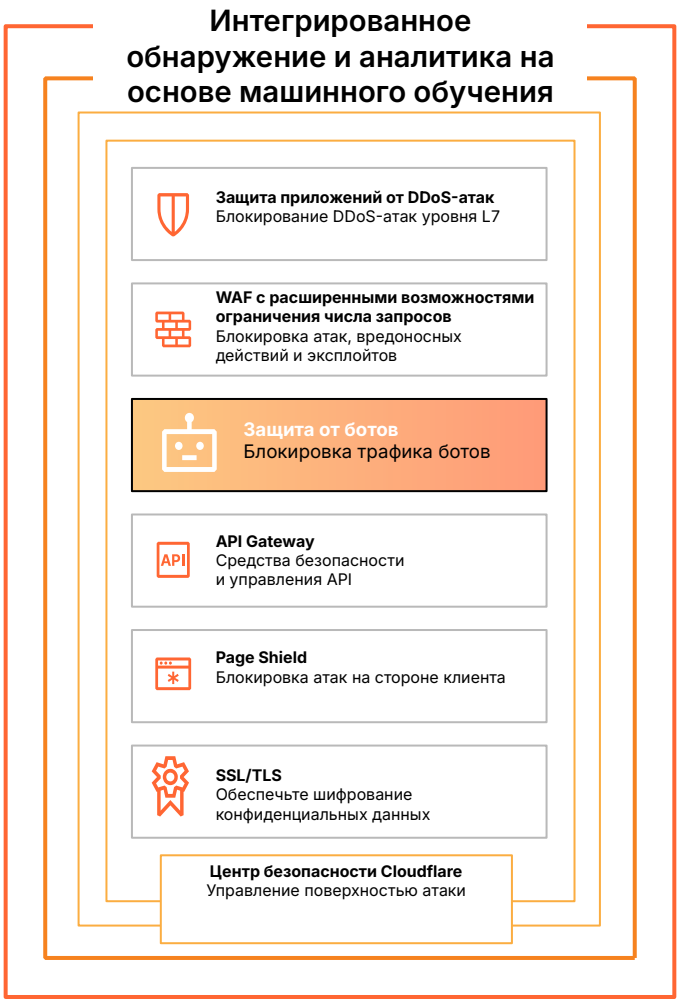


Рисунок 1: Cloudflare Bot Management (Управление ботами), интегрированное в наш портфель средств защиты приложений

Источники

1. Данные Cloudflare Radar, 2024 г.
2. W3techs, статистика использования и доли рынка сервисов обратного прокси-сервера, 2025 г.

Принцип работы Cloudflare Bot Management (Управление ботами)

Cloudflare объединяет многоуровневое обнаружение, использующее глобальное и зависящее от приложений машинное обучение, клиентский JavaScript, мобильные устройства и эвристические алгоритмы, в единую оценку для ботов, присваиваемую каждому HTTP-запросу. Оценка бота показывает, насколько вероятно, что запрос поступил от бота. Эта оценка бота используется для стандартных ответов, таких как блокировка или разрешение, а также для пользовательских политик ответа в других продуктах Cloudflare. Аналитика ботов, в том числе оценка ботов, метаданные HTTP-запросов и другие данные, доступны в пользовательском интерфейсе панели управления Cloudflare или через API Cloudflare в сторонних инструментах.

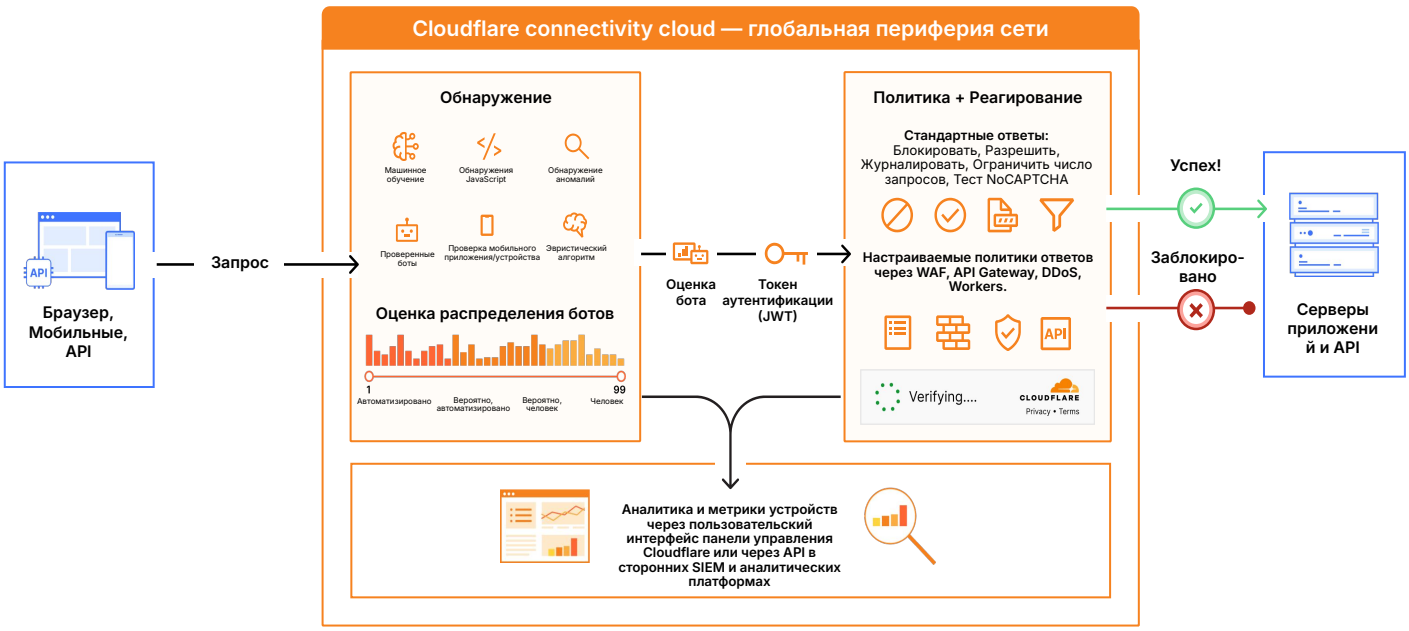


Рис. 2. Пример пути запроса через Cloudflare Bot Management (Управление ботами)

