approov
mobile security

SOLUTION BRIEF

Why Mobile Apps Are the New Frontline in Airline Cybersecurity

Executive Summary

Airlines now operate in a mobile-first world. From flight booking to boarding, passengers expect seamless digital experiences — but these conveniences come with rising cybersecurity risks. Mobile apps, APIs, and third-party systems have emerged as major targets in the aviation threat landscape.

With 2025 seeing five airlines hacked within just two months, this is an industry under active and escalating attack. High-profile breaches — like the WestJet app compromise and the Qantas third-party vendor breach — reveal how attackers exploit indirect vectors to infiltrate airline ecosystems, often through mobile-related infrastructure.

As with the connected car industry, mobile apps in aviation are now central to customer engagement and backend access. It's no longer enough to protect the perimeter. Approov's Zero Trust approach secures mobile traffic at the point of origin, verifying that every app and request is legitimate before it reaches your APIs.

1. Mobile Apps Are the New Cybersecurity Perimeter in Aviation

Passengers are increasingly relying on mobile apps to manage their journeys, from check-in and boarding passes to tracking loyalty rewards. However, these apps sit on consumer devices, outside enterprise control, making them highly exposed to reverse engineering, tampering, and API abuse. The urgency is growing: in just two months of 2025, five separate airlines were breached, underscoring the fact that this sector is being directly targeted by well-resourced adversaries.

Recent airline breaches make this risk painfully clear:

- Qantas Breach (2025):
  - Attackers compromised a **third-party vendor** platform used by a Qantas call center, exposing data for up to **6 million customers** — including names, emails, birth dates, phone numbers, and frequent flyer numbers. While no credit card or passport data was accessed, experts warn the exposed data will likely fuel **phishing attacks and account takeovers**.
- WestJet Mobile App Breach (2025):
  - Attackers exploited insecure APIs tied to WestJet's mobile app to hijack loyalty accounts and steal personal data.

These incidents align with broader threats from advanced groups like **Scattered Spider**, known for attacking airlines and retailers through **social engineering** and **third-party platforms**.

Key Insight: Third-party platforms and mobile apps are now the most vulnerable — and most exploited — points of entry for attackers targeting airlines.

2. Common Attack Vectors in Airline Mobile Apps

Airline apps, like those in connected car ecosystems, face a blend of technical and human-targeted threats:

- **Reverse Engineering and Secrets Theft**
  - Attackers disassemble app binaries to extract API keys, tokens, and backend logic. This enables the creation of spoofed apps and credential-stuffing tools.
- **API Abuse**
  - Fake apps or scripts impersonate real clients.
  - Loyalty programs are hijacked using stolen credentials.
  - Automated attacks overwhelm backend systems and exploit business logic.
- **On-Device Exploits**
  - Apps running on jailbroken/rooted devices are susceptible to:
  - Runtime manipulation
  - Hooking via tools like Frida
  - Man-in-the-middle (MitM) interception
- **Unauthorized Apps and Clones**
  - Cloned or third-party apps replicate official app functionality and connect to backend APIs — introducing risks similar to those that led to the

Qantas vendor breach, where trust in external systems proved misplaced.

- **Secrets Sprawl**
  - Hardcoded secrets (API keys, tokens) frequently leak in:
  - Public code repositories
  - Debug logs
  - Decompiled apps

3. Why Traditional Defenses are No Longer Sufficient

- **OS-Level Integrity Tools Fall Short:** Apple App Attest and Google Play Integrity offer basic tamper checks — but they don't protect against app clones, or runtime attacks.
- **API Gateways Can't Distinguish Good from Malicious:** Traditional network security tools can't tell if a request is from a real app or a bot. That's how cloned or hijacked apps continue to exploit backend APIs unnoticed.
- **Static Security Tools are Outdated:** Tools like static certificate pinning, code obfuscation, or even 2FA can be bypassed.

4. Approov: Zero Trust Mobile Security for Airlines

The Qantas breach underscores that **even trusted vendors** can become weak links. The answer lies in applying **Zero Trust principles** not only at the network level, but **inside your mobile ecosystem**.

Approov Delivers Zero Trust for Mobile Channels:

Zero Trust Principle	Approov Delivers
Never trust, always verify	Attests every mobile app and request in real-time before granting backend access.
Defense-in-depth	Secures mobile apps, APIs, secrets, and runtime behavior against tampering and fraud.
Runtime, continuous validation	Identifies jailbreaks, hooking tools, emulators, and spoofed requests on the fly.
Assume breach readiness	Enables instant secret/key rotation, app revocation, and suspicious device blocking.

Core Approov Capabilities:

- App Attestation**:** Verifies that each API request originates from a genuine, untampered app — not a bot or script.
- Dynamic Secrets Management**:** Removes hardcoded secrets from app binaries, preventing theft and leakage.
- Runtime Appliction Self-Protection (RASP)**:** Detects tools like Frida, Xposed, or Magisk — stopping attackers from modifying app behavior.
- Dynamic Certificate Pinning**:** Prevents MitM attacks — even when users are on compromised networks or devices.
- Bot Protection at the Source**:** Stops bots from flooding backend APIs or executing loyalty program fraud.

5. Business Benefits of Approov for Airlines

Benefit	What it Means
Enhanced Security	Stops app cloning, credential theft, API abuse, and mobile-originated breaches.
Operational Continuity	Blocks bot traffic and fraud that would otherwise disrupt systems and support.
Monetary Savings	Reduces cloud spend from unauthorized API traffic and minimizes fraud losses.
Reputation Protection	Prevents headlines like those from the Qantas and WestJet breaches.
Flexibility & Resilience	Rotate secrets, revoke access, and block threats in real-time — no app update needed.

Whether your risk stems from mobile APIs, third-party vendors, or cloned apps — the threat is real, and growing. Airlines must now **treat mobile app traffic with the same rigor as internal systems**.

Approov Mobile Security offers the industry's leading mobile runtime protection platform — designed to **verify, protect, and adapt** to evolving airline threats.

Ready to Fortify Your Mobile Frontline? Contact us today to schedule a threat assessment or technical demo.