

Управління ботами від Cloudflare для туристичних компаній

Розпізнайте та зупиніть три найпоширеніші бот-атаки в туристичній галузі та захистіть довіру до вашого бізнесу.



Шкідливі боти складають понад 40% всього трафіку на сайтах авіакомпаній та туристичних сайтах. Якщо їх не зупинити, вони можуть заблокувати бронювання та здійснити шахрайські транзакції, що може значно зменшити ваш дохід, а також знизити довіру клієнтів до вашого бренду. Cloudflare Bot Management застосовує автоматизовані, розумні, засновані на даних підходи, щоб зупинити цих ботів на їхньому шляху.

Чому управління ботами важливе

Запобігайте крадіжці даних вебсайту

Боти, націлені на туристичну галузь, можуть викрасти списки квитків і номери готелів з вашого сайту, а потім розмістити ту саму інформацію на сайті, який вони контролюють. Це може дозволити сайтам конкурентів випередити вас у пошуковій видачі.

Заощаджуйте на втрачених доходах і компенсаціях клієнтам

Боти створюють серйозні перешкоди для клієнтів, ускладнюють процес покупок, що негативно впливає на дохід компанії. Коли бот заволодіває акаунтом реального клієнта і здійснює шахрайські транзакції, туристичні компанії змушені компенсувати збитки. Це коштує їм мільйони доларів щороку.

Збережіть довіру до бренду

Коли клієнти втрачають віру та довіру до бренду, який зазнав атак, вони просто звертаються до конкурентів. Обдурені клієнти можуть публічно розповісти про свій негативний досвід у соціальних мережах або звернутися до засобів масової інформації. Публічний скандал, пов'язаний із ботами, може серйозно підірвати довіру до вашого бренду на роки вперед.

Поширені бот-атаки в туристичній галузі

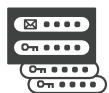
Тактика ботів, що націлені на туристичні компанії, може мати різні форми, але це одні з найпоширеніших:



Накопичення запасів, коли боти постійно додають квитки та бронювання до кошика, але ніколи не завершують покупку. Ця технологія блокує інвентар та не дає реальним клієнтам змоги придбати його, що негативно впливає на ваші продажі, доходи та користувацький досвід.



Вилучення контенту, коли боти автоматично витягують з вашого сайту контент, наприклад, інформацію про наявність вільних місць, а потім розміщують його на сайті, котрий контролюється зловмисниками. Це часто робиться для того, щоб підвищити пошуковий рейтинг сайтів ваших конкурентів.



Наповнення облікових даних, коли боти заволодівають обліковими записами користувачів, автоматично застосовують раніше викрадені облікові дані. Ці фейкові акаунти можуть бути використані для здійснення шахрайських транзакцій або викрадення персональних даних, які згодом продаються в даркнеті.

Ключові особливості

ПРОСТЕ РОЗГОРТАННЯ

В один клік розгортайте швидко і точно рішення для управління ботами без складної конфігурації та обслуговування.

Bot Management

Automatically enables custom firewall rules and the `_cf_bm` cookie on your zone to manage incoming traffic that matches criteria associated with bots.

On

When incoming requests match...

Use expression builder

```
(ip.src ne 2601:625:c100:200c:988c:105d:3f1c:f557 and http.referer eq "cloudflare.com" and http.request.uri.path eq "/login" and http.user_agent ne "1.1.1.1 iOS App" and not cf.client.bot and score le 30)
```

Then...

Choose an action

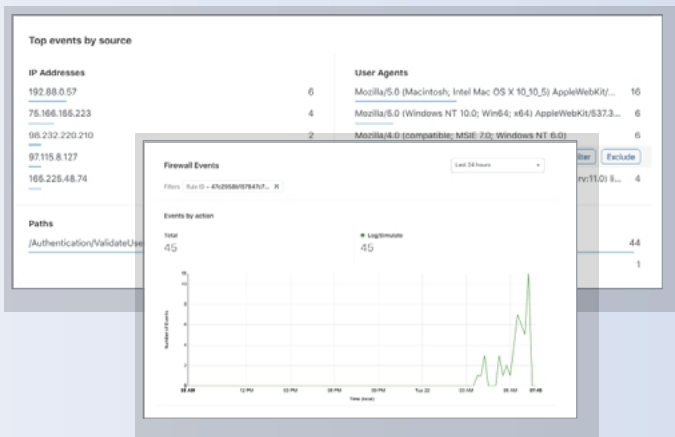
Challenge (Captcha)

КОНТРОЛЬ І КОНФІГУРАЦІЯ

Налашуйте правила управління ботами відповідно до ваших конкретних потреб, що постійно змінюються. Визначайте правила з різними атрибутами, такими як: конкретний шлях або шаблон URI, метод запиту, чутливість оцінок. Створіть індивідуальні методи пом'якшення наслідків, включаючи журнал, капчу, блокування або альтернативний контент.

БАГАТА АНАЛІТИКА ТА ЖУРНАЛИ

Отримуйте аналітичну інформацію за допомогою дашбордів, які допомагають підвищувати ефективність рішення завдяки графікам часових рядів із можливістю деталізованого перегляду. Логи містять дані про спрацювання правил, виконані дії та розширену метадані про кожен запит, що дозволяє вам аналізувати стан безпеки за допомогою сторонніх інструментів, таких як SIEM системи або програми бізнес-аналітики.



Відмінність Cloudflare

Без правильних інструментів управління ботами може стати виснажливою і дорогою справою. Cloudflare Bot Management має три ключові відмінності:



Масштабна розвідка загроз

Точно ідентифікуйте ботів, застосовуючи поведінковий аналіз, машинне навчання та дактилоскопію до різноманітних і великих обсягів глобально розподілених даних.



Інтегрована безпека та продуктивність

Рішення Cloudflare для управління ботами легко інтегрується з продуктами WAF, DDoS і CDN, що підвищує безпеку, зручність користування та продуктивність.



Повнота без складності

Миттєве розгортання та захист від повного спектру бот-атак без впровадження Javascript та мобільного SDK.

iIT Distribution є офіційним Value Added дистриб'ютором, який постійно розвивається у сфері проєктної дистрибуції складних B2B рішень в Україні, Польщі та країнах Балтії. Ми представляємо програмні рішення від провідних світових постачальників. Наша місія полягає в тому, щоб забезпечити організації будь-якого розміру сучасними можливостями IT-інфраструктури, забезпечуючи їхній захист від переважаючих загроз інформаційної безпеки.

E-mail: sales.ua@iitd.io | Більше інформації на сайті: <https://iitd.ua/>