+357 96 030922
info@marketpublishers.com

Aerospace Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Type, Threat Type, Application, End User and By Geography

https://marketpublishers.com/r/A231B9293566EN.html
Date: October 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: A231B9293566EN

Abstracts

According to Stratistics MRC, the Global Aerospace Cybersecurity Market is accounted for $32.2 billion in 2025 and is expected to reach $56.4 billion by 2032 growing at a CAGR of 8.3% during the forecast period. Aerospace cybersecurity refers to the protection of digital systems, networks, and data used in aviation and space operations from cyber threats. It encompasses safeguarding aircraft avionics, satellite communications, air traffic control systems, and ground infrastructure against unauthorized access, data breaches, and cyberattacks. As aerospace platforms increasingly rely on interconnected technologies like IoT, AI, and cloud computing, cybersecurity becomes critical to ensuring operational safety, national security, and passenger privacy. Aerospace cybersecurity involves implementing robust encryption, intrusion detection, secure software development, and compliance with international standards to defend against evolving threats in both commercial and defense aerospace environments.

Market Dynamics:

Driver:

Rising Cyber Threats

The aerospace cybersecurity market is driven by escalating cyber threats targeting aviation and space systems. Increasing reliance on digital technologies like IoT, AI, and cloud computing has expanded the attack surface across aircraft, satellites, and ground

+357 96 030922
info@marketpublishers.com

control networks. Sophisticated cyberattacks pose risks to operational safety, national security, and passenger data. As threat actors grow more advanced, aerospace organizations are investing heavily in proactive cybersecurity measures, including intrusion detection, encryption, and secure software development, to safeguard critical infrastructure and ensure mission continuity.

Restraint:

High Implementation Costs

High implementation costs remain a major restraint in the market. Deploying comprehensive security solutions across complex aerospace systems requires significant capital investment. Expenses include advanced software, hardware upgrades, skilled personnel, and testing infrastructure. Legacy systems often need costly integration with modern cybersecurity frameworks. These financial barriers limit adoption. Despite growing threats, budget constraints and long deployment cycles challenge scalability, making cost a critical factor that slows widespread implementation of cybersecurity technologies in aerospace operations.

Opportunity:

Digital Transformation in Aerospace

Digital transformation in aerospace presents a significant opportunity for cybersecurity growth. The integration of smart technologies—such as AI, IoT, and cloud computing—into aircraft, satellites, and ground systems enhances operational efficiency but also introduces new vulnerabilities. As aerospace platforms become more connected, the demand for robust cybersecurity solutions rises. This transformation drives innovation in threat detection, secure communications, and data protection. With governments and private firms, cybersecurity becomes essential for enabling safe, resilient, and future-ready aerospace ecosystems.

Threat:

System Integration Challenges

System integration challenges pose a notable threat to the market. Many aerospace platforms operate on legacy systems that are difficult to align with modern cybersecurity frameworks. Integrating new security protocols without disrupting mission-critical

+357 96 030922
info@marketpublishers.com

operations requires careful planning and technical expertise. Compatibility issues, data migration risks, and operational downtime can hinder implementation. These challenges slow adoption and increase vulnerability to cyberattacks. As aerospace systems grow more complex, overcoming integration barriers becomes vital to ensuring seamless and secure digital transformation.

Covid-19 Impact:

The COVID-19 pandemic disrupted the aerospace cybersecurity market by delaying R&D projects, straining budgets, and interrupting supply chains. Travel restrictions and remote work environments exposed new vulnerabilities in aerospace networks. However, the strategic importance of cybersecurity led to continued investment, especially in defense and critical infrastructure. Post-pandemic recovery has accelerated digital transformation, prompting renewed focus on securing aerospace systems.

The network security segment is expected to be the largest during the forecast period

The network security segment is expected to account for the largest market share during the forecast period, due to increasing need to protect interconnected systems such as aircraft avionics, satellite links, and air traffic control networks from cyber threats. As aerospace platforms adopt IoT and cloud-based technologies, securing data transmission and communication channels becomes critical. Network security solutions, including firewalls, intrusion detection systems, and encryption protocols, are essential for maintaining operational integrity and preventing unauthorized access across aerospace infrastructures.

