2026

seceon

The Strategic State of Cybersecurity for USA Airports and Avionics:

2026 Resilience and the Seceon Autonomous Paradigm

How Autonomous Security Strengthens Cyber Resilience Across U.S. Airports and Avionics Systems

Executive Summary

By 2026, U.S. airports and aircraft have evolved into highly connected, AI-driven digital ecosystems. Airports now operate as integrated data hubs, and modern aircraft function as networked platforms reliant on continuous connectivity. While this transformation has improved efficiency, safety, and passenger experience, it has significantly expanded the aviation cyber attack surface.

The sector has become a high-value target for both nation-state and criminal threat actors, capable of exploiting legacy systems, supply-chain dependencies, and always-on connectivity. Recent incidents demonstrate that cyber failures can rapidly cascade across airports, airlines, and vendors, impacting operations, safety, and public trust.

As a result, cybersecurity is no longer a supporting IT function but a core operational and safety requirement. Regulatory mandates now emphasize continuous monitoring, rapid incident response, and resilience. To meet these demands, aviation organizations increasingly rely on autonomous, AI-driven security platforms that can detect and respond to threats at machine speed.

Key Findings

- **Aviation has become a prime cyber target** due to its critical role in national security, safety, and economic continuity.
- **Expanded digital connectivity has eroded traditional security boundaries**, exposing legacy IT, OT, and avionics systems to modern threats.
- **Nation-state and criminal actors increasingly exploit persistence and supply-chain access**, enabling large-scale, cascading disruptions.
- **Regulatory bodies now treat cybersecurity as an operational and safety requirement**, not an IT best practice.
- **Autonomous, AI-driven security is essential**, as manual and reactive defense models cannot match the speed or complexity of aviation cyber threats.

The Inflection Point: The 2026 Landscape of Aviation Interconnectivity

The year 2026 represents a critical inflection point in the technological evolution of the global aviation sector, characterized by the convergence of hyper-connectivity, autonomous intelligence, and a radically expanding digital attack surface. Airports in the United States have undergone a profound transition, moving away from traditional infrastructure models to become integrated digital hubs that prioritize operational efficiency and a seamless passenger journey through data-driven decision-making and artificial intelligence.

This evolution is underpinned by a widespread commitment to digital capabilities, with 94% of airport executives now identifying these advancements as essential for commercial returns and 95% of airports actively exploring or deploying AI solutions.

Modern aircraft have simultaneously transitioned into sophisticated "flying data centers," where once-isolated avionics systems are now deeply embedded in a digital ecosystem that includes passenger Wi-Fi, electronic flight bags, and satellite communication links.

While this "nose-to-tail" connectivity enhances fuel efficiency and navigational precision, it effectively erodes the traditional air gaps that historically protected safety-critical flight systems. The consequence of this transformation is an industry that is simultaneously more efficient and more vulnerable than at any point in its history. Cybersecurity has therefore shifted from a peripheral IT concern to a primary operational imperative, with the potential to impact not only business continuity but also passenger safety and national security.

Aviation Digital Transformation Theme (2026)	**Primary Technology Drivers**	**Core Operational Benefit**	**Cybersecurity Risk Factor**
Intelligent Passenger Processing	Biometrics, Facial Recognition, Digital ID.	Reduced queues and frictionless boarding.	Exposure of biometric datasets and identity theft.
Autonomous Ground Operations	Robotics, Autonomous Apron Vehicles, AI Baggage Handling.	Operational cost reduction and increased throughput.	IoT/OT endpoint proliferation and command injection.
Connected Flight Decks	NextGen Avionics, EFBs, Satcom.	Real-time maintenance and optimized routing.	Lateral movement from passenger cabin to flight control domain.
Digital Twin Operations	Virtual replicas of airport and airspace.	“What-if” testing and predictive maintenance.	Intellectual property theft and simulation manipulation.
AI-Driven Infrastructure	Agentic AI, Predictive Maintenance, Smart Retail.	Proactive engagement and high-efficiency facilities.	Automated reconnaissance and agentic AI exploitation.

The Adversary Ecosystem: APT Strategies and Geopolitical Sabotage

The threat landscape in 2026 is dominated by highly sophisticated nation-state actors and professionalized cybercriminal syndicates that utilize advanced persistent threat (APT) methodologies to achieve long-term strategic objectives. In the context of U.S. critical infrastructure, the primary concern has shifted from traditional cyber espionage-the theft of information-toward pre-positioning for future sabotage. Adversaries are increasingly establishing latent footholds within transportation and communication networks that can be activated to disrupt military mobilization or civilian logistics during a geopolitical crisis.

Volt Typhoon and the Doctrine of Stealth Persistence

Volt Typhoon, a threat actor attributed to the People's Republic of China, stands as the preeminent threat to the U.S. airport and transportation sectors in 2026. Active since at least 2021, the group specializes in long-term intrusions into critical infrastructure, including communications, energy, water, and transportation hubs. Their pattern of behavior is fundamentally different from traditional espionage; the U.S. government assesses with high confidence that Volt Typhoon is pre-positioning on IT networks to enable lateral movement to operational technology (OT) assets for potential destructive or disruptive attacks.

The hallmark of Volt Typhoon’s operations is the use of "Living Off the Land" (LOTL) techniques, which involve the exclusive use of native, legitimate system tools to execute their objectives. By avoiding custom malware, they blend into normal network activity and evade traditional security tools for extended periods, in some cases remaining undetected for over 300 days.

