

Aerospace Cybersecurity Solutions Market Forecasts to 2034 - Global Analysis By Solution Type (Network Security, Endpoint Security, Application Security, Cloud Security, Data Security, Identity & Access Management (IAM) and Security Information & Event Management (SIEM)), Deployment Mode, Security Offering, Application, End User and By Geography

<https://marketpublishers.com/r/A70217967C98EN.html>

Date: September 2026

Pages: 200

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

ID: A70217967C98EN

Abstracts

According to Statistics MRC, the Global Aerospace Cybersecurity Solutions Market is accounted for \$12.8 billion in 2026 and is expected to reach \$23.5 billion by 2034 growing at a CAGR of 7.9% during the forecast period. Aerospace Cybersecurity Solutions are designed to secure aircraft, spacecraft, satellites, ground infrastructure, communication platforms, and aviation networks against increasingly sophisticated cyber risks. They incorporate technologies such as continuous monitoring, threat detection, intelligence platforms, access controls, encryption, and incident management to identify and address security vulnerabilities. These solutions help prevent unauthorized system access, malicious software, ransomware, information theft, and operational disruptions. With aerospace systems becoming more interconnected and digitally controlled, cybersecurity plays an important role in preserving system integrity, safeguarding sensitive information, supporting compliance, and improving resilience across aviation, defense, and space environments.

According to EASA, airports accounted for more than 50% of recorded targeted cyberattacks against aviation in late 2024, highlighting the growing requirement for cybersecurity protection across aviation infrastructure.

Market Dynamics:

Driver:

Rising frequency and sophistication of cyber threats

Growing cyber risks and increasingly advanced attack methods are creating strong demand for cybersecurity solutions across the aerospace industry. Aerospace companies manage highly sensitive technical, operational, commercial, and defense information, making their digital infrastructure attractive targets for cybercriminals and state-backed attackers. Ransomware, malware, credential theft, unauthorized access, information breaches, and supply-chain compromises can create significant operational and financial consequences. To address these risks, aerospace organizations are adopting stronger security measures, including continuous threat monitoring, endpoint security, encryption, access management, network protection, and incident response capabilities.

Restraint:

High cost of implementing advanced cybersecurity solutions

Significant implementation expenses can restrict the adoption of cybersecurity technologies within the aerospace industry. Advanced protection requires investments in specialized security platforms, monitoring systems, encryption capabilities, threat intelligence tools, and skilled cybersecurity professionals. Integrating these technologies into existing aircraft, avionics, communication infrastructure, satellite systems, and ground networks can further increase project costs and complexity. Smaller airlines, aerospace contractors, and newer space businesses may struggle to dedicate adequate financial resources to comprehensive cybersecurity initiatives. Furthermore, ongoing maintenance, system updates, vulnerability assessments, compliance requirements, and workforce training generate continuing expenditures.

Opportunity:

Expansion of connected and autonomous aerospace systems

Increasing adoption of connected and autonomous technologies across aerospace applications offers substantial growth opportunities for cyber security providers. Aircraft, drones, satellites, and space vehicles are incorporating networked sensors, artificial intelligence, cloud infrastructure, and automated decision-making capabilities to enhance performance and operational efficiency. However, greater connectivity also increases exposure to cyber attacks involving communications, navigation, onboard systems, control networks, and sensitive data. Companies can leverage this opportunity by introducing integrated protection, real-time monitoring, secure communications, and advanced threat detection technologies.

Threat:

Rapidly evolving cyberattack techniques

The continuous advancement of cyberattack methods poses a major challenge to the aerospace cybersecurity industry. Malicious actors, including organized cybercriminals and state-supported groups, are constantly developing new techniques to target aircraft technologies, satellite platforms, communications networks, and interconnected supply chains. Artificial intelligence-assisted attacks, sophisticated malware, ransomware, automated intrusion methods, and social engineering can bypass traditional protective measures. Aerospace organizations therefore need frequent security enhancements, continuous monitoring, and updated threat intelligence to respond effectively to changing risks. Maintaining protection against rapidly evolving attacks can increase technological complexity and expenses.

Covid-19 Impact:

COVID-19 produced both negative and positive effects on the Aerospace Cyber security Solutions Market. Reduced aviation activity and financial pressures caused some aerospace organizations to postpone technology investments and cyber security upgrades while prioritizing immediate operational needs. At the same time, increased remote work, digital collaboration, and dependence on interconnected technologies expanded the potential exposure to cyber risks. As organizations gradually recovered and accelerated digital transformation, cybersecurity gained greater importance for protecting remote access, communications, operational systems, sensitive information, and connected aerospace infrastructure.

