IntelliFend

CASE STUDY

Shielding Ticketing and Reservation Platforms from AI Bot Attacks

Customer

International airline and sister hotel-booking platform

Industry

Travel & Hospitality

Challenge

- **Bot attacks** distorting demand data and inflating prices
- **Fake holds** blocking inventory from real customers
- **Account takeover** and loyalty points theft
- **Price scraping** for competitor undercutting
- **Payment fraud** causing chargebacks
- **Server overload** degrading booking performance

Result

- **98%** Booking Success: Fake Holds and Scalping Virtually Eliminated
- **60-70%** Reduction in Account Takeover Attempts
- **40%** Less Infrastructure Strain: Scraper Traffic Crushed
- **Zero** Compliance Violations Across All Audits
- **25%** Higher Customer Satisfaction + 12% Revenue Growth

OVERVIEW

An international airline and its sister hotel-booking platform faced a surge of AI-driven bots that distorted demand data, hoarded inventory, hijacked loyalty accounts, and jeopardized compliance with PCI DSS, IATA NDC, and regional privacy laws.

The engagement started with a proof of concept in detect-only mode, instrumenting VisitorTag across search and booking flows to baseline human vs. bot behavior. AccuBot then generated policy recommendations, including rate-limit thresholds, challenge triggers, crawler permissions, and a WAF Rule Advisory, which were reviewed with the client's infrastructure team.

Selected controls were implemented by the client on their CDN/WAF, while IntelliFend policies were activated gradually (monitor → challenge → block) within our enforcement layer. Throughout, Push Log was used to track each change and its impact, and thresholds were fine-tuned in real time based on live telemetry.

THE CHALLENGE: BATTLING SOPHISTICATED BOT ATTACKS ON BOOKING ENGINES

Revenue & Inventory Manipulation

As the travel brand entered its busiest season, phantom searches began to flood the booking engine, each one a carefully orchestrated strike by automated bots. These phantom availability checks misled the airline's revenue-management system into believing demand far exceeded reality—fares crept upward, and real customers were greeted with "sold out" messages, even when seats and rooms remained.

Meanwhile, behind the scenes, unscrupulous third parties scraped live fare and rate data in real time. Armed with these stolen prices, they reposted listings on Online Travel Agencies (OTAs) at a discount, undercutting official channels and siphoning off bookings that rightfully belonged to the airline and its hotel partner.

At the same time, another wave of bots employed inventory locking tactics, placing fake holds on seats and rooms as soon as they became available. Genuine travelers, eager to finalize their plans, found their preferred options disappearing in seconds—only to see those inventory blocks vanish moments later, their trust in the brand shaken.

Account & Payment Fraud

The betrayal extended to passengers' own accounts. Credential stuffing scripts bombarded the login portal with stolen username and password combinations, hijacking loyalty profiles and draining accumulated points. Customers discovered that their hard-earned miles had vanished overnight, eroding faith in the airline's security.

When some bots succeeded in booking with stolen card numbers, the fallout hit the bottom line. Reservations made by these scripts were promptly canceled or never claimed—leaving the airline with a tangle of refunds, no-show slots, and expensive chargebacks that threatened profitability.

System Performance & Brand Damage

All the while, these malicious bots hammered the site with high-volume requests, overwhelming servers and slowing page loads. What should have been a seamless booking experience turned into frustration, as genuine users faced sluggish performance or even temporary outages during peak booking windows.

And to compound the damage, fake reviews and duplicate listing sites began to appear across the web. Potential travelers encountered misleading ratings and were steered toward unauthorized booking platforms, further diluting the airline's brand reputation and damaging its hard-won search rankings.

THE CHALLENGE: BATTLING SOPHISTICATED BOT ATTACKS ON BOOKING ENGINES

1. Skewed Demand Forecasting

Bots generated thousands of fake searches and holds, skewing pricing and availability.

HOW INTELLIFEND HELPED

- VisitorTag profiled session behavior at IntelliFend's enforcement layer—mouse movements, scroll cadence, and request timing—while AccuBot throttled non-human patterns in real time, restoring accurate demand signals.