They achieve initial access by exploiting public-facing edge devices such as routers, firewalls, and VPN hardware from vendors like Fortinet, Cisco, and Ivanti. Once inside, they use tools like Impacket and PsExec to traverse the environment and PowerShell to query Windows event logs for specific user activity, allowing them to extract security logs and credentials while minimizing their footprint.

Sandworm (APT44) and the Professionalization of Sabotage

Russian state-sponsored group Sandworm, also known as APT44, continues to represent the "apex of state-sponsored destructive hacking" in 2026. Linked to GRU Unit 74455, Sandworm's operations have expanded from traditional espionage into a full-spectrum capability that includes sabotage and battlefield support.

By late 2025 and early 2026, the group demonstrated an evolution in operational tradecraft, integrating new wiper families such as AcidPour and ZEROLOT against critical infrastructure, particularly energy and transportation sectors.

Sandworm frequently targets the telecommunications and shipping industries, with APT detections in the telecom sector increasing by 92% in the first quarter of 2025. Their tactics often involve supply-chain compromises and the hijacking of firmware update workflows to maintain long-term, stealthy persistence on network equipment globally. Unlike groups motivated by financial gain, Sandworm's campaigns are explicitly aligned with Russian military and geopolitical priorities, where collateral damage is often considered an intentional outcome to undermine public belief in Western institutions.

North Korean and Criminal Actor Convergence

The North Korean Lazarus Group remains a potent threat, particularly in the theft of aerospace and defense technology. In late 2025, Lazarus was observed targeting European defense manufacturers to exfiltrate sensitive data on advanced drone components and manufacturing processes. These operations are often combined with revenue-generating financial attacks, including cryptocurrency theft, which support the regime's strategic goals.

Simultaneously, the cybercrime ecosystem has become highly professionalized through the Ransomware-as-a-Service (RaaS) model. Groups like Rhysida and Scattered Spider have demonstrated the capability to paralyze major transportation hubs, as seen in the 2024 breach of the Port of Seattle. Criminal actors are increasingly sharing infrastructure and payloads with nation-states, further blurring the line between purely financial extortion and geopolitical disruption.

Threat Actor Group	Key Affiliation	Primary 2026 TTPs	Strategic Aviation Sector Target
Volt Typhoon	PRC State-Sponsored.	LotL, Edge device exploitation, SOHO router proxying.	US Airfield OT, HVAC systems in server rooms, Communication hubs.
Sandworm (APT44)	Russian GRU.	Wiper malware (AcidPour, ZEROLOT), Firmware hijacking, Supply-chain sabotage.	NATO Transportation and Shipping, Energy providers, Logistics.
Lazarus Group	North Korea.	Social engineering (Fake Job Lures), Crypto-drainers, RATs.	Aerospace Manufacturers, Drone Tech, Defense Supply Chain.
Scattered Spider	Cybercrime/“Young ‘Show-offs’”.	Vishing, Help-desk fraud, Cloud token theft, Identity drift.	SaaS providers, Airline booking portals, Administrative workflows.
Rhysida	Cybercrime (RaaS).	Double extortion, Data theft without encryption, Legacy system exploitation.	Airport ticketing systems, Check-in kiosks, Passenger databases.

Systematic Failures and Breaches: 2023-2026 Analysis

The period leading into 2026 has been marked by a staggering 131% rise in cyberattacks across the aviation industry, driven by vulnerabilities in outdated operational technology (OT), interconnected supply chains, and sprawling digital networks. High-profile breaches have demonstrated that the industry is under constant threat, with failures in cybersecurity leading to grounded flights, passenger data compromise, and revenue losses amounting to billions of dollars annually.

The vMUSE and Collins Aerospace Platform Failure (September 2025)

A defining incident of late 2025 was the ransomware attack targeting Collins Aerospace’s vMUSE airport operations platform. The malware encrypted backend servers that manage check-in and boarding systems, forcing several major international airports, including London Heathrow, Brussels, and Berlin, to revert to manual, paper-based check-in processes.

This attack resulted in hundreds of flight delays and highlighted the "single point of failure" risk inherent in centralized airport technology providers. It illustrated that an attack does not need to target an airline directly to ground its fleet; targeting the shared infrastructure used by multiple carriers can achieve the same disruptive effect at scale.

The Delta and CrowdStrike Supply-Chain Catastrophe (July 2024)

While not a malicious breach, the July 2024 CrowdStrike outage remains a primary case study in aviation operational resilience. A faulty software update from the cybersecurity vendor crashed approximately 8.5 million Microsoft Windows computers globally, leading to a systemic failure of Delta Air Lines’ scheduling and crew-tracking systems.

