Cloudflare One is agile SASE for airlines

Connect and protect your nomadic crew, third-party partners, AI agents, and in-flight passengers with one of aviation's most trusted networks.

Truly unified SASE

The "platform" promise, finally delivered

Stitched-together VPNs, branch firewalls, and fragmented tools leave gaps that airlines adversaries exploit. First-generation SASE solutions promised simplicity but delivered a patchwork of proxies and complex policies that slow down a nomadic workforce.

Cloudflare One is the unified platform that other SASE providers promised but couldn't build. We eliminate the friction of legacy security and networking with one control plane, data plane, and infrastructure layer.

- **Protecting aviation globally:** 20% of the web is protected by Cloudflare, providing unmatched Internet visibility.
- **Securing airline AI:** ~80% of the top 50 GenAI companies run with Cloudflare, giving us a unique position to secure GenAI usage and govern AI agents.
- **Low-latency coverage anywhere:** 300+ cities delivering full SASE (>3x other SASE vendors) for resilient, consistent experiences across airports, lounges, and connected aircraft.

SASE on Cloudflare's global network

Experience unmatched consistency for security and performance with a platform that is easier to deploy and built to last. As airlines accelerate fleet connectivity and modernize the passenger experience, you need an architecture that is unified by design, not by stitched-together acquisitions.

Why Cloudflare

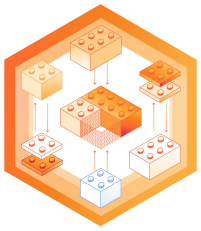
Deploy faster. Adapt instantly.

The fast path to safe AI adoption

Don't just manage shadow AI — secure your aviation infrastructure. We are the first SASE platform to secure connections to MCP servers, protecting sensitive data from leaking into unapproved LLMs.

The easy-to-use SASE

Stop paying for bloated tools you can't deploy. Remove the complexity of legacy SASE, replace aging MPLS, and accelerate the time to roll out high-value, zero trust security and networking capabilities for pilots, ground handlers, and partners.



A truly composable, programmable platform

Augment your existing stack, integrate loyalty and advertising analytics at the edge, and infinitely customize your SASE deployment to fit sophisticated aviation needs alongside our expert design partners.

Where to get started

Connect and protect your nomadic crew, ground operations, and connected aircraft without disruption.

Transforming your airline's network doesn't have to mean a massive, risky overhaul that threatens on-time performance. Solve your most urgent pain point today, like replacing a sluggish VPN for pilots across 80+ countries, securing high-speed in-flight Wi-Fi, or discovering shadow AI, and modernize your long-term architecture at your own pace.

Safely adopt AI

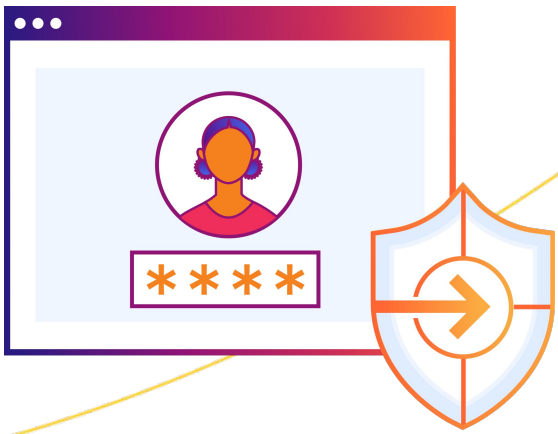
Move beyond simple blocking to secure AI adoption across revenue, customer service, and ops teams.

- **Govern AI agents:** Be among the first to govern connections between your workforce, MCP servers, and internal aviation data.
- **Control shadow AI:** Discover unsanctioned AI tools being used across your network and manage access. Redirect employees to approved apps.
- **Secure sensitive aviation data:** Analyze AI prompt content and intent to block highly regulated PNR data, payment information, and crew PII from leaking into public models.

