

Quantum-Safe Aviation Infrastructure

Protecting biometric identity, AI-driven flight operations, legacy ground systems, and unmanned vertiports against quantum and AI-era threats — without disrupting flight operations.

[← Aerospace & Transportation](#)

In this paper

1. Executive summary
2. The 2026 threat landscape
3. The iBlades architecture
4. Regulatory & compliance mapping
5. A low-risk pilot path

1. Executive summary

Aviation is pivoting to biometric "smart travel," AI-driven operations, and new eVTOL vertiport networks. This hyper-connectivity concentrates irreplaceable data — passenger biometrics, loyalty records, and AI training sets — while critical ground operations still run on legacy operational technology (OT) that cannot be easily patched.

iBlades secures this environment with a single, hardware-anchored, post-quantum security fabric that overlays existing systems. It protects data in transit against future quantum decryption, isolates legacy and unmanned assets from attack, and counters AI-driven attacks by shrinking the exposed software surface — all without changing avionics or production-critical airline applications.

2. The 2026 threat landscape

Harvest Now, Decrypt Later (HNDL)

Adversaries capture encrypted biometric and passenger data today to decrypt once quantum computers mature. Aviation is acutely exposed: biometric identifiers, unlike passwords, can never be reissued after a breach, and passenger and crew records must remain confidential for decades.

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing thousands of APIs and services at once, generating evasive malware, and mapping trust relationships to move laterally after a foothold. Against AI-driven flight and passenger systems, **data poisoning** (spoofed telemetry or sensor feeds) becomes a safety concern, not just a data concern.

The real target is complexity. AI attacks feed on exposed APIs, admin consoles, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Legacy ground OT and unmanned vertiports

Baggage handling, fuel farms, and runway lighting often run outdated software that cannot be patched without voiding warranties or halting operations. New eVTOL vertiports add remote, physically exposed, often unmanned infrastructure to the attack surface.

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM for key exchange, ML-DSA/Dilithium for signatures; FIPS 203/204) with keys generated locally and rotated autonomously.

- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh; encrypts biometric and AI data pipelines and cryptographically signs telemetry to prevent spoofing.

- **GuardTron™** — plug-and-play hardware edge node that isolates legacy ground OT and low-power vertiport infrastructure; agentless and warranty-safe.
- **ManoTron™** — hardware-secured mobile communications for crews and electronic flight bags on any network.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement even after a compromise.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, EDR/XDR, SASE, and identity tools.

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric
ICAO Aviation Cybersecurity	Protection of aviation systems & data	PQC data-in-transit, OT isolation, audit logging
IATA	Airline cyber-resilience practices	Secure crew mobility, zero-trust vendor access
ISO 27001	Information security management	Zero-trust access, immutable audit trails

5. A low-risk pilot path

- **Select** a non-critical subsystem (e.g., a remote cooling station, secondary baggage controller, or crew-lounge network).
- **Deploy** the edge node inline — a fast install with no changes to avionics or production systems.
- **Validate** isolation with a red-team exercise; legitimate traffic passes, attacks are blocked.
- **Demonstrate** post-quantum key rotation and audit evidence; reverse cleanly if desired.

Ready to secure your aviation operations?

Request a briefing to see how a low-risk pilot would work in your environment.

[Request a briefing](#)

[↓ Download PDF](#)

[Back to overview](#)

Prefer email? Reach us at hello@ibldes.ai



Safe, effective, secure.

Next-generation cyber architecture making
cybersecurity simple, reliable, and accessible for
everyone.

hello@iblades.ai

Products

[NetTron™](#)

[GuardTron™](#)

[ManoTron™](#)

[Pricing](#)

Solutions

[Financial Institutions](#)

[Healthcare](#)

[Infrastructure](#)

[Government & Military](#)

Company

[About Us](#)

[Partners](#)

[Documentation](#)

[Contact](#)

Compliance

NIST Approved

SOC 2 Type II

HIPAA Compliant

ISO 27001

FedRAMP Ready

HEADQUARTERS

127 Spring Street, Suite 120
Pleasanton, CA 94566

R&D CENTER

795 24th Street
Ogden, UT 84401

© 2026 iBlades.ai. All rights reserved. All trademarks and technologies are the property of their respective owners.