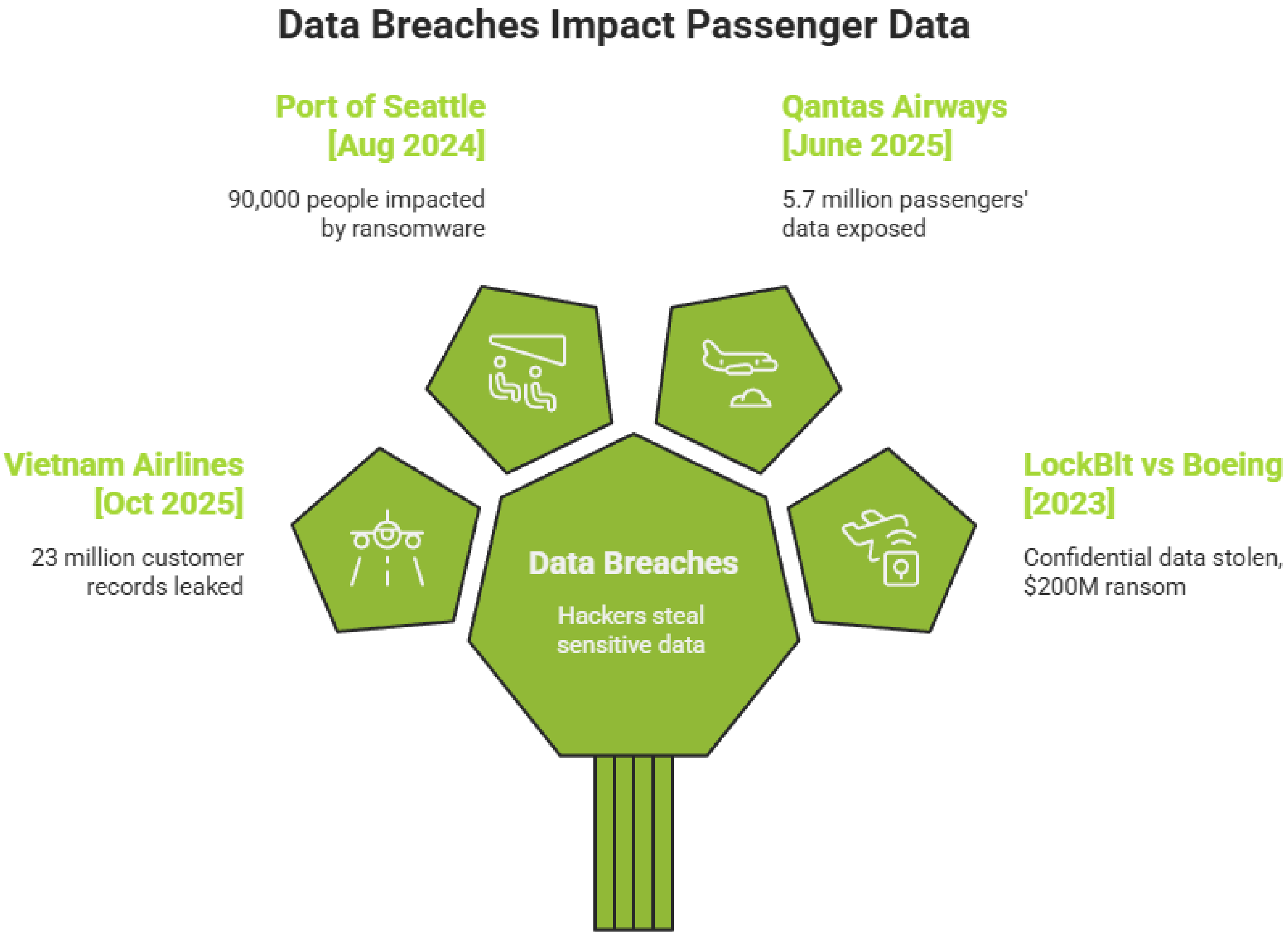
The resulting cancellation of over 7,000 flights and the delay of 35,500 more affected 1.3 million passengers and led to a $500 million lawsuit. This incident underscored how a single vulnerability in the cybersecurity supply chain can trigger cascading failures across an entire interconnected ecosystem.

Strategic Data Breaches and Passenger Impacts

Data theft remains a primary objective for financially motivated actors and state entities seeking intelligence.

- **Vietnam Airlines (October 2025):** Hackers compromised an online customer service platform belonging to a technology partner, leading to the upload of 23 million customer records onto data-trading forums.

- **Port of Seattle (August 2024):** The Rhysida ransomware group paralyzed ticketing and check-in kiosks at Seattle-Tacoma International Airport (SEA). The attack impacted 90,000 people and exposed sensitive employee, contractor, and parking data.
- **Qantas Airways (June 2025):** A compromise of a third-party customer servicing system exposed the personal data of 5.7 million passengers, including names, birth dates, and contact information.
- **LockBit vs. Boeing (2023):** The LockBit group faces a $200 million ransom demand after breaching Boeing's network and stealing confidential data, highlighting the vulnerability of the defense-aerospace supply chain.


Data Breaches Impact Passenger Data
Port of Seattle [Aug 2024]
90,000 people impacted by ransomware
Qantas Airways [June 2025]
5.7 million passengers' data exposed
Vietnam Airlines [Oct 2025]
23 million customer records leaked
LockBIt vs Boeing [2023]
Confidential data stolen, $200M ransom
Data Breaches
Hackers steal sensitive data

Technical Vulnerabilities in NextGen Avionics and Flight Decks

As aircraft transition into "E-Enabled" platforms, the technical vulnerabilities of traditional and NextGen avionics protocols have become a central focus of cybersecurity research and airworthiness certification. Modern aircraft segment their networks into distinct domains-the Aircraft Control Domain (ACD), Airline Information Services Domain (AISD), and Passenger Information and Entertainment Services Domain (PIESD)-but the historical "air gap" between these domains is increasingly being replaced by logical gateways.

