

Aircraft Cybersecurity Market Forecasts to 2034 – Global Analysis By Security Type (Network Security, Wireless Security, Cloud Security, Application Security, and Endpoint Security), Solution, Platform, Application, End User and By Geography

<https://marketpublishers.com/r/A8396B4D0FB7EN.html>

Date: March 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: A8396B4D0FB7EN

Abstracts

According to Statistics MRC, the Global Aircraft Cybersecurity Market is accounted for \$11.3 billion in 2026 and is expected to reach \$29.4 billion by 2034, growing at a CAGR of 11.2% during the forecast period. Aircraft cybersecurity is the comprehensive protection of aircraft systems, onboard networks, and communication interfaces from cyber threats, unauthorized access, and malicious attacks. It encompasses the safeguarding of avionics, flight control systems, passenger connectivity, ground communication links, and maintenance data networks to ensure operational integrity, data confidentiality, and flight safety. With increasing aircraft digitization and connectivity, cybersecurity measures integrate advanced encryption, intrusion detection, continuous monitoring, and regulatory compliance to prevent system disruption, data breaches, and potential risks to aviation safety and reliability.

Market Dynamics:

Driver:

Increasing digitization and connectivity in aircraft

The modern aviation ecosystem is rapidly embracing digital technologies, with aircraft becoming increasingly connected through systems like in-flight Wi-Fi, electronic flight bags (EFBs), and real-time maintenance monitoring. This enhanced connectivity, while improving operational efficiency and passenger experience, significantly expands the

attack surface for potential cyber adversaries. Consequently, the imperative to secure these complex digital networks and protect sensitive flight data from unauthorized access and cyberattacks is a primary driver compelling airlines and OEMs to invest heavily in robust, multi-layered cybersecurity solutions.

Restraint:

High implementation and certification costs

The costs associated with developing, testing, and installing secure hardware and software are significant. Furthermore, the aviation industry is governed by stringent certification processes from bodies like the EASA and FAA. Any modification to aircraft systems, including cybersecurity upgrades, must undergo rigorous and expensive certification to ensure they do not compromise airworthiness. These high barriers to entry and the lengthy certification timelines can deter smaller operators and create a financial burden for all stakeholders, slowing the pace of widespread, advanced security adoption across the global fleet.

Opportunity:

Growing demand for securing unmanned aerial vehicles (UAVs)

Unlike manned aircraft, UAVs rely almost entirely on autonomous or remotely controlled operations via data links, making them uniquely susceptible to hijacking, GPS spoofing, and communication jamming. As UAV usage expands for package delivery, surveillance, and infrastructure inspection, the need for dedicated, lightweight cybersecurity solutions to protect command-and-control links and onboard data becomes critical. Developing tailored security protocols and hardware for this rapidly expanding segment offers a lucrative avenue for innovation and market expansion for cybersecurity providers.

Threat:

Evolving sophistication of cyber threats

Threats are evolving from simple malware to complex, multi-vector attacks targeting specific avionics software, supply chain vulnerabilities, and third-party service providers. The increasing use of artificial intelligence (AI) by attackers to automate and enhance their strategies means that defensive measures must be constantly updated, a process

that often lags behind. This dynamic and asymmetrical threat landscape makes it challenging for cybersecurity solutions to remain perpetually effective, posing a constant risk of undetected intrusions that could compromise flight safety.

Covid-19 Impact:

The COVID-19 pandemic had a mixed impact on the aircraft cybersecurity market. Initially, a steep decline in air travel led to reduced revenues for airlines, forcing them to delay capital expenditures, including some cybersecurity upgrades. However, the pandemic also accelerated digital transformation initiatives within the industry, such as contactless travel and increased reliance on data. This shift underscored the critical need for robust security protocols for remote access and passenger data, ultimately reinforcing the long-term importance of cybersecurity as a non-negotiable investment for operational resilience.

