goldilock

USE CASE 06

Aviation sector

Protecting aviation systems through cyber and operational resilience for all aviation, ground and avionics systems.

The interconnected world relies on airports, airlines, and air traffic management systems as the very arteries of global mobility.

From everyday flight operations, passenger travel and intricate air traffic choreography to critical cargo delivery and sensitive government aviation, these systems are all indispensable. Yet, their importance is matched only by the escalating and relentless sophistication of the threats they face. Aviation organisations are constantly battling a rising tide of risks, including evasive ransomware attacks, the pervasive danger of social engineering, insidious insider threats, and the stealthy lateral movement of malicious actors across their complex IT/OT environments. While essential, conventional software-based security often proves inadequate against these advanced threats, leaving critical assets exposed when software controls are circumvented, compromised, misconfigured, or suffer from inherent flaws.

Aviation infrastructure holds undeniable importance, a fact cemented by international aviation authorities such as ICAO and EASA, and national regulators, who have issued directives classifying airports, air navigation service providers, and airline IT systems as essential services. This crucial designation integrates them into national and international critical infrastructure regulatory frameworks, highlighting their crucial role in a thriving modern society. It places them on par with the energy, water, and the other transportation sectors. Consequently, this status demands increased oversight, regulatory oversight, and an intensified focus on deploying the strongest security measures to defend against the entire range of potential threats.

Furthermore, the emergence of Artificial Intelligence (AI) is fuelling a significant demand for highly specialised aviation systems. These advanced AI platforms, designed for applications such as predictive maintenance, nuanced passenger analytics, and increasingly autonomous airport operations, underscore an even greater imperative for robust and adaptive security solutions across the whole infrastructure.

Goldilock's FireBreak™ solution

The innovative solution introduces a fundamental change in aviation cybersecurity: the capability for hardware-enforced, on-demand physical isolation of mission-critical aviation systems and their data, all via secure remote control.

This hardware-enforced separation provides an ultimate, last line of defence, acting as a controlled physical airgap when software-based controls have been bypassed or rendered ineffective during a cyber incident.

FireBreak offers an incremental layer of cyber resilience that extends far beyond logical segmentation, ensuring the absolute inaccessibility of targeted aviation assets to malicious actors at the most fundamental level, a capability now indispensable as airports and airlines are increasingly recognised as critical national assets.

Goldilock's FireBreak Physical Connection Controller delivers a revolutionary, hardware-enforced cyber defence purpose-built for the modern aviation sector, where the stakes have never been higher. As airports and airline systems already represent the digital backbone of global transportation, they face relentless cyber threats, unprecedented operational demands, and stringent regulatory scrutiny. FireBreak transcends traditional software barriers by proving the capability to physically isolate critical IT and Operational Technology (OT) systems, air traffic management (ATM) platforms, cargo and logistics infrastructure, baggage handling systems, terminal access control, surveillance systems, public-facing web services, and backup systems from all network connectivity, on demand, as required, eliminating remote attack vectors entirely.

By physically disconnecting these assets from all networks and segments when not in use, during maintenance, or at times of heightened risk, FireBreak renders them invisible and inaccessible to cyber threats. This creates a totally shielded security perimeter, crucial for aviation environments where downtime, data loss, or compromise can have catastrophic ripple effects across industries and nations. FireBreak's network-invisible control channel enforces a hardware isolation barrier that software alone cannot match. Consequently, this physically disconnected environment becomes an unassailable domain for sensitive aviation information. It inherently supports tamper-proof evidence, indispensable for meeting regulatory audit requirements and swift post-incident analysis, while guaranteeing full adherence to aviation-specific data mandates, offering aviation enterprises unparalleled assurance for their critical operations.