The Legacy Challenge: ARINC 429 and MIL-STD-1553

The ARINC 429 data bus is a de-facto standard for civil avionics communication, designed in the 1970s with an emphasis on reliability and fault tolerance rather than security. It lacks any form of encryption or authentication, making it inherently insecure against contemporary cyber threats. Hardware-in-the-loop simulations have proven that a compromised ARINC 429 bus can be exploited to execute denial-of-service attacks on multi-function displays (MFDs), effectively disabling navigational aids by flooding the bus with spoofed terrain warnings or rogue data.

Similarly, the MIL-STD-1553 bus, used widely in military and some commercial aircraft, is vulnerable to many attacks that could damage the entire system, as it also lacks message origin authentication.

NextGen Protocols: ARINC 664 and the Ethernet Risk

To handle the high bandwidth requirements of modern flight decks, the industry adopted Avionics Full-Duplex Switched Ethernet (AFDX), codified as ARINC 664. While AFDX provides deterministic communication, it inherits standard vulnerabilities from the TCP/IP and Ethernet stacks. If an attacker gains access to the avionics switch fabric, standard network attacks like MAC address spoofing or switch flooding become theoretically possible. The most critical risk involves "pivoting" from the passenger domain to the cockpit by exploiting vulnerabilities in the in-flight entertainment (IFE) media server and bypassing misconfigured firewalls or logical gateways.

Air-to-Ground Link Exposure: ADS-B and ACARS

External communication links like Automatic Dependent Surveillance-Broadcast (ADS-B) and the Aircraft Communications Addressing and Reporting System (ACARS) operate over unencrypted radio frequencies, making them accessible via low-cost Software Defined Radio (SDR) hardware.

- **ADS-B Vulnerabilities:** The technical specification (DO-260B) includes no mechanism for cryptographic authentication. This allows an attacker to generate "ghost aircraft" on air traffic control screens, creating dangerous confusion and potential denial-of-service in crowded airspace.
- **ACARS Risks:** Transmitted in cleartext ASCII, ACARS messages lack integrity codes. A sophisticated attacker can theoretically intercept a message, modify critical flight data such as waypoint coordinates, and retransmit it to the aircraft’s Flight Management System (FMS).

GNSS Spoofing and Electronic Flight Bag (EFB) Vectors

Navigation systems are also increasingly targeted through Global Navigation Satellite System (GNSS) spoofing, where counterfeit signals cause the FMS to calculate an incorrect position, leading to autopilot course corrections based on false data. Furthermore, portable Electronic Flight Bags (EFBs) used by pilots deliver a significant payload vector. If a pilot’s tablet is infected, potentially via a public hotel Wi-Fi, and then connected to the Aircraft Interface Device (AID), it can bypass external perimeters and deliver a payload directly into the cockpit environment.

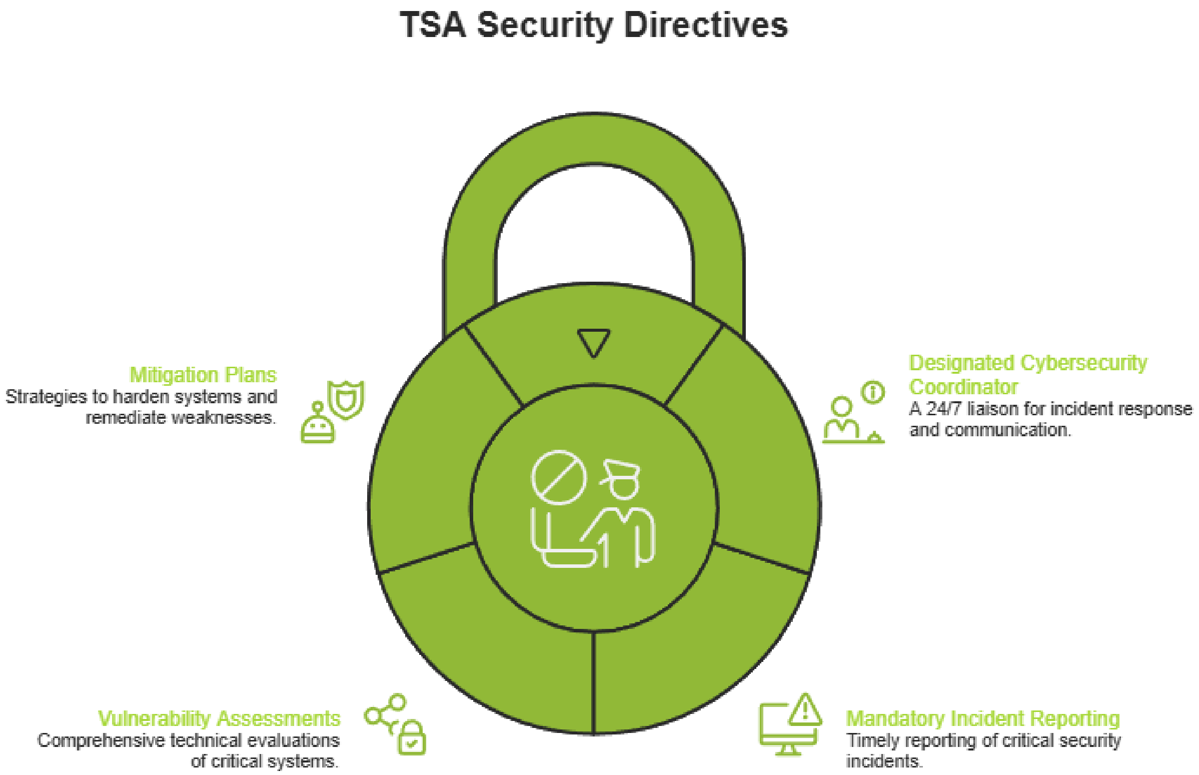
The Regulatory Framework: Compliance Mandates and Federal Action

By 2026, the regulatory landscape for aviation cybersecurity has shifted from advisory frameworks to mandatory, performance-based requirements enforced by the TSA and FAA. These regulations aim to secure the entire transportation ecosystem, from the ground-based industrial control systems (ICS) at airports to the software code powering aircraft engines.

