SCOTTS
INTERNATIONAL

Aviation Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Aviation Cyber Security Market Analysis

The aviation cyber security market size is valued at USD 11.51 billion in 2025 and is projected to reach USD 18.23 billion by 2030, reflecting a solid 13.12% CAGR during the forecast window. Rising cyber-attack frequency since 2020, rapid cloud migration, and the surge of connected assets across airports, aircraft, and air traffic control (ATC) systems underpin this expansion. North American regulatory funding, European harmonized rules, and Middle-Eastern infrastructure build-outs collectively elevate spending levels. Technology priorities are shifting toward zero-trust architectures, managed detection-and-response services, and quantum-safe encryption, while operators pursue outsourcing to address the sector's persistent shortage of aviation-domain security talent. Intensifying merger activity among incumbents and niche vendors aims to close capability gaps in operational-technology (OT) protection, threat intelligence, and compliance automation across the aviation cyber security market.

Global Aviation Cyber Security Market Trends and Insights

Surge in Integrated Digital Aviation Ecosystems Expanding Cyber-Attack Surface

The convergence of passenger services, airport OT, aircraft data links, and third-party logistics is redefining the aviation cyber security market. In August 2024 a Port of Seattle breach brought down peripheral systems, demonstrating how lateral movement can disrupt operations even when flight safety is maintained. US Transportation Security Administration allocated USD 136.17 million toward aviation-focused cyber defenses for FY 2025, signaling that perimeter-centric strategies are no longer sufficient.

Stakeholders now prioritize holistic architectures that map and secure interdependencies across the entire aviation cyber security market.

Rapid Adoption of Open-Architecture Avionics & IoT Sensors in Aircraft Fleets

Open standards cut lifecycle costs and enable plug-and-play upgrades, yet they propagate identical vulnerabilities across fleets. The FAA's August 2024 proposal underscores risks from maintenance laptops, airport Wi-Fi, and Bluetooth sensors that can pivot to flight-critical domains. CISA advisories exposing flaws in collision-avoidance transponders add urgency. Airlines and OEMs thus must blend secure-coding practices with runtime monitoring to mitigate systemic exposure within the aviation cyber security market.

Fragmented Legacy Systems Hindering Unified Security Governance

Defense Industrial Base studies find that 98% of aviation organizations sustain supply-chain partnerships hit by cyber incidents, propagating risk across decades-old ATC and baggage networks. Encryption, multifactor authentication, and centralized logging remain absent from many legacy nodes, forcing airlines to juggle redundant controls that inflate cost while leaving material gaps.

Other drivers and restraints analyzed in the detailed report include:

Growth in Cloud-Based Airport Operations Platforms & SaaS Flight Applications / Integration of 5G & Satellite Connectivity in ATC Networks Requiring Zero-Trust Security / High Certification & Air-Worthiness Validation Costs Delaying Deployments /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Threat Intelligence & Response solutions captured 28% of 2024 revenue within the aviation cyber security market share, evidencing the sector's pivot to proactive monitoring. Managed Security Services exhibit a 13.8% CAGR through 2030. This momentum stems from a limited pool of aviation-literate analysts and the need to meet 24□7 regulatory logging mandates without inflating internal headcount.

OEMs and airlines turn to managed offerings that bundle SIEM, OT anomaly detection, and compliance dashboards. The aviation cyber security market size for managed services is forecast to increase in tandem with mandatory incident-reporting timelines and zero-trust rollouts. Vendor differentiation now centers on possessing flight-certified engineers able to integrate with avionics and ATC workflows rather than generic SOC staffing models.

Network Security retained 32% of 2024 spend, underlining residual reliance on perimeter firewalls. Yet Cloud Security leads growth at a 15.1% CAGR as multi-cloud, containerized workloads move passenger check-in, crew rostering, and predictive maintenance off-premise. The aviation cyber security market size for cloud controls benefits from shared-responsibility education campaigns and the rollout of sovereign-cloud regions tailored for regulated sectors.

Endpoint protection stretches from crew tablets to engine-health sensors, compelling vendors to unify policy engines across distinct hardware. Application-level firewalls, API gateways, and runtime code-scanning also accelerate because SaaS flight-planning tools must pass both cyber and safety audits before release in the aviation cyber security market.

The Aviation Cyber Security Market is Segmented by Solution (Threat Intelligence and Response, Identity and Access Management, Data Loss Prevention, and More), Security Type (Network Security, Endpoint Security, Application Security, and

More), Deployment Mode (On-Premise, Cloud-Deployed), Application (Airline Management, Air Cargo Management, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America leads the aviation cyber security market with 40% revenue in 2024, underpinned by the FAA's USD 35 million cybersecurity line item for FY 2026 and TSA's USD 136.17 million allocation to harden airports. All major U.S. carriers now embed AI-driven threat detection, and Canadian ANSP NAV CANADA adopts zero-trust blueprints mirroring federal best practices. The region's vendor ecosystem also benefits from defense primes cross-selling hardened solutions into commercial fleets.

Europe maintains robust adoption through EASA Part-IS and EUROCONTROL CERT coordination. Pan-EU harmonization reduces duplication and increases pooled intelligence sharing. Thales' three-year AI partnership with CEA to develop trusted GenAI for defense highlights regional innovation targeted at detection-and-response acceleration. GDPR adds another compliance dimension, prompting privacy-by-design encryption and tokenization efforts inside the aviation cyber security market.

The Middle East posts a 12.5% CAGR driven by Gulf hub expansion and a documented 183% DDoS spike during Q1 2024, pushing operators to secure multi-airport portfolios rapidly. Flag carriers in the region now mandate managed SOC coverage for ground systems and deploy satellite-route diversity to counter spoofing attempts. Asia-Pacific, led by China, Japan, and India, follows close behind through large-scale fleet additions, government smart-airport grants, and the region's first ministerial aviation-cyber summit hosted in Delhi in September 2024. Diverse regulatory baselines encourage both international vendors and regional specialists to localize offerings for different certification regimes.

List of Companies Covered in this Report:

Honeywell International Inc. / Cisco Systems Inc. / Thales Group / Raytheon Technologies Corporation / BAE Systems plc / Lockheed Martin Corporation / Northrop Grumman Corporation / Collins Aerospace / Unisys Corporation / Palo Alto Networks Inc. / SITA SC / Leidos Holdings Inc. / IBM Corporation / Airbus CyberSecurity / The Boeing Company / Darktrace plc / Fortinet Inc. / Trend Micro Inc. / Telespazio S.p.A. / Rohde and Schwarz GmbH and Co KG / Cyberbit Ltd. /

Additional Benefits:

The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

Aviation Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:
- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.
** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-27
		Signature	