Designed to meet the rigorous demands of international and national aviation cybersecurity frameworks including; NIS2, ICAO Annex 17, EASA, Australia's SOCI Act, and sector-specific regulatory mandates, Goldilock FireBreak offers uncompromising cyber-physical protection that aligns with Zero Trust principles. Whether safeguarding baggage handling systems, critical air traffic control servers, core airport network switches, sensitive passenger and cargo data repositories, terminal access control, or airfield operations infrastructure, FireBreak empowers aviation operators to maintain operational continuity, uphold passenger trust, and vigorously defend against the ever-escalating cyber threat landscape

Outpacing threats: Why aviation cyber demands evolution

The rapid evolution of all types of aviation systems, including airport IT, airline operational platforms, analytics, edge devices, baggage handling PLCs, airfield lighting, terminal access control, and public-facing web services, has dramatically expanded the attack surface, often outpacing traditional security measures. With global business, passenger safety, and public trust relying on secure, resilient aviation operations, protecting this infrastructure requires proactive, robust security that goes beyond reactive patching. As a core pillar of critical infrastructure, aviation demands only the most advanced solutions. Goldilock delivers a breakthrough in security with hardware-enforced physical isolation for servers, storage, network switches, and backups. This ensures aviation assets remain invisible, inaccessible, and protected from even the most sophisticated cyber threats. FireBreak empowers operators across all aviation environments to maintain uptime, passenger trust, and resilience in today's digital-first world.

As airports and airlines scale to meet the demands of digital transformation, AI, and high-density operations, uncompromising, hardware-based security is essential. Goldilock FireBreak empowers operators across all aviation environments to maintain uptime, passenger trust, and resilience in today's digital-first world.

Critical threats facing the data aviation sector

The aviation sector faces a formidable and evolving array of cyber threats, each capable of severe disruption, financial loss, and even safety hazards. These challenges are amplified by the industry's interconnectedness and its status as critical national infrastructure.

- **Advanced Persistent Threats (APTs):** State-sponsored groups specifically target aviation cargo and logistics systems to disrupt supply chains, steal sensitive operational data, or sabotage critical flight and ground operations.
- **Ransomware in converged IT / OT:** Integrated baggage handling, HVAC, airfield lighting, and other operational systems create high-risk pathways for lateral movement and ransomware propagation across airport facilities.
- **Data Manipulation / Lockout:** High-value cargo management and passenger data systems are prime targets for ransomware and data theft, risking operational paralysis for airlines and airports, alongside severe regulatory fines.
- **Third-party vendor risk:** Thousands of connected e-commerce, retail, and logistics partners significantly expand the attack surface across aviation enterprises, increasing the risk of supply chain compromise that can impact flight operations.
- **Vulnerable public-facing services:** Airports and airlines rely on a patchwork of public-facing services, including flight information displays, e-commerce portals, and third-party logistics interfaces. These systems are essential for passenger experience and operational efficiency but are also frequent entry points for attackers.
- **Regulatory scrutiny:** Aviation's critical infrastructure status, affirmed by ICAO, EASA, NIS2, and national acts (e.g., SOCI Act, TSA directives), mandates rigorous cybersecurity. This demands auditable cyber resilience, incident reporting, strict IT/OT segmentation, and adherence to standards like NIST CSF. Non-compliance carries severe penalties, directly impacting aviation operational licenses.
- **DDoS and service disruption:** Distributed denial-of-service attacks can overwhelm airport and airline networks, disrupt critical public-facing services like check-in or flight tracking, and degrade overall operational performance.

- **Insider threats (intentional or accidental):** Employees, contractors, or vendors with privileged access to aviation systems can unintentionally introduce malware or deliberately cause harm, impacting safety and operations.
- **Legacy infrastructure vulnerabilities:** Many aviation environments still rely on legacy systems and unsupported hardware that lack modern security controls, posing significant risks to air traffic control and ground operations.
- **AI and high-performance computing risks:** AI-focused aviation systems are attractive to attackers seeking to steal proprietary algorithms, sensitive training data, or disrupt critical AI workloads underpinning predictive maintenance or autonomous operations.
- **Physical security breaches:** Unauthorised physical access can lead to theft, tampering, or destruction of aviation hardware and data, directly impacting operational integrity.

Real-world deployment scenarios: Goldilock FireBreak in aviation

Airport OT protection

Challenge: Baggage handling and airfield lighting systems are exposed to ransomware and lateral movement from IT networks.