The software segment is expected to be the largest during the forecast period

The software segment is expected to account for the largest market share during the forecast period, driven by the critical need for advanced threat detection and identity management. Solutions like Security Information and Event Management (SIEM) and Identity and Access Management (IAM) are fundamental for monitoring complex avionics networks and controlling access to sensitive systems. The rising sophistication of cyber threats requires equally sophisticated software that uses AI and machine learning for anomaly detection.

The military aviation segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the military aviation segment is predicted to witness the highest growth rate, fueled by escalating geopolitical tensions and the modernization of defense platforms. Military aircraft, including fighter jets, transport aircraft, and especially unmanned aerial vehicles (UAVs), are prime targets for state-sponsored cyber espionage and electronic warfare. Defense departments globally are prioritizing the hardening of communication links, mission systems, and avionics suites against cyber intrusion.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest

market share, due to the presence of major aircraft OEMs like Boeing and a strong defense budget in the U.S. The region is home to leading cybersecurity innovators and benefits from stringent regulatory mandates from the FAA that enforce rigorous cybersecurity protocols. High adoption of connected aircraft technologies by major airlines and significant government funding for protecting military aviation assets from cyber warfare further solidify its dominance.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, driven by the rapid expansion of its commercial aviation fleet and increasing defense spending. Countries like China, India, and Japan are modernizing their air forces and investing in indigenous fighter and UAV programs, which require embedded cybersecurity. The surge in air passenger traffic is leading airlines to adopt more connected IFE systems, increasing their vulnerability and subsequent demand for security solutions.

Key players in the market

Some of the key players in Aircraft Cybersecurity Market include Honeywell International Inc., Collins Aerospace, Thales Group, Airbus S.A.S., Boeing Company, Lockheed Martin Corporation, Northrop Grumman Corporation, BAE Systems plc, Leonardo S.p.A., Elbit Systems Ltd., General Dynamics Corporation, Raytheon Technologies Corporation, Palo Alto Networks, Inc., Cisco Systems, Inc., and Fortinet, Inc.

Key Developments:

In February 2026, Honeywell announced that it has entered into an amended agreement to acquire Johnson Matthey's Catalyst Technologies business segment, which adjusts the total consideration from \$1.8 billion to \$1.325 billion and extends the long stop date to July 21, 2026. In the event that any of the regulatory approvals are not satisfied by the long stop date, the long stop date may be extended to August 21, 2026, if certain conditions are met.

In February 2026, Boeing and Air Cambodia announced the airline's largest single-aisle order for up to 20 737 MAX airplanes in an agreement unveiled at the Singapore Airshow. This marks the Southeast Asian carrier's first purchase of fuel-efficient Boeing airplanes. The airline finalized its firm order for 10 737-8 jets and opportunity for 10

more in December 2025. The order was previously unidentified on Boeing's Orders and Deliveries website.

Security Types Covered:

Network Security

Wireless Security

Cloud Security

Application Security

Endpoint Security

Solutions Covered:

Hardware

Software

Services

Platforms Covered:

Commercial Aviation

Military Aviation

General Aviation

Applications Covered:

Avionics Security

In-Flight Entertainment (IFE) and Connectivity Security

Airframe and Systems Security

Ground Systems Security

End Users Covered:

Original Equipment Manufacturers (OEMs)

Airlines and Operators

MRO Service Providers

Military and Defense

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of 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 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- 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)

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

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY SECURITY TYPE

- 5.1 Network Security
- 5.2 Wireless Security
- 5.3 Cloud Security
- 5.4 Application Security
- 5.5 Endpoint Security

6 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY SOLUTION

- 6.1 Hardware
 - 6.1.1 Firewalls
 - 6.1.2 Intrusion Detection/Prevention Systems (IDS/IPS)
 - 6.1.3 Encryption Devices
 - 6.1.4 Hardware Security Modules (HSMs)
- 6.2 Software
 - 6.2.1 Identity and Access Management (IAM)
 - 6.2.2 Antivirus/Anti-malware
 - 6.2.3 Data Loss Prevention (DLP)
 - 6.2.4 Security Information and Event Management (SIEM)
 - 6.2.5 Patch Management
- 6.3 Services
 - 6.3.1 Risk Assessment and Consulting
 - 6.3.2 Integration and Deployment
 - 6.3.3 Training and Education
 - 6.3.4 Support and Maintenance

