Arkose Labs

Better Together: Building a More Resilient Technology Stack for Airlines

How to combat the growing threat of account takeovers and other costly cyberattacks

Airlines have become highly adept at preventing payment fraud, but this success has driven financially motivated fraudsters to shift their focus. Today, account takeovers (ATOs) and other cyberattacks are on the rise, with cybercriminals targeting loyalty programs and frequent flier accounts to steal miles and cash out, often via ghost accounts created through registration flow attacks. Fraudsters easily purchase these miles on illicit marketplaces at a deep discount, making them a lucrative target. Compounding the issue, there is often a delay in detecting these attacks. The loss of miles remains an unrealized liability on the balance sheet until they're used, and customers may not notice the theft for some time.

With traditional defenses falling short, airlines face an urgent need to modernize their security strategies. By integrating advanced solutions like Arkose Bot Manager with existing CDN and WAF infrastructure, airlines can effectively fight off these evolving threats and protect both customers and the bottom line.

30-40%
Increase in ATOs within the airline industry[1]

166%
Surge in bot-driven attacks on airlines[2]

30%
Spike in cases of airline loyalty fraud[3]

How Traditional Defenses Fall Short

Airlines often rely on content delivery networks (CDNs) and web application firewalls (WAFs) – such as Akamai and Cloudflare – to protect their infrastructure from common cyber threats like distributed denial of service (DDoS) attacks and low-level bots. These types of solution providers were developed to solve specific security issues, which they do very well.

[1]www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/
[2]www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/
[3]www.infosecurity-magazine.com/news/airlines-battle-loyalty-program/

However, as attacks grow more sophisticated with the help of AI, the weaknesses in traditional defenses become increasingly evident. The rise of cybercrime-as-a-service (CaaS) has commoditized advanced attack tools, enabling bad actors to purchase subscriptions and access fully outsourced criminal operations. In this attacker-to-attacker model, CaaS entities provide hosted platforms for conducting attacks or offer enabling services to assist subscribers in launching their own, and many defenses struggle to keep pace with these evolving threats.

Even advanced defenses, such as multi-factor authentication (MFA), are not immune. MFA is no longer a silver bullet due to the rise of sophisticated schemes like man-in-the-middle reverse proxy phishing, where attackers use phishing emails to direct users to proxy servers that capture both real credentials and MFA codes, effectively bypassing this layer of protection.

As a result, some of these bots slip through your security stack, exposing your networks and systems to risk. Here are some reasons why:

Increasing Bot Sophistication ›

Attackers now use advanced bots powered by artificial intelligence (AI) that can mimic human behavior, hijacking customer accounts with speed and volume beyond human capabilities. These bots evade detection by traditional security tools, which often focus on simple, signature-based detection methods. AI-driven bots can adapt their behavior, making it difficult for CDNs and WAFs to identify them as malicious.

Privacy Tools and Obfuscation ›

With increasing concerns about privacy, many users – and, by extension, cybercriminals – leverage tools to mask their identities online. For example, features in modern devices such as iPhones allow users to mask their IP addresses and randomize browser fingerprints, making it even harder for traditional defenses to differentiate between legitimate users and attackers. Cybercriminals exploit these tools to launch attacks anonymously.

Complexity of Legacy Systems ›

Many airlines operate on legacy systems that are difficult to modernize. These "spaghetti code" systems make it challenging to implement new security measures because they may be highly interdependent and incompatible with modern technologies.

Why Cybercriminals Are Targeting Airlines

Value of Loyalty Programs: Airlines' success in preventing payment fraud has shifted the attack vector toward loyalty programs, which hold immense value. U.S. airlines generate approximately $25 billion from co-branded credit cards, with billions of dollars tied up in loyalty programs.

