eBook

THALES
Building a future we can all trust

CYBERSECURITY

imperva

Bad Bots in the Travel Industry

Think of bots as hidden passengers in your systems.

They don’t queue at check-in or pay for tickets, but they consume resources, distort demand, and drain revenue.

Table of Contents

Introduction

Every minute, automated bots are stealing seats, scraping prices, and draining loyalty value from travel platforms. Whether you're new to understanding the role of bots in the travel industry or already well-versed in digital fraud, this eBook is designed to give you a clear, business-focused view of the risks and how to stay ahead of them. It's not a technical manual, but a guide to recognizing the growing impact of bots on airlines, hotels, booking platforms, car rentals, and cruise lines, and how to chart a stronger path toward protection.

Bots aren't just background noise in travel web traffic. They actively target the systems that power modern customer experiences, loyalty programs, booking APIs, inventory management, and payment flows. While some automated traffic is benign (such as search engines indexing sites), the majority that matters to travel businesses comes with malicious intent. Attackers use bots to steal customer data, siphon loyalty rewards, manipulate prices, hoard inventory, and disrupt operations.

Think of bots as hidden passengers in your systems. They don't queue at check-in or pay for tickets, but they consume resources, distort demand, and drain revenue. And unlike human travelers, they never stop. Bots operate at scale, around the clock, and now, with AI, mimic real users so effectively that traditional defenses often fail to detect them.

Unless otherwise stated, the data in this report covers traffic to Thales Imperva customer sites in five key travel categories; airlines, hotels and accommodation, booking & travel platforms, car rental & ground transportation, and cruise lines & maritime—from **January to July 2025.**

This eBook explores:

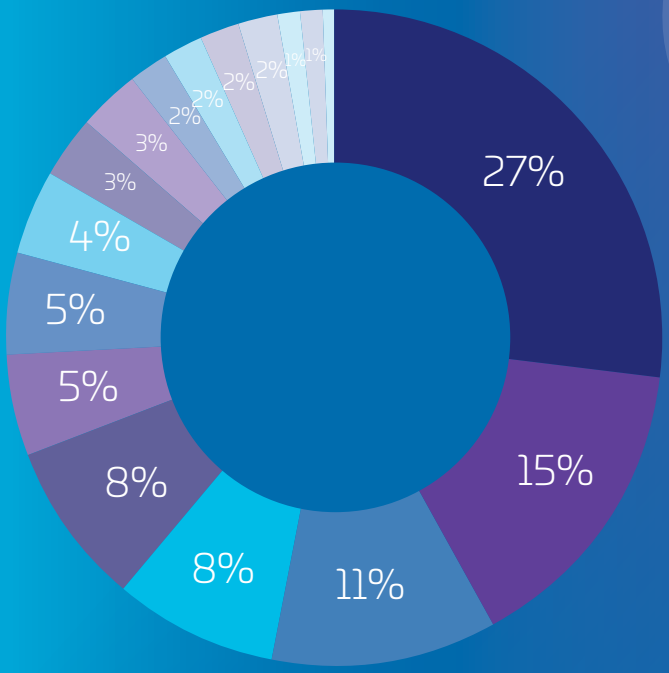
1. **The Bot Threat Landscape in Travel**
   How automation is reshaping risk across the sector
2. **APIs as a Target**
   Why the digital backbone of travel is also its biggest vulnerability
3. **Account Takeover (ATO)**
   Why loyalty and booking accounts are prime targets
4. **Industry Breakdowns**
   How different subsectors face distinct challenges

The more digital and connected the travel experience becomes, the more attractive it is to attackers. By understanding the attack vectors and learning how automation is abused, you'll be better equipped to protect your business and your customers.

Industry Overview

The impact of bot traffic and automated cyberattacks on the travel sector continues to grow, making it one of the most attractive targets for threat actors. Why? Because the stakes are high. The industry is thriving, has a wide global reach, spans multiple sub-sectors of commercial travel and tourism, and processes an enormous volume of financial transactions. For attackers, that means the potential return on investment is significant.

According to the Thales Imperva Bad Bot Report, travel accounted for 27% of all bot attacks in 2024, up from 21% the year before. In 2024, nearly half (48%) of traffic to travel sites consisted of bad or malicious bots, rising from 44% the previous year.



