

Travel Booking Site Cuts Malicious Bot Traffic by 99% and Raises Look-to-Book Ratio from 1% to 6% with Arkose Titan

One of the world's largest travel booking sites, serving both consumer and business travelers across hotels, airfare, car rentals, cruises, and more. A high-value target for bad actors deploying bots at scale to scrape pricing and inventory data.



The Challenges

Tens of millions of malicious bots hitting the site per day, scraping data without making purchases.

Bot traffic drove the look-to-book ratio down to approximately 1%, below the thresholds required by contractual agreements with airline and hospitality providers.

Massive daily bot volume created significant strain on cloud infrastructure, driving up server costs and creating operational inefficiency.

Needed a solution that stopped automated scraping without disrupting the experience for legitimate consumers.



The Arkose Titan Solution

Arkose Titan was deployed across new user registration, login flows, and the search API that bots were directly targeting.

Automated traffic was detected in real time and served adaptive enforcement challenges designed to stop scripted and bot-driven activity.

Nearly all bot traffic was unable to load the challenge at all, preventing access to the site entirely.

Legitimate consumers passed through without disruption, preserving the site's reputation for a seamless digital experience.

The Arkose Global Intelligence Network contributed cross-network threat data to strengthen detection.



Business Results

Malicious bot traffic reduced by more than 99% following deployment.

Look-to-book ratio increased from 1% to over 6%, satisfying contractual requirements with airline and hospitality providers.

Cloud server strain significantly reduced, improving operational efficiency and lowering infrastructure costs.

Legitimate consumer experience fully preserved throughout.

**SCHEDULE CALL
WITH AN EXPERT**

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America. © 2026 Arkose Labs. All rights reserved.