

AGENTIC AI & TRAVEL

Agentic AI and Bots: Friends or Foes?

Darwinium's perspective on the agent era of travel: how to welcome trusted agents while stopping malicious ones.

AI agents are already moving through travel's customer journeys: searching fares, comparing loyalty redemptions, changing bookings, and managing accounts for real customers. Fraudsters are using the same automation to stuff credentials, drain loyalty balances, scrape inventory, and scale attacks. For a decade, the industry asked, "Is this a bot?" and blocked accordingly. In the agent era, that question fails in both directions. Block all automation and you risk rejecting valuable customers; allow it all and you invite industrialized fraud. The question that matters now is:

"Is this an agent, and can we trust it right now?"

What airline and travel leaders told us

From Darwinium's 2026 agentic AI fraud research, based on travel and hospitality respondents.

63%

expect agents to perform account actions, including booking changes, cancellations, and loyalty updates — the highest share of any industry.

33%

estimate 26–50% of traffic is already non-human, 10 points above the cross-industry average.

30%

estimate 51–75% of attacks are AI-assisted, 9 points above average.

~40%

Payment fraud, account takeover and refunds/chargebacks are experiencing approximately 40% increase in AI-driven attacks in travel.

28%

say customers should bear liability when agent-driven transactions go wrong — the highest of any industry.

97%

of organizations across industries reported an increase in AI-assisted fraud attacks over 12 months.

The Same Agent Can Play Two Very Different Roles

FRIENDS — TRUSTED AUTOMATION

- Customer-authorized assistants finding and booking the best fares
- Agents managing changes, cancellations, and disruption rebooking
- Loyalty members using AI to track, redeem, and maximize points
- Corporate travel agents transacting legitimately at scale

FOES — WEAPONIZED AUTOMATION

- Credential stuffing and loyalty account takeover, where points function like cash
- Fare scraping, seat spinning, and inventory hoarding
- Hijacked legitimate agents preloaded with stolen credentials
- Refund, chargeback, and promotion abuse at machine speed

Every interaction is now one of four things: trusted human, risky human, trusted agent, or risky agent. Legacy bot management sees only human-versus-bot, risking more fraud and friction.

Darwinium's Take: Do Not Block Agents. Authenticate Intent.

Identity protocols such as Web Bot Auth allow agents to prove cryptographically who they are. That proof alone is not sufficient. Darwinium validates these signatures at the edge, then adds behavioral biometrics, device and network intelligence, timing analysis, and full-journey context, determining not only who an agent is, but what it is doing, continuously from first browse through payment, loyalty changes, and refunds.

PERMIT

Allow trusted agent traffic to move friction-free through low-risk actions.

VERIFY

Add device, identity, and cryptographic agent verification when confidence is lower.

CHALLENGE

Step up to the human principal when financial or identity risk emerges.

PREVENT

Block clearly malicious automation, including credential stuffing and scraping.

The Darwinium Difference: Built for Airlines and Travel

Edge-native, journey-wide. Deploy through your CDN, including Cloudflare, CloudFront, or Akamai. One integration protects search, booking, loyalty, check-in, and refunds, with no code changes or added latency.

Detects agents that do not self-declare. Behavioral, device, network, and timing signals expose undeclared automation, including Browser Use, Playwright, Selenium, Puppeteer, and AI browser agents, even when it imitates human behavior.

Binds trust to human moments. In hybrid journeys, a person may log in before an agent takes over. Trust is anchored to verified human proof, such as MFA or a passkey, then reassessed at sensitive actions.

Built for the agent economy. Native support for Web Bot Auth (RFC 9421), Know Your Agent frameworks, and trusted-agent allowlists with volume thresholds and journey-specific policies.

Proven outcomes. Darwinium's edge-based platform delivers up to 50% less fraud and 40% greater operational efficiency.

To find out more and see a demo of Darwinium in action, visit darwinium.com or email contact@darwinium.com