TOP TARGETED INDUSTRIES

- Travel
- Retail
- Education
- Financial Services
- Business
- Computing & IT
- Healthcare
- Law & Government
- Telecom & ISPs
- Gaming
- Automotive
- Lifestyle
- Society
- Food & Groceries
- Entertainment
- Gambling
- Sports
- News

What does this tell us?

It shows that despite increased awareness and security investment, travel remains the number one industry targeted by bots. This is because attackers see it as the perfect combination of opportunity and vulnerability: a highly digital ecosystem, millions of daily customer interactions, frequent logins and bookings, high-value personal and financial data, and reliance on real-time availability.

Adding fuel to the fire, AI has become a significant accelerator. Attackers are now using AI-powered bots that can mimic human behavior, evade detection, and scale attacks at speed. This makes credential stuffing, price scraping, loyalty fraud, and inventory hoarding even harder to spot and stop.

In short, travel offers the richest rewards for automated attacks. Until security strategies evolve as fast as AI-driven threats, it will remain a prime target.

BACK TO TABLE OF CONTENTS

Travel Category – Definitions

AIRLINES
Airlines and aviation-related sites

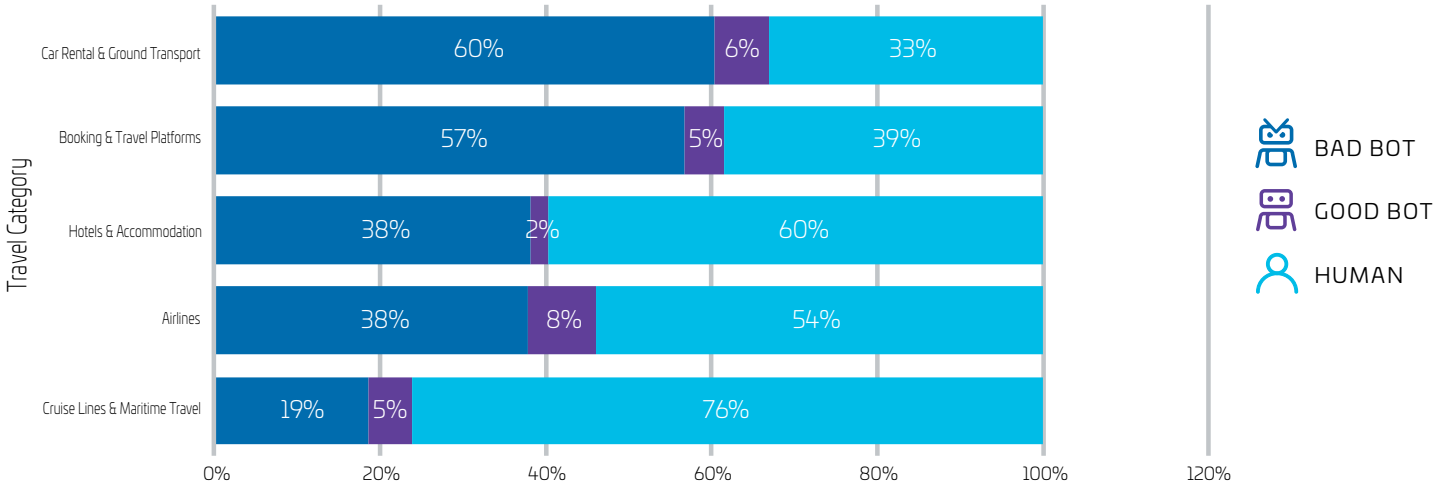
CAR RENTALS & GROUND TRANSPORT
Car rental agencies, bus travel, taxis, ground transportation sites

BOOKING & TRAVEL PLATFORMS
Travel agencies, guided tours, travel insurance

HOTELS & ACCOMMODATIONS
Primarily hotels; can include hostels, short-term holiday letting sites

CRUISE LINES & MARITIME TRAVEL
Cruise lines, sailboat tours, river cruises

BAD BOTS VS GOOD BOTS VS HUMAN BY TRAVEL CATEGORY



TOP 5 MOST TARGETED COUNTRIES

54%	9%	8%	2%	2%
UNITED STATES	AUSTRALIA	UK	CANADA	NETHERLANDS

ACCOUNTING FOR 70% OF ALL ATTACKS ON THE TRAVEL SECTOR

APIs – Connecting Modern Travel

APIs are the digital backbone of modern travel. They connect airlines, hotels, booking platforms, car rentals, and cruise lines, powering everything from flight scheduling and room availability to mobile check-ins, loyalty programs, and real-time payments. For travelers, APIs make journeys seamless. For businesses, they unlock efficiency, agility, and new revenue streams.