Modernize remote access

Stop relying on clunky, insecure VPNs that slow down a globally distributed workforce of pilots, cabin crew, and corporate staff. Provide identity-first, quantum-safe access to internal apps and infrastructure from anywhere in the world.

- **Accelerate third-party onboarding:** Quickly grant safe, frictionless, and auditable access to MRO (maintenance) vendors, ground handlers, and alliance partners in minutes, not days.
- **Speed up airline integrations:** Integrate the networks of acquired carriers or regional partners more efficiently, without complex IP overlapping or rigid firewall rules.
- **Stop ransomware and ensure resilience:** Replace broad network access with granular zero trust rules that prevent threats from spreading laterally and grounding flights, accelerating your readiness for mandates like EASA Part-IS.



Block targeted aviation phishing & BEC

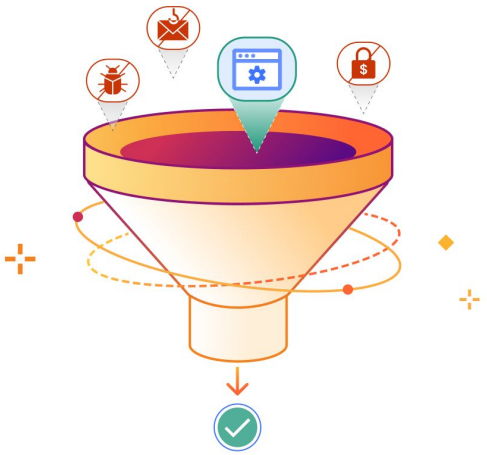
Aviation is a prime target for supply chain and finance-based attacks. AI-powered email security stops phishing, crew impersonation, malware, and business email compromise before threats reach users' inboxes.

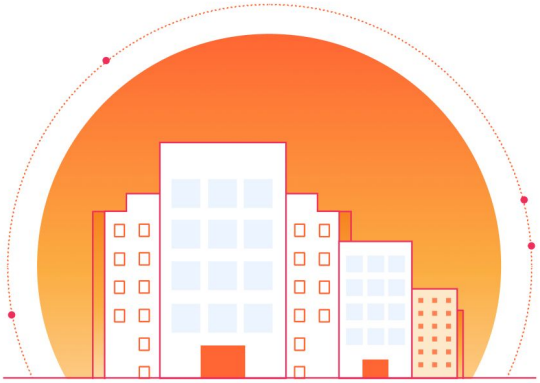
- **Block with precision:** Thwart elusive phishing threats aiming to compromise crew credentials or supply chain logistics that routinely bypass native Microsoft 365 or Google Workspace defenses.
- **Deploy faster:** Get started instantly with flexible MX and API deployment methods that need minimal configuration and no tuning.
- **Extend workspace security:** Add native SASE controls across email and collaboration apps, automatically isolating risky web links in a secure browser before they reach an employee's device.

Protect the connected aircraft & airport Wi-Fi

Implement DNS and HTTP filtering to protect connected fleets, airport lounges, and distributed corporate branches from malware, phishing attacks, and malicious websites.

- **Get instant results on LEO networks:** Use clientless deployments that overcome Starlink's technical constraints to block Internet threats without requiring software on passenger devices.
- **Protect without friction:** Enforce flexible security rules for high-speed in-flight Wi-Fi using the world's fastest public DNS resolver, ensuring low latency at 35,000 feet.
- **Enforce acceptable use:** Secure corporate and passenger Wi-Fi with safe, private visitor experiences. Segment passenger traffic from crew operational traffic with dedicated resolver IPs.





Deploy coffee shop networking across hubs

Treat every airport lounge, MRO hangar, and call center like a coffee shop. Deliver consistent, high-performance connectivity across all global operations.

- **Minimize appliances and legacy MPLS:** Reduce complexity by replacing expensive, rigid MPLS lines and aging branch firewalls with a more efficient "light-branch, heavy-cloud" SASE approach.
- **Unify access policies:** Use composable ZTNA and WAN services to enforce the same security policies for a pilot logging in from an international hotel as a ground handler at the terminal.
- **Consolidate infrastructure:** Enable a zero trust posture everywhere your crew works, all with a simpler infrastructure stack.