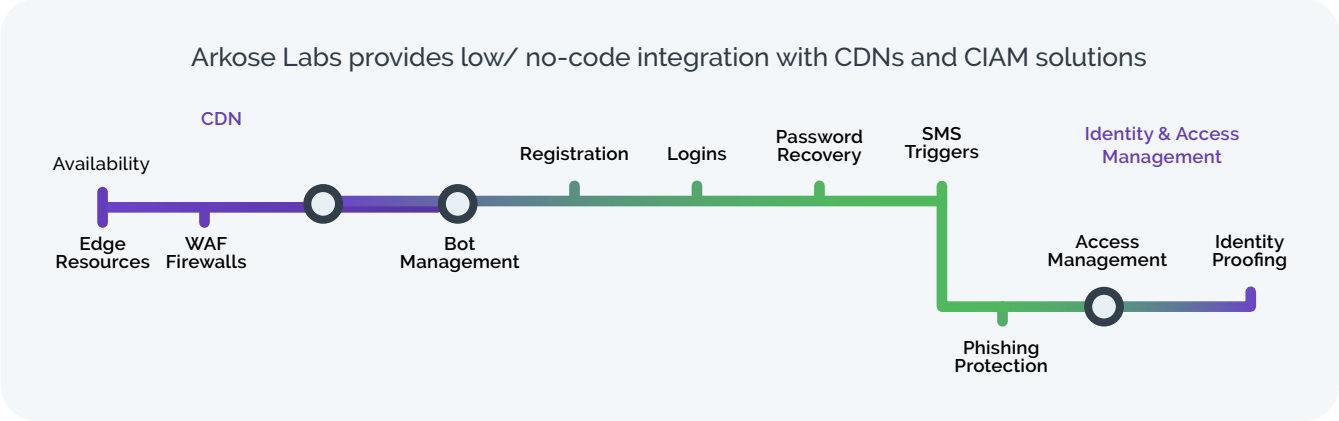
Budget Allocation Gaps: Airlines traditionally prioritize maintaining aircraft operations, with only 7% of their overall IT budget dedicated to cybersecurity, compared to airport spending at 10%. This creates vulnerabilities that fraudsters exploit.

[4]www.ideaworkscompany.com/wp-content/uploads/2024/04/Airline-Loyalty-and-Co-Branding.pdfw
[5]www.thepaypers.com/expert-opinion/loyalty-fraud-in-the-airline-industry-key-insights-and-specificities--1267027
[6]www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf

The Arkose Labs Solution: A "Better Together" Approach

Given the increasing sophistication of attacks, airlines need a comprehensive solution that complements traditional tools like CDNs/WAFs, MFA and consumer identity and access management (CIAM). This is where Arkose Bot Manager comes in.

Arkose Bot Manager brings added strength to your cybersecurity stack by providing advanced bot detection and mitigation strategies that complement existing solutions. By offering real-time feedback and adaptive challenge mechanisms, Arkose Bot Manager significantly reduces false positives and improves overall security efficacy. You gain a managed-service experience with dedicated experts who have industry-specific knowledge and a proactive approach, giving you a robust defense-in-depth strategy that leads to significant cost savings and enhanced security. And we make it easy to deploy this "better together" risk mitigation stack by offering a low-code integration and easy set-up.



Here's how Arkose Bot Manager enhances enterprises' cybersecurity infrastructure and why it is the ideal complement in your tech stack:

Enhanced Detection ›

Arkose Bot Manager classifies traffic into low-, medium- and high-risk ranges, managing detection strategies dynamically. This approach ensures that sophisticated attacks are identified effectively, offering unparalleled efficacy in threat detection. Unlike traditional web application firewalls and content delivery networks, our advanced labeling capabilities ensure higher accuracy and effectiveness in detecting and preventing fraudulent activities. Additionally, we provide extensive data sets, enabling our customers to fine-tune, investigate and develop their own risk models internally. This empowers you with the insights necessary to enhance your security measures and stay ahead of evolving threats. Plus, at no extra cost, you can provide us with truth data for our rules engine, so that false positives can be drastically minimized.

Sophisticated Mitigation and Adaptive Response ›

As attacks grow more complex, traditional solutions become less effective and more resource-intensive. Arkose Labs addresses this by offering advanced mitigation techniques that evolve with the threat landscape. Unlike traditional bot managers that offer simple triage options (allow, deny or challenge), Arkose Bot Manager challenges are integrated into the detection framework, ensuring more accurate and effective responses to threats. Additionally, we deliver world-class threat intelligence from our Arkose Cyber Threat Intelligence Research (ACTIR) unit, Security Operations Center (SOC) and Global Intelligence Network, a powerful data consortium.