But APIs are also under attack. Bad bots target them relentlessly, not just overwhelming endpoints with traffic but exploiting the very business logic that powers critical operations. **Business logic abuse, responsible for 34% of all attacks on travel APIs**, is now the most common threat facing the sector.

Why does this matter? Because business logic defines how APIs process bookings, manage payments, validate loyalty points, and allocate inventory. When bots manipulate these rules, the impact goes far beyond system strain. It strikes at the core of how travel companies operate and serve customers.

BUSINESS LOGIC ABUSE IS RESPONSIBLE FOR

34%

OF ALL ATTACKS ON TRAVEL APIs

Examples include:

INVENTORY HOARDING
Bots block flights, hotel rooms, or car rentals to distort pricing and availability.

ACCOUNT TAKEOVER
Attackers test stolen credentials on booking platforms and loyalty programs.

DATA SCRAPING
Competitors or fraudsters harvest pricing and availability data at scale.

FRAUDULENT TRANSACTIONS
Automated abuse of payment and rewards systems siphons revenue and damages trust.

For an industry built on real-time interactions, even short-lived disruptions can have cascading effects: including lost sales, frustrated travelers, higher operational costs, and reputational harm.

What does this signify?

That APIs, while essential to the travel experience, are also the sector's most exposed attack surface. Business logic abuse highlights how attackers are shifting from brute-force attacks to precision strikes that exploit the rules of the business itself. Defending APIs requires more than perimeter protection; it demands security that understands and protects the logic at the heart of travel operations.