FireBreak solution: Physically air-gaps OT systems by default, only connecting for scheduled maintenance or validated vendor access. Instantly isolates OT if threats are detected.

Impact: Stops ransomware spread, ensures compliance, and maintains operational continuity.

Air Traffic Control (ATC) system isolation

Challenge: ATC servers require maximum protection; compromise risks flight safety and airspace integrity.

FireBreak Solution: Physically disconnects ATC systems from all non-ATC networks, only connecting for critical updates via secure, out-of-band methods.

Impact: Prevents remote manipulation, guarantees ATC integrity, and supports rapid emergency recovery.

Passenger and cargo data security

Challenge: Sensitive passenger and cargo data are prime targets for ransomware and data theft.

FireBreak solution: Keeps data servers and backups offline except for authorised, scheduled access. SIEM triggers instant isolation on suspicious activity.

Impact: Prevents data exfiltration, supports regulatory compliance, and protects privacy.

Terminal Access Control & Surveillance

Challenge: Legacy access control and surveillance systems are vulnerable to cyberattack, risking physical security.

FireBreak solution: Default isolation of access control and surveillance servers; connects only for updates or admin tasks. SIEM triggers immediate isolation on anomalies.

Impact: Blocks cyber-physical breaches, enables rapid incident response, and logs all activity for audits.

Public-facing services and third-party interfaces

Challenge: Flight info displays, e-commerce portals, and logistics interfaces are frequent attack entry points, causing maximum disruption and airport outages

FireBreak solution: Physically disconnects public-facing servers during off-peak or threat conditions. Enforces time-bound, logged access for third-party vendors, with SIEM/SOAR-triggered automation.

Impact: Reduces attack surface, secures supply chain access, and enables instant breach containment.

Core network infrastructure hardening

Challenge: Compromised switches, routers, or firewalls can disrupt all airport operations.

FireBreak solution: Isolates management interfaces, connecting only for authorised admin via secure out-of-band channels. Instantly disconnects on detected anomalies.

Impact: Protects network backbone, ensures resilient management, and enforces Zero Trust.

Goldilock FireBreak extends precise, hardware-enforced protection across the entire aviation spectrum: from disaster recovery and regional airports to AI/analytics platforms, payment/loyalty systems, and vital onboard aircraft systems. This capability directly enhances operational resilience, simplifies regulatory compliance, and offers unparalleled assurance for aviation operators confronting evolving cyber threats.

Why aviation operators choose Goldilock FireBreak

Absolute invisibility

Eliminating the Attack Surface When critical aviation systems such as air traffic control (ATC) servers, baggage handling PLCs, airfield lighting controls, sensitive passenger and cargo data repositories, and essential backup infrastructure are physically isolated by FireBreak, they vanish from the digital landscape. There's no IP address to scan, no digital footprint to detect, and zero pathway for remote attack. This creates a truly zero attack surface, rendering these vital assets invisible to even the most advanced cyber adversaries. For aviation, this level of invisibility is not just a technical advantage, it is fundamental for maintaining flight safety, protecting operational continuity, and ensuring regulatory compliance in an era of relentless and sophisticated threats

Future-proof security across all aviation environments

FireBreak is purpose built to deliver uncompromising protection across the entire aviation ecosystem. It integrates seamlessly with legacy airport OT, modern cloud-native airline IT, and advanced AI-driven platforms, defending everything from sprawling international hubs and regional airports to airline operations centers and even critical avionics on board aircraft. FireBreak eliminates the need for costly or disruptive infrastructure upgrades, allowing operators to enhance security without hindering operational efficiency or innovation.

Rapid, non-disruptive deployment

In aviation, every second counts. FireBreak is designed for swift, flexible deployment, utilising secure out-of-band methods such as SMS commands, physical key switches, or seamless API integration with existing Security Operations Center (SOC) tools. This enables installation and activation with zero interruption to airport or airline operations, ensuring continuous service and safety.