TSA Security Directives for Airports and Aircraft Operators

The TSA has issued a series of Security Directives (SDs) and Emergency Amendments (EAs) that mandate four primary elements for airport and aircraft operators. Failure to comply can result in civil penalties of up to $13,910 per violation.

1. **Designated Cybersecurity Coordinator:** Each airport must designate a qualified coordinator available 24/7 to serve as the primary liaison with TSA and CISA and manage incident response procedures.
2. **Mandatory Incident Reporting:** Critical incidents affecting operational systems or data integrity must be reported to CISA within 24 to 72 hours. The threshold is low, often including attempted intrusions or suspicious network activity.
3. **Vulnerability Assessments:** Airports must conduct comprehensive technical assessments identifying critical systems, including navigation aids, airport lighting, fuel management, and emergency notification systems.
4. **Mitigation Plans:** Based on assessment findings, airports must implement a realistic Cybersecurity Implementation and Mitigation Plan to harden systems and remediate weaknesses.


TSA Security Directives
Mitigation Plans
Strategies to harden systems and remediate weaknesses.
Designated Cybersecurity Coordinator
A 24/7 liaison for incident response and communication.
Vulnerability Assessments
Comprehensive technical evaluations of critical systems.
Mandatory Incident Reporting
Timely reporting of critical security incidents.

FAA Airworthiness and Maintenance Digitization

The FAA has codified new rules to address cybersecurity vulnerabilities in aircraft design, engines, and propellers. Under the FAA Reauthorization Act of 2024, the Administrator has sole rulemaking authority to implement these regulations.

- **14 CFR Part 25 and Part 39 Updates:** Design applicants must conduct risk assessments for potential "intentional unauthorized electronic interactions" (IUEI) and develop vulnerability mitigation plans. Airworthiness Directives (ADs) now frequently include restrictive limitations to prevent structural or systemic failures prompted by cyber vulnerabilities.
- **Maintenance Digitization (Effective July 1, 2025):** All Part 145 repair stations are required to maintain digital records with electronic signature capabilities, audit trail maintenance, and real-time reporting of component installations. This transition focuses on ensuring data integrity and the traceability of life-limited parts.
- **DO-326A/ED-202A:** This set of standards remains the de facto mandatory guidance for cybersecurity airworthiness certifications in the U.S. and Europe, focusing on the Airworthiness Security Process (AWSP) and Security Risk Assessment Process (SRAP).

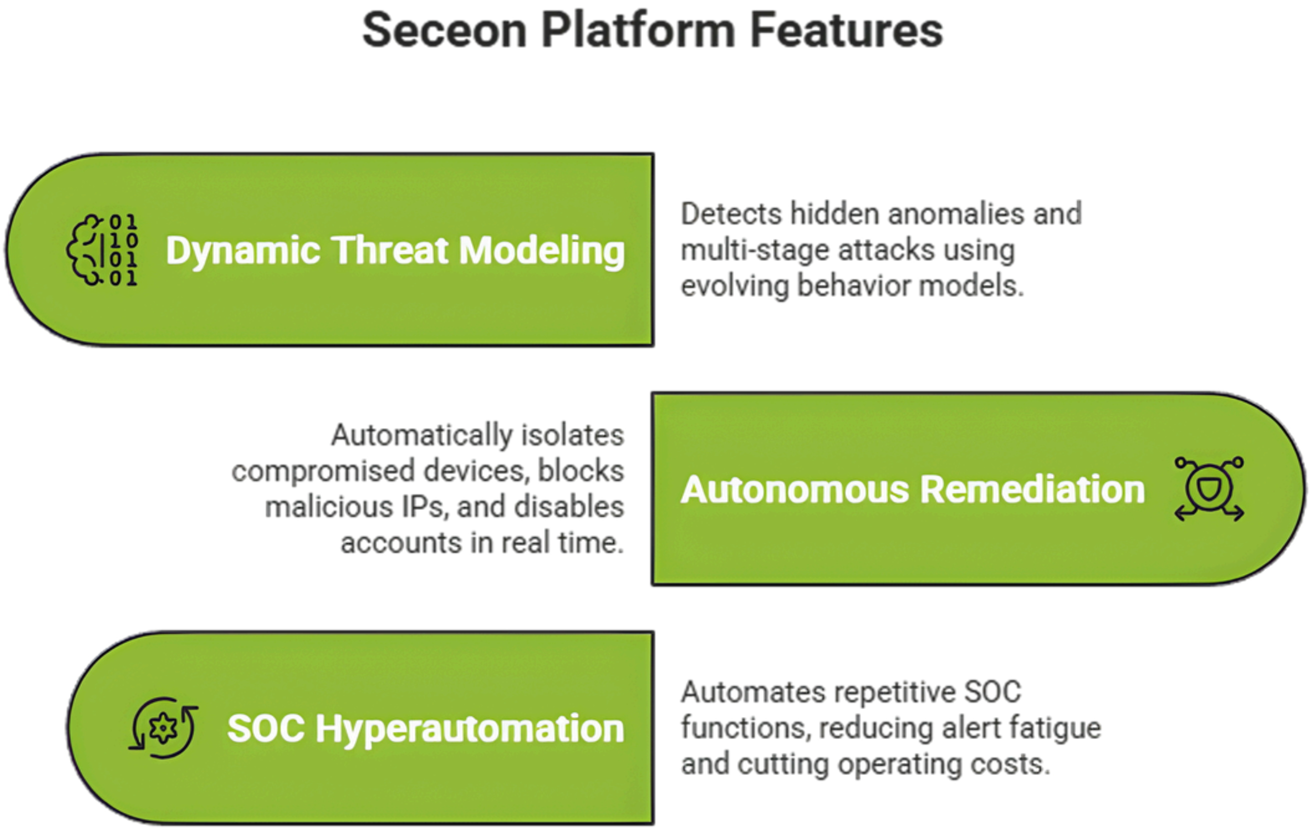
Regulatory Mandate (2025–2026)	Primary Agency	Key Requirement	Sector Applicability
TSA SD 1580/82-2022-01D	TSA.	Rail and Airport OT mitigation and testing.	Airport Operators, Freight/Passenger Rail.
TSA SD Pipeline-2021-02F	TSA.	Incident Response Plans and CAP (Assessment Plans).	Aviation Fuel Supply, Critical Pipelines.
14 CFR Part 25 UEI Rule	FAA.	Design-level risk mitigation for transport category aircraft.	Aircraft/Engine Manufacturers (DAHs).
FAA Part 145 Digital Records	FAA.	Electronic signatures and time-stamped digital maintenance entries.	Repair Stations, Maintenance Organizations.
ICAO Cybersecurity Strategy	ICAO.	Global harmonization of regulations and information sharing.	International Civil Aviation.