BACK TO TABLE OF CONTENTS

Most Common API Threats – All Categories

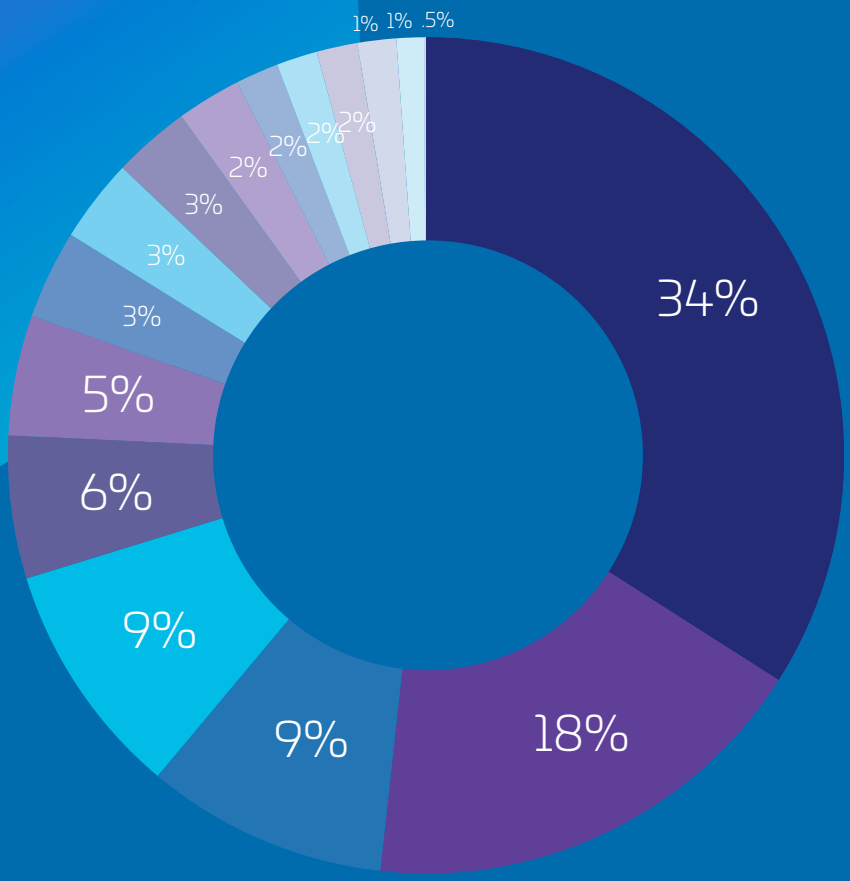
34%
BUSINESS LOGIC ABUSE

18%
DATA LEAKAGE

9%
API VIOLATION

9%
RCE / RFI

6%
PATH TRAVERSAL



MOST COMMON THREATS TO TRAVEL APIs

- Business Logic Abuse
- Data Leakage
- API Violation
- Remote Code Execution (RCE)/ Remote File Inclusion (RFI)
- Path Traversal / Local File Inclusion (LFI)
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Automated Attack (Bot Activity)
- Protocol Manipulation
- Authentication Bypass
- Backdoor/Trojan Infection
- Server-Side Request Forgery (SSRF)
- Miscellaneous (MISC)
- Malicious File Upload
- Account Takeover (ATO)
- Distributed Denial of Service (DDoS)

BACK TO TABLE OF CONTENTS

Account Takeover in Travel

Account Takeover (ATO) attacks remain one of the most persistent threats to the travel industry. The reason is simple: for attackers, **the return on investment is high.**

Think about the sheer volume of accounts tied to travel services. Airlines run frequent flyer programs, hotels operate loyalty and rewards schemes, booking platforms hold stored payment details, car rental firms manage membership discounts, and cruise lines offer passenger loyalty benefits. These accounts are treasure troves, rich with personal information, stored credit card data, travel itineraries, and valuable points or miles that can be resold on the dark web.

For attackers, the incentive is clear:

MONETIZATION OF REWARDS

Airline miles and hotel points can be converted into flights, room nights, or even cash-equivalent vouchers.

STORED VALUE

Many accounts store credit card details or prepaid balances, making them easy targets for fraudulent purchases.

TRAVEL PERKS

Premium memberships often include lounge access, upgrades, and discounts—all benefits that can be exploited or resold.

IDENTITY DATA

Travel accounts typically hold passport details, addresses, and phone numbers—valuable for identity theft and wider fraud campaigns.

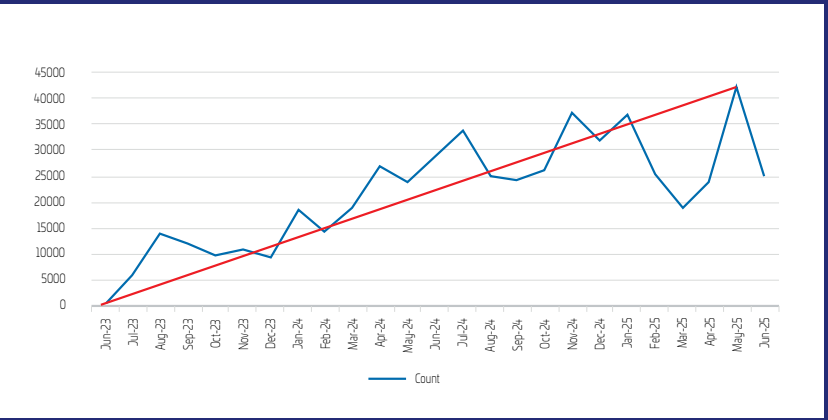
The travel industry also presents another advantage for attackers: **High volumes of customer logins and transactions happening in real time.** With millions of users constantly booking, checking in, or redeeming points, automated credential-stuffing attacks can blend in without immediately triggering suspicion.

Bottom Line

Travel accounts represent more than just a booking record. They're digital wallets of personal data, loyalty value, and financial information. Until stronger protections are in place, ATO will remain one of the most common and profitable attack vectors in the industry.

The following chart shows the growth of ATO attacks targeting the travel sector from June 2023 to June 2025.

ATP ATTACKS ON TRAVEL - JUN 23 TO JUN 25

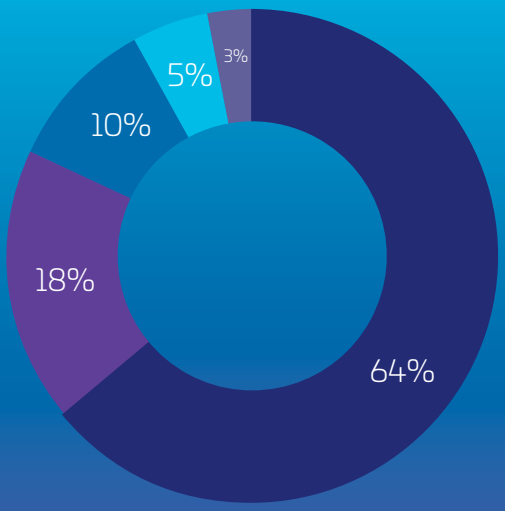


ATTACKS HAVE INCREASED

x50

OVER THE LAST TWO YEARS

Source: Imperva Threat Research Data June 2023 to 2025



TOP TARGETED TRAVEL CATEGORIES

- Airlines
- Booking & Travel Platforms
- Car Rentals & Ground Transport
- Hotels & Accommodations
- Cruise Lines & Maritime Travel