7 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY PLATFORM

- 7.1 Commercial Aviation
 - 7.1.1 Narrow-Body Aircraft
 - 7.1.2 Wide-Body Aircraft
 - 7.1.3 Regional Aircraft
 - 7.1.4 Business Jets
- 7.2 Military Aviation

- 7.2.1 Fighter Aircraft
- 7.2.2 Transport Aircraft
- 7.2.3 Helicopters
- 7.2.4 Unmanned Aerial Vehicles (UAVs)
- 7.3 General Aviation

8 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY APPLICATION

- 8.1 Avionics Security
 - 8.1.1 Flight Management Systems (FMS)
 - 8.1.2 Communication Systems
 - 8.1.3 Navigation Systems
 - 8.1.4 Surveillance Systems
- 8.2 In-Flight Entertainment (IFE) and Connectivity Security
 - 8.2.1 Passenger Wi-Fi
 - 8.2.2 IFE Systems
 - 8.2.3 Cabin Management Systems
- 8.3 Airframe and Systems Security
 - 8.3.1 Control Systems
 - 8.3.2 Sensor Systems
- 8.4 Ground Systems Security
 - 8.4.1 Maintenance and Diagnostic Systems
 - 8.4.2 Data Loaders
 - 8.4.3 Ground Support Equipment

9 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY END USER

- 9.1 Original Equipment Manufacturers (OEMs)
- 9.2 Airlines and Operators
- 9.3 MRO Service Providers
- 9.4 Military and Defense

10 GLOBAL AIRCRAFT CYBERSECURITY MARKET, BY GEOGRAPHY

- 10.1 North America
 - 10.1.1 United States
 - 10.1.2 Canada
 - 10.1.3 Mexico
- 10.2 Europe

- 10.2.1 United Kingdom
- 10.2.2 Germany
- 10.2.3 France
- 10.2.4 Italy
- 10.2.5 Spain
- 10.2.6 Netherlands
- 10.2.7 Belgium
- 10.2.8 Sweden
- 10.2.9 Switzerland
- 10.2.10 Poland
- 10.2.11 Rest of Europe
- 10.3 Asia Pacific
 - 10.3.1 China
 - 10.3.2 Japan
 - 10.3.3 India
 - 10.3.4 South Korea
 - 10.3.5 Australia
 - 10.3.6 Indonesia
 - 10.3.7 Thailand
 - 10.3.8 Malaysia
 - 10.3.9 Singapore
 - 10.3.10 Vietnam
 - 10.3.11 Rest of Asia Pacific
- 10.4 South America
 - 10.4.1 Brazil
 - 10.4.2 Argentina
 - 10.4.3 Colombia
 - 10.4.4 Chile
 - 10.4.5 Peru
 - 10.4.6 Rest of South America
- 10.5 Rest of the World (RoW)
 - 10.5.1 Middle East
 - 10.5.1.1 Saudi Arabia
 - 10.5.1.2 United Arab Emirates
 - 10.5.1.3 Qatar
 - 10.5.1.4 Israel
 - 10.5.1.5 Rest of Middle East
 - 10.5.2 Africa
 - 10.5.2.1 South Africa