The Seceon Platform: Autonomous Security for the 2026 Aviation Infrastructure

The speed and volume of AI-powered attacks in 2026 have rendered human-dependent security operations centers (SOCs) insufficient. In this landscape, the Seceon Open Threat Management (OTM) platform has emerged as a vital technology for airports and avionics providers, moving beyond reactive detection to autonomous, self-learning defense. Seceon’s unique approach integrates data from logs, networks, clouds, and applications into a unified behavioral analytics framework.

aiSIEM and aiXDR-PMax: Unified Visibility and Real-Time Containment

Seceon’s platform overcomes the limitations of legacy SIEMs by ingesting raw, real-time streaming data from over 900 devices and systems without storage or indexing delays. This provides a 99.7% detection rate and reduces "Mean Time to Detect" (MTTD) by 95% compared to traditional solutions.



Seceon Platform Features

Dynamic Threat Modeling

Detects hidden anomalies and multi-stage attacks using evolving behavior models.

Autonomous Remediation

Automatically isolates compromised devices, blocks malicious IPs, and disables accounts in real time.

SOC Hyperautomation

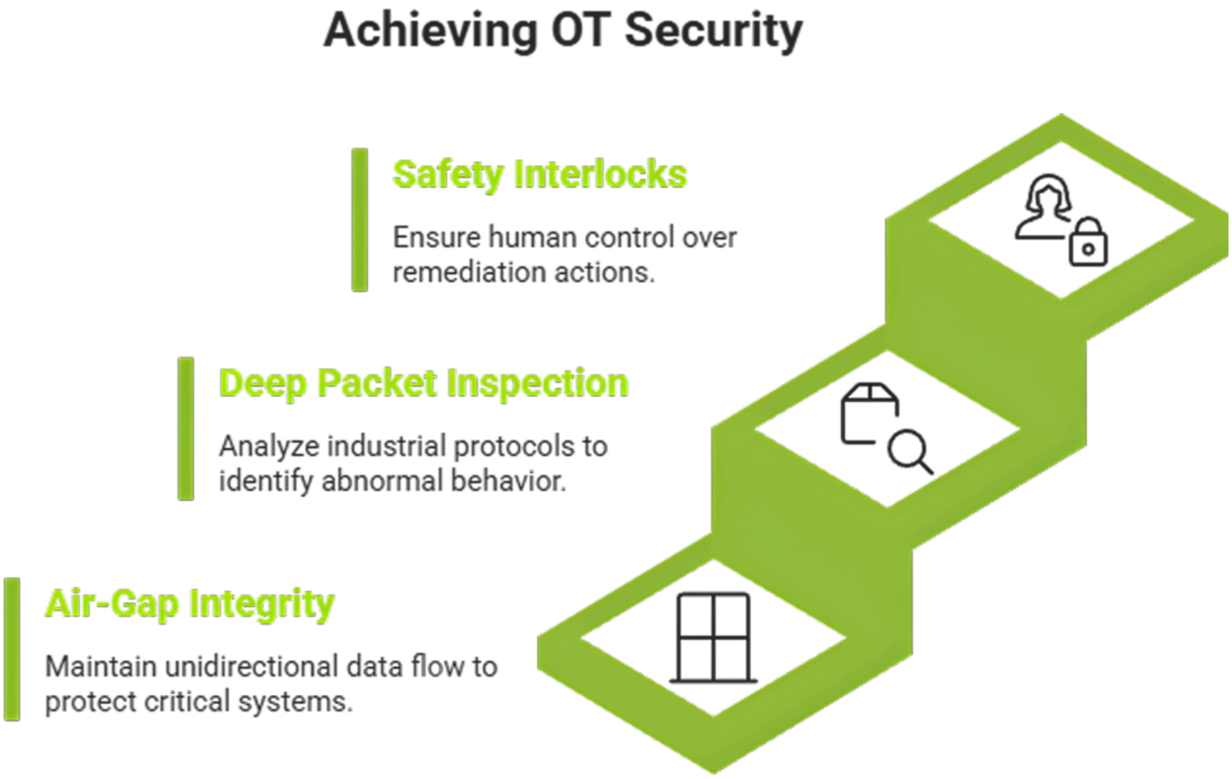
Automates repetitive SOC functions, reducing alert fatigue and cutting operating costs.