Real ROI for aviation

A recent Forrester™ Total Economic Impact™ study found a composite organization achieved significant operational and financial benefits by consolidating on Cloudflare, outcomes directly applicable to airlines burdened by legacy tech debt:

35%
time savings on security and IT management

90%
reduction in VPN-related IT tickets

~$5.2 M
in connectivity-related savings

Airlines securing the future of flight

Top US network carrier

A major US airline flying hundreds of thousands of passengers per day engaged Cloudflare to protect their fleet-wide rollout of Starlink Internet. The airline needed to apply entirely different filtering policies for their passenger network versus their crew network, but Starlink's basic filters could not support this granularity.

Cloudflare was selected over legacy competitors including Cisco Umbrella, DNSFilter, and Infoblox because we could navigate the unique constraints of the LEO architecture.

Top US low-cast carrier

A major US airline selected Cloudflare as the programmable bridge between Starlink in-flight Wi-Fi and the airline's analytics platform, preserving multi-million-dollar annual passenger intent data revenue that would otherwise have been lost in the Starlink transition.

Cloudflare was selected as a tech-enabled travel platform for its performance, global reach as a "Starlink value-add," and dedicated resolver IPs that let the airline tie every request back to a specific aircraft.

JAPAN AIRLINES

Major airline
Read case study

~35k
Employees inboxes protected
against phishing threats

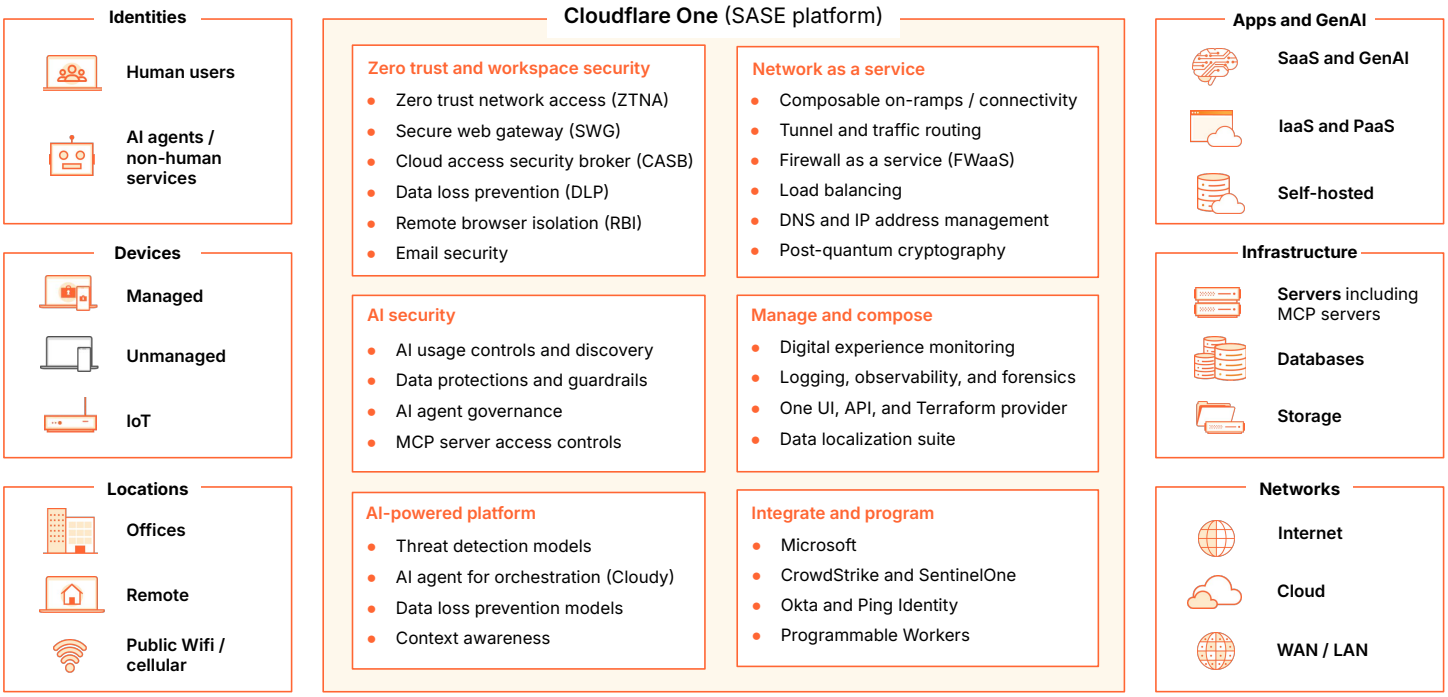
Other airlines protected by Cloudflare:
Top Canadian airline, top Korean carrier, major international airport operator, top US ULCC, top Australian airport, UK flag carrier, top Thai flag carrier, mid-size US LCC, Norwegian LCC, Peruvian regional carrier, and more...