2. Content Scraping & Rate Undercutting

Competitors scraped fare and rate APIs to repost on OTAs.

HOW INTELLIFEND HELPED

- IETF AI Preferences tags on rate APIs let IntelliFend automatically block unauthorized crawlers, while a "good bot" whitelist permitted only approved search engines and GDS partners.

3. Inventory Hoarding ("Locking")

Bots placed hundreds of fake holds, creating artificial scarcity.

HOW INTELLIFEND HELPED

- AccuBot detected rapid repeated hold requests via intent scoring, then applied dynamic rate limits or injected step-up challenges to bot traffic, freeing real inventory.

4. Account Takeover & Loyalty Fraud

Credential-stuffing scripts hijacked accounts and drained points.

HOW INTELLIFEND HELPED

- Behavioral biometrics (typing cadence, navigation flow) plus device reputation triggered MFA only for high-risk logins, blocking 70% of ATO attempts without impacting genuine users.

5. Booking Fraud & Chargebacks

Stolen-card bookings caused cancellations and chargebacks.

HOW INTELLIFEND HELPED

- Real-time fraud detection on payment flows routed high-risk transactions through additional verification, cutting chargebacks by over 65%.

6. Performance Degradation

Bot storms mimicked peak traffic, overwhelming servers.

HOW INTELLIFEND HELPED

- By blocking malicious bots at the CDN layer, IntelliFend improved page-load times by 40% and maintained 98% uptime even at 5× normal traffic.

IntelliFend

THE RESULTS: STRENGTHENED SECURITY, REDUCED COSTS, AND IMPROVED UX

Following the IntelliFend deployment, the gaming platform saw dramatic improvements in security, efficiency, and cost savings:

98% **Booking Success: Fake Holds and Scalping Virtually Eliminated**

After IntelliFend went live, fake holds and scalping activity dropped to a negligible baseline, and genuine booking success held near 98% during peak windows.

60–70% **Reduction in Account Takeover Attempts**

In login and loyalty flows, behavioral checks and risk-based step-ups reduced account-takeover and points-draining attempts by ~60–70% over the observation period, while keeping friction low for real customers.

40% **Less Infrastructure Strain: Scraper Traffic Crushed**

With VisitorTag at the IntelliFend edge and AccuBot managing traffic upstream, scraper-driven compute and bandwidth consumption decreased materially (≈30–40% in observed periods). Queueing delays fell by ~50%, average login times improved by ~30%, and the platform sustained 99.9% uptime throughout peak booking windows.

Zero **Compliance Violations Across All Audits**

Compliance audits passed with zero findings, and IntelliFend's real-time monitoring, adaptive challenges, and exportable Push Log entries ensured full adherence to IATA NDC, PDPA/APPI, and other regional mandates.

25% **Higher Customer Satisfaction**

12% **Revenue Growth**

These technical gains translated directly into business success: customer satisfaction with booking reliability climbed by 25%, and net booking revenue grew by 12% year over year.

IntelliFend

ABOUT INTELLIFEND

IntelliFend, a product of Innovenx, delivers advanced, cost-effective AI-powered bot management solutions with unparalleled accuracy. Our platform, driven by the AccuBot Detection Engine and unique VisitorTag tracking technology, leverages multi-layered analysis of both client-side and server-side signals to provide precise, real-time bot detection and mitigation. IntelliFend's sophisticated visitor-level analysis ensures more accurate identification of bot threats, helping businesses reduce false positives and improve overall security. Gaining trust from enterprises across various sectors, IntelliFend offers rapid deployment, seamless integration, and detailed analytics, delivering robust bot protection and operational efficiency.

TALK TO INTELLIFEND TODAY

Contact us to learn how IntelliFend can protect your ticketing and reservation platform from advanced bot threats, ensure full regulatory compliance, and deliver seamless booking experiences to real customers.

www.intellifend.com

support@intellifend.com

https://www.facebook.com/intellifend

https://www.linkedin.com/company/intellifend

https://www.youtube.com/@intellifend