- **Dynamic Threat Modeling (DTM):** The platform uses patented DTM technology to build evolving models of user and network behavior, allowing it to detect hidden anomalies and multi-stage attacks, such as those used by Volt Typhoon, that bypass static, rule-based methods.
- **Autonomous Remediation:** Seceon aiXDR-PMax extends this detection to endpoints and IoT assets. It can automatically isolate compromised devices, block malicious IP addresses, or disable accounts in real time, effectively shrinking the window of vulnerability from hours to minutes.
- **SOC Hyperautomation:** By automating repetitive SOC functions, Seceon reduces alert fatigue by 70% and cuts operating costs by an estimated 50–70%.

Bridging the OT Barrier with aiSecOT360

The protection of legacy industrial control systems (ICS) and Programmable Logic Controllers (PLCs) is perhaps the most significant challenge for airports in 2026. Many of these systems run on unsupported Windows versions and cannot host security agents. Seceon’s aiSecOT360 module, announced in early 2026, unifies NG-SIEM, NDR, and UEBA to provide holistic protection for legacy OT infrastructure.

- **Air-Gap Integrity:** The platform’s dual-stage Collection & Control Engine (CCE) maintains air-gap integrity through unidirectional data flow, a critical requirement for safety-critical airfield systems.
- **Deep Packet Inspection (DPI):** aiSecOT360 supports over 70 industrial protocols (e.g., Modbus, DNP3, BACnet), providing deep operations understanding to identify abnormal behavior in baggage systems or navigation aids that might otherwise go unnoticed.
- **Safety Interlocks:** In airport environments where an accidental system shutdown could be catastrophic, aiSecOT360 includes "safety interlocks" that ensure human operators control the final remediation action while being empowered by AI-driven actionable guidance.



Achieving OT Security

Safety Interlocks

Ensure human control over remediation actions.

Deep Packet Inspection

Analyze industrial protocols to identify abnormal behavior.

Air-Gap Integrity

Maintain unidirectional data flow to protect critical systems.

Conclusion: Strategic Resilience for the Next Decade

As the aviation industry looks beyond 2026, the strategy must shift from a "secure the perimeter" mindset to a comprehensive "Assume Breach" architecture. Organizations implementing Zero Trust AI Security have already reported 76% fewer successful breaches and a 67% reduction in security administrative overhead. The future of aviation cybersecurity lies in the successful integration of autonomous defense systems that can counter AI-driven threats at machine speed.

Airports and avionics manufacturers must prioritize the modernization of legacy OT systems, the digitization of supply-chain mapping, and the adoption of unified platforms like Seceon that bridge the gap between IT and OT. By leveraging predictive threat modeling and autonomous response, the aviation sector can ensure that its digital transformation enhances safety and efficiency without introducing unacceptable levels of risk. The proactive adoption of these technologies, coupled with rigorous compliance with emerging federal mandates, will define the resilient aviation ecosystem of 2030.

AVIATION CYBERSECURITY 2026

Resilience and Autonomous Defense for USA Airports and Avionics

The 2026 Aviation Threat Landscape

131% Increase in cyberattacks

94% Airports view digital as essential

95% Deploying AI Solutions

300+ Days threats remain hidden

Federal Compliance Requirements

- **24/7 Contact:** Designated coordinator for TSA/CISA liaison and incident response
- **Incident Alerts:** Mandatory CISA reporting within 24-72 hours. $13,910 penalties
- **System Audits:** Comprehensive vulnerability assessments of navigation, lighting, fuel
- **Remediation:** Implementation plans to harden infrastructure and address gaps
- **Aircraft Design:** 14 CFR Part 25 IUEI cyber risk assessments for new aircraft
- **Maintenance:** Part 145 digital records with e-signatures (effective July 2025)
- **Certification:** DO-326A/ED-202A airworthiness security standards

Seceon Autonomous Platform

- **aiSecOT360:** Legacy ICS/OT protection, 70+ protocols
- **aiSIEM:** 900+ device integration, real-time analytics
- **aiXDR-PMax:** Autonomous isolation and containment
- **Threat Models:** Dynamic behavioral analysis for APTs
- **Air-Gap:** Unidirectional flow for safety-critical systems
- **Protocols:** Modbus, DNP3, BACnet support
- **Automation:** SOC hyperautomation with safety interlocks

Measured Platform Performance

Volt Typhoon

PRC

Living-off-the-land stealth. Targets US airfield OT, HVAC, comms infrastructure. 300+ day persistence.