Bots & the Airline Industry

Bot Challenges & Business Impact

Airlines are the most targeted sector in travel. According to Thales Imperva data, between January and August 2025, they accounted for 64% of all bot attacks across all travel sites.

64%
AIRLINES

18%
BOOKING PLATFORMS

10%
CAR RENTALS

5%
HOTELS

Attackers launch credential stuffing campaigns against frequent flyer programs, scrape fare data, hoard seat inventory, and abuse verification systems with SMS pumping. These activities directly translate into lost loyalty value, distorted seat availability, inflated infrastructure spend, and reputational damage.

Benefits of Bot Protection

Secure loyalty programs and stored payment data

Stop fare scraping and revenue leakage

Prevent fake booking and inventory hoarding

Reduce SMS pumping costs

Ensure accurate forecasting and preserve customer trust

Common Threats

CREDENTIAL STUFFING
Frequent flyer accounts are goldmines of loyalty points, stored payment details, and personal information.

FARE SCRAPING
Competitors or fraudsters harvest real-time pricing and availability to gain unfair advantage.

SMS PUMPING
Attackers flood mobile verification systems with fake requests.

INVENTORY HOARDING
Fake bookings and seat holds distort revenue management systems.

THE IMPACT IS CLEAR

Revenue loss from fraudulent activity, erosion of customer trust when loyalty accounts are compromised, and increased infrastructure costs to process waves of automated traffic.

In 2025,

85% OF AIRLINE BOT ATTACKS TARGETED BUSINESS LOGIC,

showing a decisive shift away from brute-force attacks towards precision exploits of booking and pricing APIs.

BACK TO TABLE OF CONTENTS

Booking & Travel Platforms

Bot Challenges & Business Impact

Booking platforms and Online Travel Agencies (OTAs) rely heavily on APIs to deliver real-time pricing and availability from hundreds of suppliers. This dependence makes them prime targets for bot attacks that exploit those APIs by scraping fares, abusing booking engines, and inflating traffic volumes. In some cases, scraping traffic has been observed making up over 90% of visits to travel sites *(The Hacker News)*.

Look-to-Book Ratio

Measures how many travel searches ("looks") convert into actual bookings ("books"); high ratios indicate lots of browsing but low conversion rates.

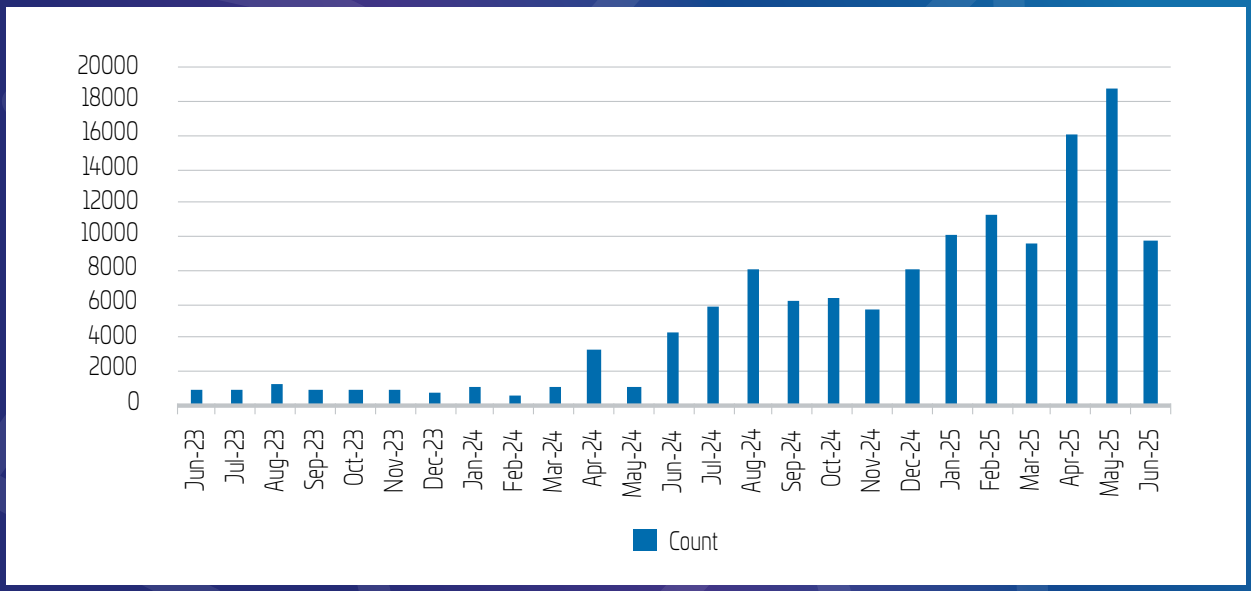
Bot-driven API abuse skews look-to-book ratios, drives up API and Global Distribution System (GDS) costs undermining customer experience, creating false demand signals and eroding trust.

