

CYBER RESILIENCE FOR AVIATION:

Secure the Systems That Keep Aviation Moving with Identity-Based Microsegmentation

Zero Networks closes the pathways attackers depend on without disrupting critical systems.

Aviation networks connect reservation systems, ground support equipment, baggage handling, and jet bridge controls – legacy and modern, IT and OT – while a constantly evolving list of third-party vendors need targeted access to keep operations moving. When downtime can spiral into a ground stop, aviation organizations need to contain risk without adding operational friction.

That's where Zero Networks' automated, identity-based microsegmentation comes in – Zero contains threats by design to preserve uptime even if attackers get inside.

What Zero Networks Delivers: Capabilities Tailored to Aviation



Identity-based microsegmentation

Access follows the identity, not a static network rule, so ground crew, gate agents, and third parties stay scoped to what their role actually requires – and breaches stay contained.



Just-in-time MFA for privileged access

With patented network-layer MFA, sensitive flight operations systems, maintenance platforms, and admin tools require identity verification before they can be accessed.



Automated policy lifecycle

Policies are generated based on learned network behavior via Zero's deterministic, human-on-the-loop automation engine – enforcement adapts without manual rule-writing or ongoing tuning.



Governed third-party and vendor access

Identity-based controls extend to ground handlers, MRO providers, and other vendors or contractors, giving security teams visibility into and control over every connection.



Built-in compliance with TSA requirements

Identity-based microsegmentation means airport and aircraft operators meet TSA requirements for network segmentation and access control by default.



Agentless deployment

Zero's agentless architecture integrates seamlessly with existing infrastructure, orchestrating native controls to protect the entire environment without introducing new potential points of failure.

Where Risk Lives in Aviation Networks – and How Zero Networks Contains It

The Problem	What It Looks Like	How Zero Helps
IT/OT convergence	Ground support equipment, baggage systems, and more increasingly connect to IT networks. Attackers rarely breach OT directly – they gain a foothold in IT then move laterally.	Identity-based microsegmentation applies granular least privilege policies between assets so only approved connections are allowed; no unauthorized lateral movement from IT to OT or between OT assets.
Third-party connection sprawl	Ground handlers, MRO providers, caterers, and fuel suppliers often gain broader network access than the task requires.	Third-party connections are constrained to least privilege, so a compromised vendor credential doesn't deliver broad internal access.
Legacy system vulnerabilities	Older systems where agents can't be deployed and patches can't be applied without risking operations leave aviation networks vulnerable.	Zero's agentless solution is layered on top of legacy systems – access is governed by identity-driven policies using the existing infrastructure.
Outage risks in uptime-critical environments	Legacy segmentation tools that require manual tuning or agents deployed on every endpoint introduce outage risks in environments where uptime is non-negotiable.	Deterministic, human-on-the-loop automation generates policies based on observed network behavior, dynamically updates them as the network changes, and scales enforcement by orchestrating host-OS firewalls.
Compliance pressure	TSA's cybersecurity requirements call for network segmentation and more robust access controls.	Identity-based microsegmentation enforces IT/OT segregation, least-privilege access, and breach containment by design.
Enterprise AI adoption	AI adoption across aviation business units is creating a fast-growing, ungoverned blind spot.	AI Segmentation delivers visibility and control over AI – governing which AI tools users can reach and constraining agent access to least privilege.
Multi-tenant airport infrastructure	Multiple airlines and operators often share underlying network infrastructure at the same airport.	Microsegmentation contains breaches proactively, so a minor cyber incident doesn't escalate into a ground stop.

Contain threats by design to make cyber resilience your default.
See how Zero Networks secures the systems that keep aviation running.

[Request a Demo→](#)