Transparency and Confidence ›

By working in tandem with CDNs and WAFs, Arkose Bot Manager enhances their capabilities, providing a comprehensive defense strategy that is more effective than other standalone bot solutions. We offer absolute transparency into risk attribution, going beyond an abstract risk score by sharing the underlying data and rules so that your team can have full confidence.

Complementary Add-on ›

Arkose Bot Manager adds in seamlessly with the workflows of existing CDNs and WAFs, enhancing their capabilities without necessitating a complete overhaul of your cybersecurity framework.

The Changing Face of Cyber Threats: Sophisticated Bot Attacks

Along with large-scale credential stuffing attacks, common attack tactics against airlines include:

- **Ghost Account Creation:** Fraudsters use bots to create thousands of fake accounts to store stolen miles, disguising them as legitimate through years of spread-out activity to evade detection.
- **Bonus Abuse:** Attackers exploit promotional offers by signing up with large numbers of fake accounts, overwhelming the system and amassing loyalty points at scale.
- **Mileage Funneling and Brokering:** Stolen miles are funneled through compromised accounts or sold to third parties, violating airlines' terms and conditions.

Key Benefits of Arkose Bot Manager

Protection Against Account Takeovers and Loyalty Fraud ›

Arkose Bot Manager helps airlines defend against account takeover attacks (ATOs), loyalty fraud and other cyberattacks by identifying and mitigating bot-driven attempts to compromise customer accounts, safeguarding valuable frequent flier programs and customer data.

Reduced Costs ›

Every successful account takeover or fraud event not only costs airlines money but also damages customer trust. By stopping these attacks at the source, Arkose Labs helps airlines reduce the operational and financial burden of responding to fraud. Preventing fraudulent activity before it impacts customer accounts can save millions in lost revenue, fraud remediation and customer compensation. Additionally, by reducing the volume of malicious traffic that needs to be processed, Arkose Bot Manager lowers the downstream operational and security costs associated with managing bot attacks.

Preserved Customer Trust and Brand Reputation ›

Loyalty programs are a key driver of customer retention and brand loyalty. Frequent flier miles represent more than just monetary value; they are a symbol of trust between the airline and its customers. A single ATO incident can erode years of customer goodwill. Arkose Labs helps airlines protect these valuable relationships by keeping customer accounts secure and free from fraudulent activity.

The Arkose Labs Advantage

175+ risk signals and assements shared
Receive hundreds of session insights to enrich and tune your internal decisioning models.

Financial Warranties
Best efforts aren't good enough. We back our platform with million-dollar warranties and SLAs.

Arkose Global Intelligence Network
We see 99% of internet traffic every 20 minutes. Benefit from global risk signals and mitigation intel from our customer base.

Trusted by the most recognizable brands in the world
Built for enterprises, our technology, support, certifications and architecture meet your scalability requirements.

Global, proactive support
24/7/365 real-time SOC support with proactive incident response vs "on call".

Harnessing AI to stop evolving threat vectors
We're leveraging AI to defend against AI-driven bots.

A Unified Defense Strategy for Airlines

As fraudsters continue to evolve their tactics, airlines must evolve their defenses. Traditional cybersecurity measures like CDNs and WAFs, while essential, are not enough to combat today's sophisticated, AI-driven bots. By integrating Arkose Labs' advanced bot management solution, airlines can close the security gaps left by legacy systems and protect their most valuable asset – their customers.

With Arkose Labs and your CDN working together, your airline can safeguard loyalty programs, reduce operational costs, and preserve the trust and loyalty of your customers in an increasingly hostile digital landscape. This "better together" approach ensures that you are not only defending against today's threats but are also future-proofing your cybersecurity strategies for tomorrow's challenges.

BOOK YOUR DEMO

Arkoselabs.com