



From Unseen Risks to Complete Visibility: How a global airline strengthened security and gained operational insight with Aeris IoT Watchtower™

POWERED BY  aeris®

COMPANY

European airline

PRODUCT

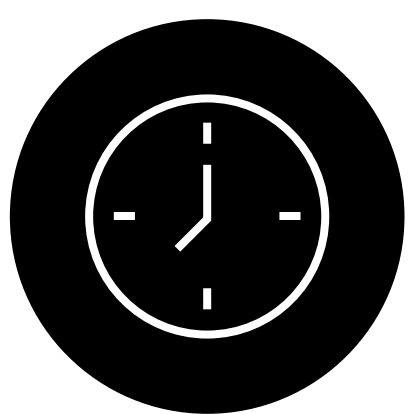
Aeris IoT Watchtower™

LOCATION

Global

SPECIALTY

Aviation



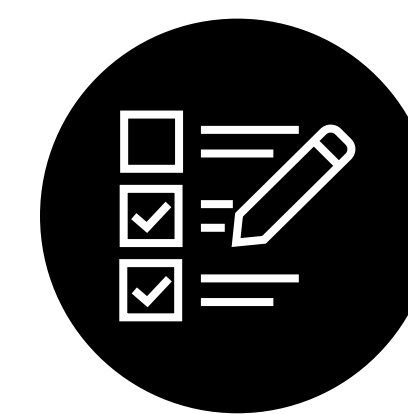
Incident diagnosis
reduced from
days to minutes.



Proactive anomaly
detection across
~10,000 devices.



**Reduced unnecessary
data consumption** via
configuration tuning.



**Continuous, audit-
ready security reporting**
aligned to device roles.

THE CHALLENGE: THE HIGH COST OF LIMITED VISIBILITY

A global airline operates a globally connected fleet of aircraft, along with thousands of mission-critical mobile assets used by pilots, cabin crew, and ground staff. These devices, including electronic flight bags (EFBs), maintenance tablets, and crew devices, are essential for flight planning, passenger manifests, in-flight service, and technical operations.

While the organization had a mature network architecture with strong foundational security, including mobile device management (MDM) controls and a secure VPN overlay, a critical gap remained: end-to-end operational visibility.

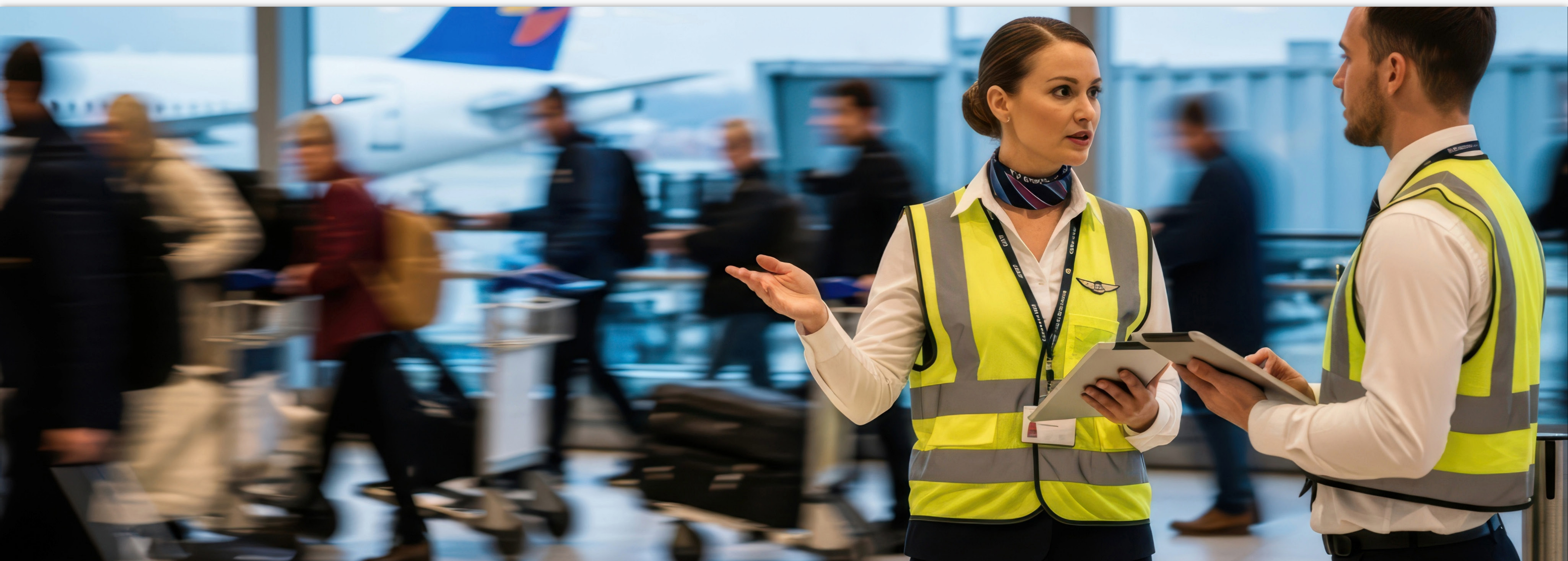
With approximately 10,000 tablet devices moving globally, the IT operations team could see aggregated SIM usage but lacked the granular insight needed to diagnose anomalies. This limitation increased operational risk, inflated data costs, and extended incident resolution times.