10.5.2.2 Egypt

10.5.2.3 Morocco

10.5.2.4 Rest of Africa

11 STRATEGIC MARKET INTELLIGENCE

11.1 Industry Value Network and Supply Chain Assessment

11.2 White-Space and Opportunity Mapping

11.3 Product Evolution and Market Life Cycle Analysis

11.4 Channel, Distributor, and Go-to-Market Assessment

12 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

12.1 Mergers and Acquisitions

12.2 Partnerships, Alliances, and Joint Ventures

12.3 New Product Launches and Certifications

12.4 Capacity Expansion and Investments

12.5 Other Strategic Initiatives

13 COMPANY PROFILES

13.1 Honeywell International Inc.

13.2 Collins Aerospace (RTX)

13.3 Thales Group

13.4 Airbus S.A.S.

13.5 Boeing Company

13.6 Lockheed Martin Corporation

13.7 Northrop Grumman Corporation

13.8 BAE Systems plc

13.9 Leonardo S.p.A.

13.10 Elbit Systems Ltd.

13.11 General Dynamics Corporation

13.12 Raytheon Technologies Corporation

13.13 Palo Alto Networks, Inc.

13.14 Cisco Systems, Inc.

13.15 Fortinet, Inc.

List Of Tables

LIST OF TABLES

Table 1 Global Aircraft Cybersecurity Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Aircraft Cybersecurity Market Outlook, By Security Type (2023-2034) (\$MN)

Table 3 Global Aircraft Cybersecurity Market Outlook, By Network Security (2023-2034) (\$MN)

Table 4 Global Aircraft Cybersecurity Market Outlook, By Wireless Security (2023-2034) (\$MN)

Table 5 Global Aircraft Cybersecurity Market Outlook, By Cloud Security (2023-2034) (\$MN)

Table 6 Global Aircraft Cybersecurity Market Outlook, By Application Security (2023-2034) (\$MN)

Table 7 Global Aircraft Cybersecurity Market Outlook, By Endpoint Security (2023-2034) (\$MN)

Table 8 Global Aircraft Cybersecurity Market Outlook, By Solution (2023-2034) (\$MN)

Table 9 Global Aircraft Cybersecurity Market Outlook, By Hardware (2023-2034) (\$MN)

Table 10 Global Aircraft Cybersecurity Market Outlook, By Firewalls (2023-2034) (\$MN)

Table 11 Global Aircraft Cybersecurity Market Outlook, By Intrusion Detection/Prevention Systems (IDS/IPS) (2023-2034) (\$MN)

Table 12 Global Aircraft Cybersecurity Market Outlook, By Encryption Devices (2023-2034) (\$MN)

Table 13 Global Aircraft Cybersecurity Market Outlook, By Hardware Security Modules (HSMs) (2023-2034) (\$MN)

Table 14 Global Aircraft Cybersecurity Market Outlook, By Software (2023-2034) (\$MN)

Table 15 Global Aircraft Cybersecurity Market Outlook, By Identity and Access Management (IAM) (2023-2034) (\$MN)

Table 16 Global Aircraft Cybersecurity Market Outlook, By Antivirus/Anti-malware (2023-2034) (\$MN)

Table 17 Global Aircraft Cybersecurity Market Outlook, By Data Loss Prevention (DLP) (2023-2034) (\$MN)

Table 18 Global Aircraft Cybersecurity Market Outlook, By Security Information and Event Management (SIEM) (2023-2034) (\$MN)

Table 19 Global Aircraft Cybersecurity Market Outlook, By Patch Management (2023-2034) (\$MN)

Table 20 Global Aircraft Cybersecurity Market Outlook, By Services (2023-2034) (\$MN)

Table 21 Global Aircraft Cybersecurity Market Outlook, By Risk Assessment and

Consulting (2023-2034) (\$MN)

Table 22 Global Aircraft Cybersecurity Market Outlook, By Integration and Deployment (2023-2034) (\$MN)

Table 23 Global Aircraft Cybersecurity Market Outlook, By Training and Education (2023-2034) (\$MN)

Table 24 Global Aircraft Cybersecurity Market Outlook, By Support and Maintenance (2023-2034) (\$MN)

Table 25 Global Aircraft Cybersecurity Market Outlook, By Platform (2023-2034) (\$MN)

Table 26 Global Aircraft Cybersecurity Market Outlook, By Commercial Aviation (2023-2034) (\$MN)

Table 27 Global Aircraft Cybersecurity Market Outlook, By Narrow-Body Aircraft (2023-2034) (\$MN)

Table 28 Global Aircraft Cybersecurity Market Outlook, By Wide-Body Aircraft (2023-2034) (\$MN)