The mission systems segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the mission systems segment is predicted to witness the highest growth rate, due to rising demand for secure, real-time decision-making capabilities in aerospace operations. Mission systems encompass critical functions such as navigation, targeting, and surveillance, which require robust cybersecurity to prevent manipulation or disruption. As defense and space agencies prioritize advanced mission capabilities, investments in secure software development and system hardening are accelerating. The growing complexity of mission systems makes cybersecurity a top priority, driving rapid market growth.

+357 96 030922
info@marketpublishers.com

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share, as countries like China, India, and Japan are investing heavily in aerospace infrastructure and defense modernization, increasing the need for robust cybersecurity solutions. Rapid expansion of commercial aviation, satellite programs, and smart airport initiatives further fuels demand. Government-backed R&D and strategic partnerships with global cybersecurity firms are enhancing regional capabilities. With rising cyber threats and technological adoption, Asia Pacific leads in securing its aerospace assets.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, owing to region benefits from strong defense budgets, advanced aerospace technologies, and a mature cybersecurity ecosystem. The U.S. leads in developing secure aerospace platforms, with major players investing in AI-driven threat detection, secure communications, and resilient infrastructure. Regulatory mandates and increasing cyberattacks on aviation systems are driving adoption. As digital transformation accelerates across military and commercial aerospace sectors, North America's cybersecurity investments are expected to grow rapidly.

Key players in the market

Some of the key players in Aerospace Cybersecurity Market include Thales Group, Raytheon Technologies Corporation, Lockheed Martin Corporation, Honeywell International Inc., Boeing, Airbus, Northrop Grumman Corporation, BAE Systems, Leonardo S.p.A., General Dynamics, L3Harris Technologies, Cisco Systems Inc., Rockwell Collins (part of Collins Aerospace), IBM and Palo Alto Networks.

Key Developments:

In October 2025, BAE Systems has partnered with Czech systems integrator PragoData to enhance Integrated Product Support (IPS) in the Czech defence sector. Initially, the collaboration will deliver asset-management tools including BAE's PropheSEA™ and Eurostep's ShareAspace, to boost readiness and lifecycle support of assets such as armoured vehicles.

In June 2025, Thales and KONGSBERG have inked a deal to form a 50/50 joint venture in Norway combining Thales' crypto & secure communications business with

+357 96 030922
info@marketpublishers.com

KONGSBERG’s secure communications and military radios. The venture aims to serve Norway, NATO, and international forces with interoperable, sovereign communications systems, targeting NOK 3 billion (~€254 million) revenues by end-of-decade.

Components Covered:

- Solutions
- Services

Security Types Covered:

- Network Security
- Wireless Security
- Application Security
- Cloud Security
- Endpoint Security

Deployment Types Covered:

- On-Premises
- Cloud-Based

Threat Types Covered:

- Malware and Ransomware
- Denial-of-Service (DoS) Attacks
- Phishing and Social Engineering

+357 96 030922
info@marketpublishers.com

- Advanced Persistent Threats (APT)
- Insider Threats
- Supply Chain Attacks

Applications Covered:

- Flight Operations
- Ground Systems
- Air Traffic Management
- Satellite Systems
- Avionics Systems
- Mission Systems
- Communication Systems

End Users Covered:

- Commercial Aviation
- Space Systems
- Military Aviation

Regions Covered:

- North America
  - US

+357 96 030922
info@marketpublishers.com

- Canada
- Mexico

Europe

- Germany
- UK
- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil

+357 96 030922
info@marketpublishers.com

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

+357 96 030922
info@marketpublishers.com

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

12 KEY DEVELOPMENTS

13 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Aerospace Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Type, Threat Type, Application, End User and By Geography

Product link: https://marketpublishers.com/r/A231B9293566EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/A231B9293566EN.html