A MAJOR INCIDENT HIGHLIGHTED THE ISSUE

A routine software update for a crew application introduced a bug that caused repeated full data downloads instead of incremental syncing. Within hours, monthly data allowances were exhausted across thousands of devices. Without connection-level visibility, identifying the root cause took several days and required widespread manual intervention.

This, combined with the need to answer proactive questions such as:

- Are devices behaving consistently across fleets?
- Can misconfigurations be detected early?
- ...led the organization to seek deeper network-level intelligence.



THE SOLUTION: A PHASED ADOPTION OF AERIS IOT WATCHTOWER

In early 2024, the airline began evaluating Aeris IoT Watchtower™ through its connectivity partner. The platform was positioned as a network-level augmentation, providing an independent, external view of device behavior rather than replacing existing security infrastructure.

The rollout followed a structured, phased approach over 15 months.



PHASE 1

Initial Trial & Group-Based Strategy

A 60-day trial focused on operational visibility. The breakthrough came when the airline structured its environment in the Aeris IoT Watchtower platform to mirror its operational reality, creating three distinct device groups:

- Electronic Flight Bags
- Maintenance tablets
- Crew devices

PHASE 2

Structured Adoption & Insight Generation

This grouping strategy was immediately impactful. The airline observed that each group had a unique data profile and risk surface, and Aeris IoT Watchtower's per-group network baselines made anomalies instantly meaningful. Key capabilities they leveraged included:

Granular Connection Visibility

Destination endpoints (domains/IPs), timestamps, and per-SIM data usage.

Baseline Deviation Detection

Identification of outliers, anomalous traffic patterns, and misconfigurations.

Operational Feedback Loops

Insights used to optimize device configurations and reduce unnecessary background data usage.

PHASE 3

Operational Integration

The trial transitioned into full operational integration:

- Monthly risk assessment reports aligned to device groups
- Integration into IT operations workflows
- Planned training for operational teams

RESULTS: FROM REACTIVE FIREFIGHTING TO PROACTIVE INTELLIGENCE

Through the implementation of Aeris IoT Watchtower™, the airline transformed its operational posture:

Faster incident resolution

Root cause analysis reduced from days to minutes.

Improved security posture

Detection of unexpected endpoints, DNS activity, and anomalous data usage.

Reduced data costs

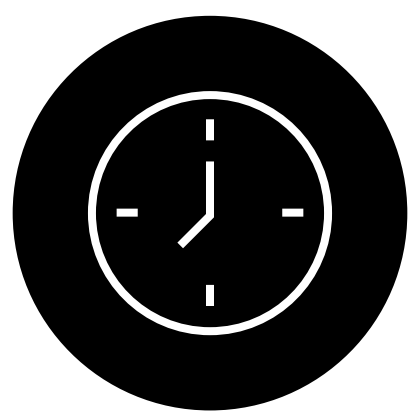
Elimination of unnecessary background traffic through configuration tuning.

Audit-ready reporting

Continuous compliance support aligned to device roles.

Operational resilience

Early detection prevents issues from escalating.



Incident diagnosis reduced from **days** to **minutes**.



Proactive anomaly detection across **~10,000 devices**.



Reduced unnecessary data consumption via configuration tuning.



Continuous, audit-ready security reporting aligned to device roles.

The organization noted that, had the platform been in place during the earlier application bug incident, the issue would have been identified almost immediately, avoiding widespread disruption.

SUMMARY

A global airline successfully transformed its approach to mobile asset management by addressing a critical visibility gap. By deploying Aeris IoT Watchtower™ and adopting a fleet-aligned grouping strategy, the organization shifted from reactive troubleshooting to proactive operational intelligence. Visibility is no longer just a security capability, it is now a core operational asset that enhances service continuity across thousands of mission-critical devices.