Основные возможности Cloudflare Bot Management (Управление ботами)

Захваты учетных записей и вредоносные действия

Защита от атак нулевого дня (zero-day) обеспечивается моделями машинного обучения, которые обнаруживают уязвимости быстрее, чем это становится известно из публичных источников. Обеспечьте защиту от рекордных DDoS-атак, защитите конфиденциальные данные, снизьте риски на стороне клиента и отслеживайте цепочку поставок программного обеспечения для ваших веб-приложений.

Защита от ботов и мошенничества

Защитите своих пользователей от захвата учетных записей и остановите вредоносных ботов, ухудшающих взаимодействие с пользователем. Остановите вредоносные ботнеты, подстановку учетных данных и карт, скрапинг контента и скупку или резервирование товаров, объединив модели машинного обучения с данными о клиентах, сети и сбор и анализ информации об угрозах.

Управление программами-обходчиками и ботами на базе ИИ

Обеспечьте более строгий контроль над контентом и затратами, блокируя программы-обходчики на базе ИИ, взимая с них плату или заманивая их в бесконечные циклы. Обеспечьте прозрачность шаблонов запросов и соответствие директивам robots.txt. Доступно всем клиентам Cloudflare.

Ключевые возможности	
Механизмы обнаружения	
Машинное обучение	Наша глобальная модель машинного обучения обучается на трафике всей глобальной сети Cloudflare, ежедневно проксирующей миллиарды запросов, для выявления автоматизированного и пользовательского трафика. Это включено в наш общий балл бота. Клиенты автоматически обновляются до последней версии.
Обнаружение аномалий	Наши модели поведенческих аномалий, использующие неконтролируемое обучение, определяют базовые шаблоны трафика для конкретных приложений и настраивают пороговые значения правил, чтобы выявлять аномальное поведение ботов по мере изменения шаблонов трафика клиентов. Это включено в наш общий балл бота.
Эвристический алгоритм	Для выявления ботов мы используем известные паттерны вредоносного поведения, основанные на предыдущем трафике ботов. Мы регулярно обновляем наши эвристические алгоритмы для всех клиентов. Это включено в наш общий балл бота.
Проверенные боты и боты на основе ИИ	В нашем каталоге ботов указаны известные идентификаторы обнаружения ботов, которые выполняют легитимные функции и прозрачно работают как проверенные боты в соответствии с политикой Cloudflare для проверенных ботов. У нас есть отдельная категория для известных ИИ-ботов, которая может учитывать или не учитывать robots.txt и скрывать свои действия от ваших приложений.
Обнаружение JavaScript	Модуль обнаружения JavaScript выявляет консольные браузеры и другие вредоносные цифровые отпечатки посредством легкой, незаметной JavaScript-инъекции на стороне клиента при каждом запросе. Мы придерживаемся очень строгих стандартов конфиденциальности и не собираем никакой персональной идентифицирующей информации в ходе этого процесса.
Оценка бота	Используйте оценку бота, чтобы создавать меньше правил для обнаружения большинства ботов, вместо создания правила для каждого идентификатора или типа. Оценка бота объединяет аналитические данные наших систем обнаружения для получения оценки от 1 до 99, которая показывает, насколько вероятно, что запрос поступил от бота. 1 оценка относится к определенно автоматическим запросам, а 99 относится к определенно человеческим запросам.
Проверка устройства с использованием SDK для мобильных устройств	Эти SDK для всех основных платформ мобильных приложений, включая Android, iOS, React Native, Unity и другие, проверяют целостность приложений, обнаруживают небезопасные среды и аутентифицируют трафик API (с помощью самостоятельно предоставляемых или одобренных Cloudflare криптографических токенов).
Политика и реагирование	
Стандартные ответы	Настройте блокировку, разрешение, ведение журнала, ограничение скорости или различные удобные проверки как ответы на трафик ботов, обнаруженный нашими механизмами обнаружения.
Политики пользовательских вариантов реагирования	Интегрируйте сигналы управления ботами в политики других продуктов Cloudflare, таких как Cloudflare WAF и DDoS, и создавайте собственные действия с помощью Workers.
Аналитика	
Информационная панель Cloudflare	Просматривайте активность ботов за последние 30 дней и фильтруйте по оценке ботов и другим ботам, трафику ботов и фильтрам запросов. Цикл обратной связи с ботами позволяет клиентам сообщать в Cloudflare о любых ложноположительных или ложноотрицательных результатах для дальнейшего расследования.
Сторонние инструменты (SIEM, озеро данных, инструменты аналитики и т. д.)	Анализируйте сигналы управления ботами во всех своих приложениях на единой панели управления с помощью сервисов безопасности Cloudflare Analytics, изучайте дополнительные данные журналов в Log Explorer и объединяйте сторонние данные с данными Cloudflare на сторонней платформе SIEM или аналитики через Log Push.

Готовы узнать больше? Зарегистрируйтесь для участия в нашей серии демонстраций по безопасности приложений.