Bot attacks targeting APIs in Booking Platforms and Aggregators more than doubled in the last 12 months increasing by

131%.

BACK TO TABLE OF CONTENTS

BOTS TARGETING BOOKING PLATFORM APIs



Benefits of Bot Protection for Booking Platforms

- Defend APIs against scraping and automated abuse
- Reduce inflated API/GDS costs
- Preserve pricing integrity across supplier networks
- Ensure reliable performance for customers and partners
- Protect revenue from fraudulent and fake bookings

BACK TO TABLE OF CONTENTS

Hotels & Accommodation

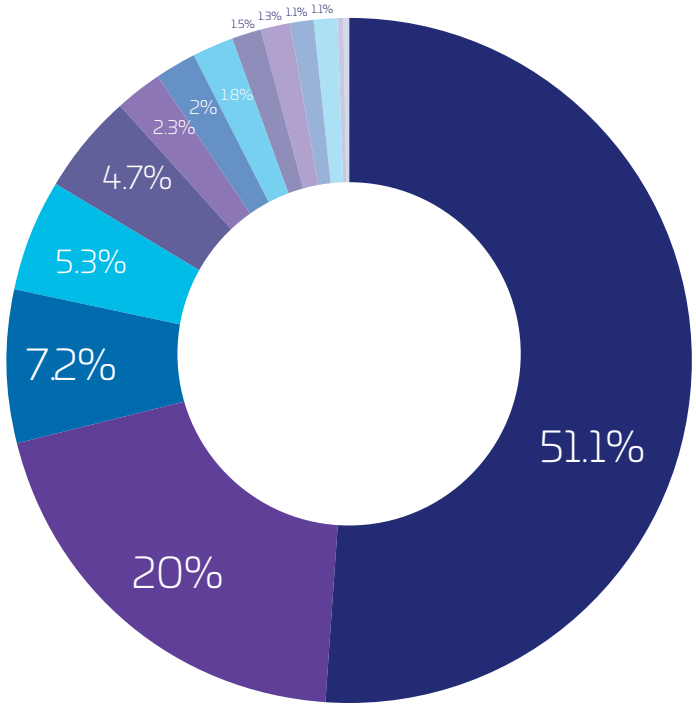
Bot Challenges & Business Impact

Hotels are prime targets for **business logic abuse** (when bots exploit the intended rules of your booking or payment system to gain unfair advantage). According to Thales Imperva data, in 2025, 51% of all attacks against hotel and accommodation APIs involved **business logic abuse.** Bots also scrape room rates from distribution partners and flood reservation systems during peak periods.

Why hotels? Because their APIs expose high-value data and processes: real-time availability, dynamic pricing, loyalty points, and promotional codes. Attackers exploit these to steal customer value, gain competitive intelligence, or block inventory for resale.

Business Logic Abuse

When bots exploit the intended rules of your booking or payment system to gain unfair advantage.