Table 29 Global Aircraft Cybersecurity Market Outlook, By Regional Aircraft (2023-2034) (\$MN)

Table 30 Global Aircraft Cybersecurity Market Outlook, By Business Jets (2023-2034) (\$MN)

Table 31 Global Aircraft Cybersecurity Market Outlook, By Military Aviation (2023-2034) (\$MN)

Table 32 Global Aircraft Cybersecurity Market Outlook, By Fighter Aircraft (2023-2034) (\$MN)

Table 33 Global Aircraft Cybersecurity Market Outlook, By Transport Aircraft (2023-2034) (\$MN)

Table 34 Global Aircraft Cybersecurity Market Outlook, By Helicopters (2023-2034) (\$MN)

Table 35 Global Aircraft Cybersecurity Market Outlook, By Unmanned Aerial Vehicles (UAVs) (2023-2034) (\$MN)

Table 36 Global Aircraft Cybersecurity Market Outlook, By General Aviation (2023-2034) (\$MN)

Table 37 Global Aircraft Cybersecurity Market Outlook, By Application (2023-2034) (\$MN)

Table 38 Global Aircraft Cybersecurity Market Outlook, By Avionics Security (2023-2034) (\$MN)

Table 39 Global Aircraft Cybersecurity Market Outlook, By Flight Management Systems (FMS) (2023-2034) (\$MN)

Table 40 Global Aircraft Cybersecurity Market Outlook, By Communication Systems (2023-2034) (\$MN)

Table 41 Global Aircraft Cybersecurity Market Outlook, By Navigation Systems

(2023-2034) (\$MN)

Table 42 Global Aircraft Cybersecurity Market Outlook, By Surveillance Systems

(2023-2034) (\$MN)

Table 43 Global Aircraft Cybersecurity Market Outlook, By In-Flight Entertainment (IFE) and Connectivity Security (2023-2034) (\$MN)

Table 44 Global Aircraft Cybersecurity Market Outlook, By Passenger Wi-Fi

(2023-2034) (\$MN)

Table 45 Global Aircraft Cybersecurity Market Outlook, By IFE Systems (2023-2034) (\$MN)

Table 46 Global Aircraft Cybersecurity Market Outlook, By Cabin Management Systems (2023-2034) (\$MN)

Table 47 Global Aircraft Cybersecurity Market Outlook, By Airframe and Systems Security (2023-2034) (\$MN)

Table 48 Global Aircraft Cybersecurity Market Outlook, By Control Systems (2023-2034) (\$MN)

Table 49 Global Aircraft Cybersecurity Market Outlook, By Sensor Systems (2023-2034) (\$MN)

Table 50 Global Aircraft Cybersecurity Market Outlook, By Ground Systems Security (2023-2034) (\$MN)

Table 51 Global Aircraft Cybersecurity Market Outlook, By Maintenance and Diagnostic Systems (2023-2034) (\$MN)

Table 52 Global Aircraft Cybersecurity Market Outlook, By Data Loaders (2023-2034) (\$MN)

Table 53 Global Aircraft Cybersecurity Market Outlook, By Ground Support Equipment (2023-2034) (\$MN)

Table 54 Global Aircraft Cybersecurity Market Outlook, By End User (2023-2034) (\$MN)

Table 55 Global Aircraft Cybersecurity Market Outlook, By Original Equipment Manufacturers (OEMs) (2023-2034) (\$MN)

Table 56 Global Aircraft Cybersecurity Market Outlook, By Airlines and Operators (2023-2034) (\$MN)

Table 57 Global Aircraft Cybersecurity Market Outlook, By MRO Service Providers (2023-2034) (\$MN)

Table 58 Global Aircraft Cybersecurity Market Outlook, By Military and Defense (2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

I would like to order

Product name: Aircraft Cybersecurity Market Forecasts to 2034 – Global Analysis By Security Type (Network Security, Wireless Security, Cloud Security, Application Security, and Endpoint Security), Solution, Platform, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/A8396B4D0FB7EN.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/A8396B4D0FB7EN.html>