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 because aerospace organizations rely extensively on interconnected systems for communication, operations, control, and information exchange. These solutions safeguard aircraft networks, satellite links, aviation infrastructure, ground-based platforms, and connected operational environments against unauthorized access and cyber threats. Key capabilities include network monitoring, firewalls, intrusion detection, secure gateways, segmentation, and protective access controls. The increasing digitalization and connectivity of aerospace systems are expanding the importance of securing communication channels and network infrastructure.

The aerospace OEMs & suppliers segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the aerospace OEMs & suppliers segment is predicted to witness the highest growth rate, positioned for rapid growth as aerospace

manufacturers and component providers expand their use of digital engineering, automated production, connected systems, cloud platforms, and digitally managed supply chains. Greater dependence on these technologies increases the requirement to safeguard proprietary designs, manufacturing environments, technical information, and interconnected supplier networks. Cybersecurity has become increasingly important for protecting intellectual property and maintaining secure collaboration across geographically distributed aerospace ecosystems.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by its well-established aviation, aerospace, defense, and space sectors. The region hosts numerous prominent aircraft manufacturers, defense organizations, airlines, technology providers, and space companies, creating strong requirements for sophisticated digital protection. Rising connectivity among aircraft, satellites, communication platforms, and ground infrastructure is increasing cybersecurity needs across the aerospace ecosystem. In addition, government security programs, regulatory requirements, defense modernization initiatives, and investments in protecting mission-critical infrastructure are encouraging cybersecurity adoption.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, as regional aviation, defense, and space industries continue expanding. Major countries, including China, India, Japan, and South Korea, are investing in aircraft modernization, airport development, satellite infrastructure, and advanced aerospace technologies. Increasing adoption of connected and digital systems is raising the need to secure avionics, communications, satellites, and ground-based platforms. At the same time, rising cyber risks and stronger government initiatives focused on digital protection are encouraging aerospace companies and agencies to implement sophisticated cybersecurity technologies throughout the region.

Key players in the market

Some of the key players in Aerospace Cybersecurity Solutions Market include Thales Group, Lockheed Martin, BAE Systems, Airbus, Honeywell, Northrop Grumman, Leonardo, General Dynamics Information Technology (GDIT), Boeing, Raytheon Technologies (RTX), Leidos, DXC Technology, IBM, Cisco Systems, Rheinmetall, Hanwha Systems, Booz Allen and Palo Alto Networks.

Key Developments:

In February 2026, BAE Systems Launchpad is a new technology incubator programme

designed to take dual-use technologies beyond the defence sector and help cutting-edge innovations reach their full commercial potential. Launchpad directly addresses the challenge of moving defence technologies beyond prototype development by spinning them out into independent start-up businesses.

In December 2025, Honeywell International Inc. has been awarded a \$58.79 million contract modification from the U.S. Department of War for work related to the automotive gas turbine 1500 engine platform. The modification, identified as P00026 to contract W56HZV-20-D-0062, is for program services and systems technical support engineering services. This latest award increases the total cumulative value of the contract to \$2.69 billion.

In June 2025, Thales and Qatar Airways have signed a Memorandum of Agreement (MoA) to support Qatar Airways' strategic fleet growth plan announced last month. This agreement sets the course for future inflight entertainment (IFE) innovations to support Qatar Airways' digital transformation journey, giving the airline access to the most innovative technologies.

Solution Types Covered:

Network Security

Endpoint Security

Application Security

Cloud Security

Data Security

Identity & Access Management (IAM)

Security Information & Event Management (SIEM)

Deployment Modes Covered:

On-Premises

Cloud-Based

Hybrid

Security Offerings Covered:

Hardware

Software

Services

Applications Covered:

Aircraft Systems

Ground Control Systems

Satellite & Space Systems

Air Traffic Management Systems

Maintenance, Repair & Operations (MRO) Systems

End Users Covered:

Commercial Aviation

Military & Defense Aviation

Space Agencies

Aerospace OEMs & Suppliers

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 AEROSPACE CYBERSECURITY SOLUTIONS MARKET, BY SOLUTION TYPE

- 5.1 Network Security
- 5.2 Endpoint Security
- 5.3 Application Security
- 5.4 Cloud Security
- 5.5 Data Security
- 5.6 Identity & Access Management (IAM)
- 5.7 Security Information & Event Management (SIEM)

6 GLOBAL AEROSPACE CYBERSECURITY SOLUTIONS MARKET, BY DEPLOYMENT MODE

- 6.1 On-Premises
- 6.2 Cloud-Based
- 6.3 Hybrid

7 GLOBAL AEROSPACE CYBERSECURITY SOLUTIONS MARKET, BY SECURITY OFFERING

- 7.1 Hardware
- 7.2 Software
- 7.3 Services
 - 7.3.1 Managed Security Services
 - 7.3.2 Professional Services