MOST COMMON THREATS TO APIS - HOTELS & ACCOMMODATIONS

- Business Logic
- Data Leakage
- Automated Attack
- RCE/RFI
- Path Traversal/LFI
- XSS
- Protocol Manipulation
- Authentication Bypass
- SQLi
- SSRF
- Backdoor/Trojan
- File Upload
- .3% MISC
- .2% Account Takeover
- 0% DDoS

Common Bot Tactics

- Scraping room rates and availability from booking partners
- Abusing loyalty programs through credential stuffing and reward theft
- Exploiting promotional codes and discounts at scale
- Fake inventory holds to block rooms and disrupt availability
- Flooding reservation systems to degrade performance during peaks

Impact on Hotels

- Revenue leakage and competitive price undercutting
- Distorted occupancy forecasts and poor yield management
- Loyalty fraud and financial loss
- Erosion of guest trust and brand reputation
- Fake inventory holds to block rooms and disrupt availability

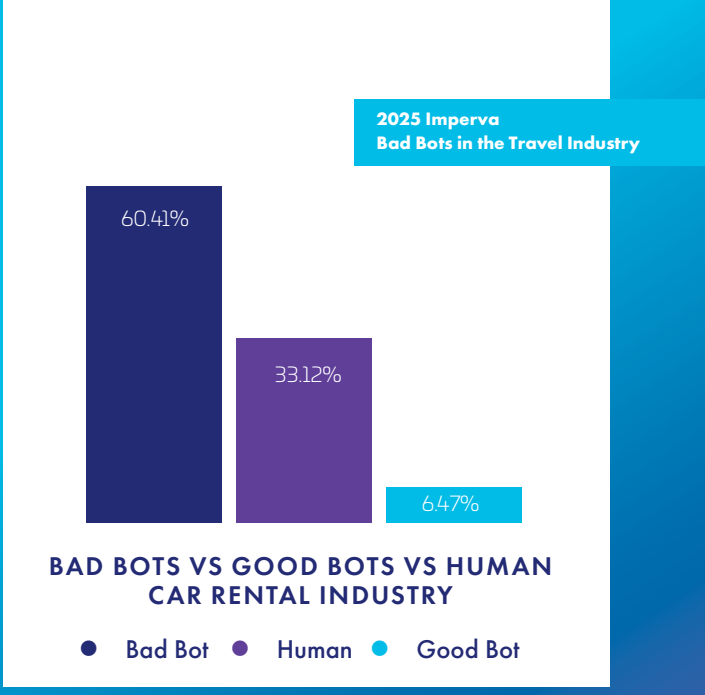
Benefits of Bot Protection

- Defend APIs against scraping and logic abuse
- Protect loyalty programs and guest accounts from takeover
- Preserve room availability and pricing integrity
- Reduce fraud losses from fake bookings and promo abuse
- Safeguard guest trust and maintain brand reputation

Car Rentals & Ground Transport

Bot Challenges & Business Impact

Car rental platforms are frequent bot targets due to their reliance on APIs for real-time vehicle availability, pricing, and promotions. Attackers scrape rates, hoard inventory, and exploit discount codes, causing distorted fleet utilization, blocked bookings, and unreliable demand forecasts. More than 60% of all traffic to Car Rental & Ground Transportation sites was made up of bad bots.



Common Bot Tactics

- Scraping vehicle rates and availability from rental sites and aggregators
- Hoarding inventory by placing fake or automated reservations
- Abusing promotional codes and discount offers at scale
- Credential stuffing against customer and loyalty accounts
- Flooding booking engines during peak travel periods

Impact on Car Rentals

- Lost revenue from fraudulent or blocked bookings
- Distorted fleet utilization and inaccurate demand forecasting
- Increased operational costs from inflated bot traffic
- Customer frustration due to unavailable inventory
- Erosion of trust and damage to brand reputation

Benefits of Bot Protection

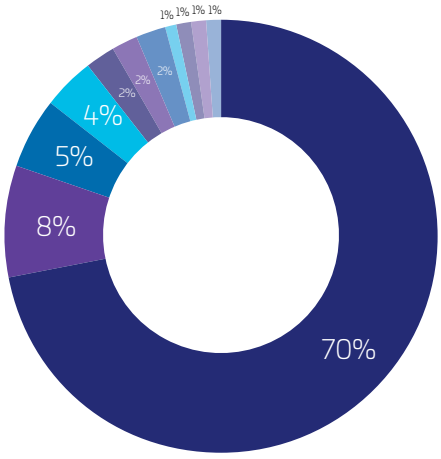
- Ensure fair vehicle availability for genuine customers
- Protect pricing strategies from large-scale scraping
- Block discount abuse and automated promo misuse
- Enable accurate fleet forecasting based on real demand
- Safeguard brand reputation by delivering consistent customer experiences

Cruise Lines & Maritime Travel

Bot Challenges & Business Impact

Cruise operators handle high-value, limited-inventory bookings, making them especially attractive to bot attackers. Common tactics include credential stuffing into loyalty accounts, scraping itineraries and cabin rates for resale, and exploiting promotions or testing stolen credentials. Since a single cruise can be worth thousands of dollars, even modest fraud levels can cause disproportionately large losses. Bots also distort demand signals, leading to poor yield management and frustrated passengers.