Sandworm

Russian GRU

Destructive wiper malware. 92% surge in telecom attacks. Targets NATO transportation.

Lazarus

N. Korea

Aerospace tech exfiltration. Drone component theft. Defense supply chain compromise.

Scattered Spider

Cybercrime

Vishing, help-desk fraud. Cloud token theft. Airline portal attacks.

Rhysida

RaaS

Double extortion model. Legacy system exploitation. Ticketing infrastructure.

Measured Platform Performance

99.7% Detection Accuracy

95% Faster mean time to detect

70% Reduction in alert fatigue

76% Fewer successful breaches

Operating Efficiency

50-70%

Cost Reduction

- **Operational resilience:** Protection for critical airport infrastructure and flight operations
- **67% administrative efficiency:** Reduced security overhead through AI automation
- **Platform consolidation:** Replace 10-15 point solutions with unified architecture
- **Real-time response:** Autonomous containment reduces exposure from hours to minutes
- **Safety-first design:** Air-gap integrity maintained for OT environments
- **Compliance automation:** Built-in TSA/FAA mandate tracking and audit trails

Autonomous Defense For Modern Aviation

Purpose-built security platforms enable airports and avionics manufacturers to counter AI-driven threats at machine speed, maintain federal compliance, and achieve Zero Trust resilience across interconnected IT/OT environments

Trusted by 9,300+ customers worldwide | Monitoring over 1.3 trillion security events per day

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,300 clients.

References and Citations:

This whitepaper is based on research and data from:

- Vantage Group. (2026). *Airports in 2026: Data-driven decision making, AI and more seamless passenger journeys*. Retrieved January 22, 2026, from https://www.vantagegroup.com/hub/airports-in-2026-data-driven-decision-making-ai-and-more-seamless-passenger-journeys/
- International Airport Review. (2026). *Top airport technology trends set to shape the future of airport operations in 2026*. Retrieved January 22, 2026, from https://www.internationalairportreview.com/article/300553/top-airport-technology-trends-set-to-shape-the-future-of-airport-operations-in-2026/
- IDSTch. (2026). *Securing the skies: 2025 avionics cybersecurity in the era of connected flight*. Retrieved January 22, 2026, from https://idstch.com/cyber-information-warfare/cyber-security-of-aircraft-avionics-on-commercial-and-military-aircrafts/
- LDRA. (2026). *DO-326B/ED-202A: Your trusted aerospace cybersecurity framework guide*. Retrieved January 22, 2026, from https://ldra.com/aerospace-security-framework/

References and Citations:

This whitepaper is based on research and data from:

- ResearchGate. (2026). *Vulnerability assessment of legacy and next-generation aviation protocols from ARINC 664 to ADS-B*. Retrieved January 22, 2026, from https://www.researchgate.net/publication/399514489_Vulnerability_Assessment_of_Legacy_and_Next-_Generation_Aviation_Protocols_From_ARINC_664_to_ADS-B
- SecureWorld. (2026). *Cybersecurity in aviation: Rising threats and modernization efforts*. Retrieved January 22, 2026, from https://www.secureworld.io/industry-news/aviation-cybersecurity-threats
- Biometric Update. (2026). *TSA touchless ID biometric entry lanes coming to 50 additional US airports*. Retrieved January 22, 2026, from https://www.biometricupdate.com/202601/tsa-touchless-id-biometric-entry-lanes-coming-to-50-additional-us-airports
- Eye Security. (2026). *The cyber threat landscape 2026: Building resilience, acting fast*. Retrieved January 22, 2026, from https://www.eye.security/blog/cyber-threat-landscape-outpacing-threat-actors-building-resilience
- Seceon. (2026). *Zero trust AI security: The comprehensive guide to next-generation cybersecurity in 2026*. Retrieved January 22, 2026, from https://seceon.com/zero-trust-ai-security-the-comprehensive-guide-to-next-generation-cybersecurity-in-2026/
- Copenhagen Optimization. (2026). *6 airport technology trends to watch in 2026*. Retrieved January 22, 2026, from https://copenhagenoptimization.com/blog/airport-technology-trends-to-optimize-your-airport

About the Author

Smit Kadakia

Co-founder, Seceon Inc.

Smit leads Seceon's data science and machine learning team, focused on developing a state-of-the-art behavior anomaly detection solution. Smit holds a B.S. from VJTI, Mumbai, an MS in Computer Science from Indian Statistical Institute, Kolkata, and an MBA from Southern New Hampshire University, Manchester. Smit and the team at Seceon have built the industry's first and only fully automated threat detection and remediation system using a combination of machine learning and artificial intelligence techniques. Seceon's approach includes analysis of all traffic, flows, and processes in and out of the network and correlates them near-simultaneously with behavioral analytics, recognized and zero-day exploits, and policies to surface threats and proposed responses in near-record real-time.

About the Author

Anamika Pandey

AI/ML Cybersecurity Engineer, Seceon Inc.

Anamika leverages artificial intelligence, machine learning, and Dynamic Threat Modeling (DTM) to fortify IT, OT, IoT, and cloud infrastructures. Her expertise lies in advancing AI-driven defense strategies that not only ensure compliance and resilience but also deliver measurable ROI. Through Seceon's OTM Platform, she helps organizations anticipate, detect, and mitigate evolving cyber threats, empowering them to stay secure, adaptive, and future-ready.