

How Kasada Protects Airlines from Scraping Attacks & Loyalty Fraud

The Growing Threat Landscape

Adversaries exploit bot-driven attacks to scrape fares, interfere with dynamic pricing, and harm customers by taking over accounts and stealing rewards.

Airline Success Story

CHALLENGE

A multi-billion dollar airline faced scraping from unauthorized Online Travel Agencies (OTAs) - up to 99% of traffic on key endpoints was bots.

One OTA scraped for virtual interlining. When travelers' OTA bookings faced problems, they blamed the airline - a poor experience and brand image issue.

SOLUTION

Kasada integrated with the airline for a 30-day Proof of Concept period to prove its efficacy vs. the current CDN-based bot mitigation vendor.

IMPACT

Uncovered the unauthorized OTA and shut down its scraping. Improved site speed and stability by 30%. Better site experience encourages direct bookings and supports company's stated goal of owning its customer relationships.

1.2%

of an airline's revenue is lost to web and mobile fraud.

Airlines are tempting targets due to vast amount of sensitive customer and payment data handled.

Source: International Air Transport Association

Problems Faced



SCRAPING

Steals fare data without permission or compensation and reselling elsewhere



ACCOUNT FRAUD

Fake account creation and ATOs steal customer data and loyalty/rewards points

Business Impacts

STOCK HOARDING

Bots buy up inventory and release unsold reservations at the last minute

SKEWED METRICS

Bot traffic pollutes the data, yielding inaccurate conversion rates and demand forecasts

HIGHER COSTS

Scraping drives excessive PSS and API queries to keep up with dynamic pricing

LOYALTY/ REWARDS FRAUD

Attackers obtain points to fraudulently book travel for themselves or others



Stop scraping and loyalty fraud

SEE KASADA IN ACTION ►