SASE solution packages

Cloudflare's Interna packages connect and protect internal systems — no billing surprises

- **Eliminate bandwidth fees for managed devices:** Secure pilot Electronic Flight Bags and crew iPads anywhere in the world without paying per gigabyte.
- **Expand your WAN with every seat:** Every security seat builds your included shared bandwidth pool for connecting lounges, gates, and hangars.
- **Access the globe for one flat rate:** Predictable OPEX forecasting, whether your crew is logging in from London, Tokyo, or New York.
- **Deploy unlimited software connectors:** Secure your SaaS environment and internal booking apps without nickel-and-diming per connection.
- **Secure SaaS inclusively:** Get full CASB coverage to protect sensitive PNR data across modern booking platforms, M365, and crew scheduling apps.
- **Unlock digital experience monitoring natively:** Pinpoint latency issues for managed devices and remote pilot EFBs as a built-in feature, not an expensive add-on.

How it works



Security and network services, built for innovators

Zero trust and workspace security

Enforce granular security policies across in-flight web traffic, SaaS crew scheduling portals, airline email, and private operational apps. Stop the lateral movement to prevent disruptive flight groundings and protect sensitive PNR data, all without slowing down your nomadic workforce of pilots, ground handlers, and corporate staff.

Network-as-a-service (NaaS)

Your private global aviation backbone and quantum-safe SASE. Seamlessly connect distributed airport hubs, remote MRO hangars, connected aircraft, and mission-critical cloud operations to a lightning-fast, secure, and DDoS-protected network built for operational resilience and on-time performance.

AI security

Safely adopt GenAI across your airline. Curate strict guardrails and govern AI agents to prevent sensitive PNR data, payment details, and crew PII from leaking into public LLMs. Manage non-human permissions across your automated booking and flight operations systems.

Manage and compose

Monitor the digital experience for in-flight passengers and remote crews, and ensure strict data sovereignty for sensitive data across different global jurisdictions. Centralize visibility and control across your entire connected fleet and ground hubs with one unified dashboard, robust APIs, and our native Terraform provider.

AI-powered platform

Detect and block threats targeting your fleet and ground operations. Improve DLP accuracy with context analysis to protect sensitive data. Analyze employee AI prompt intent to prevent data leaks, and instantly summarize policies and logs in natural language to accelerate incident response for lean airport IT teams.

Integrate and program

Adapt to your airline's complex tech stack. Integrate third-party aviation platforms (like Sabre or Amadeus), and extend capabilities using custom programmable code to match your exact business logic, from preserving loyalty and advertising integrations on in-flight Wi-Fi portals to customizing routing for ground operations.

Ready to get started with agile SASE?

Talk to an expert | **View enterprise packages**

Or, keep learning more in Cloudflare's SASE demo hub or reference architecture.