Unauthorized scraping of real-time cabin availability and pricing feeds is a growing problem for cruise operators, undermining revenue management, disrupting marketing alignment, and eroding guest trust.



MOST COMMON ATTACK TYPE - CRUISE LINES

- Business Logic
- Data Leakage
- Automated Attack
- RCE/RFI
- XSS
- Path Traversal/LFI
- SQLi
- Protocol Manipulation
- Backdoor/Trojan
- Spam
- Authentication Bypass

Benefits of Bot Protection

- Safeguard premium reservations from fraud and disruptions
- Ensure marketing promotions reach real customers, not bots
- Protect loyalty programs and passenger data
- Maintain passenger confidence and brand reputation
- Preserve booking accuracy across itineraries and cabins

Bot Threats Across Travel Sectors

SECTOR	MAIN CHALLENGES	BUSINESS IMPACT	BENEFITS OF PROTECTION
Airlines	Credential stuffing, fare scraping, inventory hoarding, SMS pumping	**64%** **of all travel bot attacks target airlines; revenue loss, loyalty theft, inflated SMS costs**	Protect loyalty programs, stop scraping, block fake bookings, cut SMS costs
Booking Platforms	Large-scale scraping, API abuse, account takeover	**Bots make up 50%+ of visits; fake bookings erode commission and partner trust**	Preserve pricing, reduce fraud, lower API costs, protect supplier data
Hotels	Loyalty fraud, booking manipulation, rate scraping	**Lost revenue, distorted occupancy forecasts, system slowdowns in peak season**	Secure loyalty points, stop fake cancellations, reduce API strain, protect guest trust
Car Rentals	Inventory hoarding, price scraping, promo abuse	**5–10%** **revenue loss in peak periods; blocked vehicles and skewed fleet allocation**	Ensure fair access, protect rates, stop discount fraud, optimize operations
Cruise Lines	Credential stuffing, itinerary scraping, promo exploitation	**High-value booking fraud; lost loyalty value; wasted marketing spend**	Safeguard premium reservations, secure loyalty, protect campaigns, preserve passenger trust

BACK TO TABLE OF CONTENTS

Conclusion

We hope this eBook has given you a clearer view of how bots are reshaping the travel industry, and why defending against them is no longer optional. From APIs to loyalty accounts, attackers are exploiting the very systems that make modern travel seamless, and the risks will only continue to grow.

The right bot protection strategy depends on your business priorities: safeguarding millions of frequent flyer accounts, preventing scraping of hotel and booking data, or keeping rental car inventory available for real customers. What is clear is that **static defenses are no longer enough.**

Introducing Thales Imperva Advanced Bot Protection (ABP)

ABP empowers travel businesses to stop malicious automation in real time, without disrupting genuine customer experiences. Using advanced detection, machine learning, and behavioral analysis, ABP detects even AI-driven bots that mimic human activity. The result: reduced fraud, preserved revenue, and stronger customer trust.

Security Analyst Services (SAS)

Thales Imperva's SAS team adds human expertise to automated protection, providing real-time adaptability, threat context, and continuous improvement to maximize your bot defense strategy.

Learn more: Thales Imperva Advanced Bot Protection

About Thales

The people you rely on to protect your privacy rely on Thales to secure their digital journeys. As organizations embrace digital transformation, Thales provides decisive technology for decisive moments, whether the challenge is bots, API protection, or online fraud prevention.

Evaluate how bots are impacting your business today, whether through lost bookings, scraped data, or compromised loyalty programs. Make a plan to modernize your defences and contact Thales for a free consultation: **Contact Thales**

THALES
Building a future we can all trust

CYBERSECURITY

imperva

Contact us

For all office locations and contact information,
please visit **cpl.thalesgroup.com/contact-us**

thalesgroup.com