Operators gain an immediate boost in cyber resilience, with the ability to rapidly isolate, reconnect, or segment critical systems as operational needs evolve. This agility is essential for maintaining uptime, adapting to new threats, and supporting ongoing innovation in the fast-paced aviation environment.

True zero trust segmentation and access control

FireBreak brings Zero Trust principles to life in aviation by delivering hardware enforced segmentation and just-in-time, role-based physical access to critical assets. Systems are only connected when absolutely necessary and for the minimum duration required, whether for routine maintenance of airfield lighting, privileged AI model training, targeted diagnostics on aircraft, or vendor updates to baggage handling PLCs. This approach drastically reduces the window of vulnerability, ensuring that even if credentials are compromised, attackers cannot persistently access isolated systems. Every connection is logged and auditable, supporting regulatory compliance and forensic investigations.

Battle-tested in high-stakes aviation and critical sectors

FireBreak is far more than a theoretical solution, it is proven in the world's most demanding and unforgiving environments, where failure is simply not an option. Deployed in aviation, national defence, and other critical national infrastructure sectors, FireBreak has demonstrated uncompromising resilience against the most formidable threats: from sophisticated ransomware and stealthy insider threats to complex supply chain attacks and persistent state sponsored adversaries. Its hardware-enforced isolation has thwarted lateral movement during real-world incidents, protected vital airport and airline operations from cascading failures, and enabled rapid recovery in the face of cyber and physical crises. This proven track record delivers unparalleled confidence for aviation leaders, regulators, and partners, ensuring that mission-critical assets remain secure, resilient, and operational in the face of today's most advanced and persistent cyber threats.

Proactive and reactive control options in a dynamic threat landscape

FireBreak keeps aviation operators ahead in a rapidly evolving threat landscape. Control of the threat surface comes from choosing when segmentation and system separation is software defined or absolute at the physical layer. As cyber risks shift from ransomware and supply chain attacks to insider and state-sponsored threats, FireBreak delivers instant, hardware-enforced isolation that blocks new attack vectors and adapts to changing risks. By physically disconnecting critical systems when threats arise, FireBreak neutralises remote attacks, regardless of how adversaries evolve. Seamless integration with SIEM and SOAR platforms enables fast, automated or manual isolation, ensuring resilience, compliance, and passenger trust, no matter how threats change.

Additional reasons aviation chooses FireBreak

- **Regulatory readiness and auditability:** FireBreak is built to support compliance with a wide range of international and national aviation cybersecurity mandates including; NIS2, ICAO Annex 17, Australia's SOCI Act, GDPR, TSA directives, and equivalent standards worldwide. It provides immutable, tamper proof logs for every connection event, streamlining forensic investigations and compliance audits across multiple jurisdictions.
- **Operational flexibility:** FireBreak enables secure, scheduled connectivity for system updates, vendor access, or emergency response without persistent exposure. This flexibility ensures that critical flight and ground operations remain uninterrupted, even as security requirements or operational needs change.
- **Supply chain and insider threat protection:** By ensuring all third-party and privileged access is always temporary, logged, and physically controlled, FireBreak closes crucial security gaps in the extended aviation ecosystem. This dramatically reduces the risk of supply chain compromise and insider attacks, which are among the most challenging threats facing aviation today.

Conclusion

With Goldilock FireBreak, aviation operators gain a decisive advantage in an era where cyber threats are relentless and operational continuity is non-negotiable. FireBreak complements and extends existing approaches to network separation, isolation and protection strategies. Delivering uncompromising, hardware-enforced security on demand, that shields every critical layer of aviation: from core airport systems and remote operations to vital onboard avionics. It makes essential assets invisible and unreachable to even the most advanced adversaries whenever needed.

This isn't just another security layer; it's a fundamental shift. FireBreak's real-time isolation enhances compliance, while auditable controls empower operators to not only meet the most demanding global regulatory requirements but also adapt swiftly to emerging risks. It fosters trust with regulators, partners, and the millions of passengers who depend on secure air travel every day.

In a sector where safety, resilience, and reputation are paramount, FireBreak stands out as the ultimate assurance: future-proof protection for aviation's most vital operations in a perpetually evolving threat landscape.