8 GLOBAL AEROSPACE CYBERSECURITY SOLUTIONS MARKET, BY APPLICATION

- 8.1 Aircraft Systems
- 8.2 Ground Control Systems
- 8.3 Satellite & Space Systems
- 8.4 Air Traffic Management Systems
- 8.5 Maintenance, Repair & Operations (MRO) Systems

9 GLOBAL AEROSPACE CYBERSECURITY SOLUTIONS MARKET, BY END USER

- 9.1 Commercial Aviation
- 9.2 Military & Defense Aviation
- 9.3 Space Agencies
- 9.4 Aerospace OEMs & Suppliers

10 GLOBAL AEROSPACE CYBERSECURITY SOLUTIONS 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 Thales Group

13.2 Lockheed Martin

- 13.3 BAE Systems
- 13.4 Airbus
- 13.5 Honeywell
- 13.6 Northrop Grumman
- 13.7 Leonardo
- 13.8 General Dynamics Information Technology (GDIT)
- 13.9 Boeing
- 13.10 Raytheon Technologies (RTX)
- 13.11 Leidos
- 13.12 DXC Technology
- 13.13 IBM
- 13.14 Cisco Systems
- 13.15 Rheinmetall
- 13.16 Hanwha Systems
- 13.17 Booz Allen
- 13.18 Palo Alto Networks

List Of Tables

LIST OF TABLES

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

Table 2 Global Aerospace Cybersecurity Solutions Market Outlook, By Solution Type (2023-2034) (\$MN)

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

Table 4 Global Aerospace Cybersecurity Solutions Market Outlook, By Endpoint Security (2023-2034) (\$MN)

Table 5 Global Aerospace Cybersecurity Solutions Market Outlook, By Application Security (2023-2034) (\$MN)

Table 6 Global Aerospace Cybersecurity Solutions Market Outlook, By Cloud Security (2023-2034) (\$MN)

Table 7 Global Aerospace Cybersecurity Solutions Market Outlook, By Data Security (2023-2034) (\$MN)

Table 8 Global Aerospace Cybersecurity Solutions Market Outlook, By Identity & Access Management (IAM) (2023-2034) (\$MN)

Table 9 Global Aerospace Cybersecurity Solutions Market Outlook, By Security Information & Event Management (SIEM) (2023-2034) (\$MN)

Table 10 Global Aerospace Cybersecurity Solutions Market Outlook, By Deployment Mode (2023-2034) (\$MN)

Table 11 Global Aerospace Cybersecurity Solutions Market Outlook, By On-Premises (2023-2034) (\$MN)

Table 12 Global Aerospace Cybersecurity Solutions Market Outlook, By Cloud-Based (2023-2034) (\$MN)

Table 13 Global Aerospace Cybersecurity Solutions Market Outlook, By Hybrid (2023-2034) (\$MN)

Table 14 Global Aerospace Cybersecurity Solutions Market Outlook, By Security Offering (2023-2034) (\$MN)

Table 15 Global Aerospace Cybersecurity Solutions Market Outlook, By Hardware (2023-2034) (\$MN)

Table 16 Global Aerospace Cybersecurity Solutions Market Outlook, By Software (2023-2034) (\$MN)

Table 17 Global Aerospace Cybersecurity Solutions Market Outlook, By Services (2023-2034) (\$MN)

Table 18 Global Aerospace Cybersecurity Solutions Market Outlook, By Managed

Security Services (2023-2034) (\$MN)

Table 19 Global Aerospace Cybersecurity Solutions Market Outlook, By Professional Services (2023-2034) (\$MN)

Table 20 Global Aerospace Cybersecurity Solutions Market Outlook, By Application (2023-2034) (\$MN)

Table 21 Global Aerospace Cybersecurity Solutions Market Outlook, By Aircraft Systems (2023-2034) (\$MN)

Table 22 Global Aerospace Cybersecurity Solutions Market Outlook, By Ground Control Systems (2023-2034) (\$MN)

Table 23 Global Aerospace Cybersecurity Solutions Market Outlook, By Satellite & Space Systems (2023-2034) (\$MN)

Table 24 Global Aerospace Cybersecurity Solutions Market Outlook, By Air Traffic Management Systems (2023-2034) (\$MN)

Table 25 Global Aerospace Cybersecurity Solutions Market Outlook, By Maintenance, Repair & Operations (MRO) Systems (2023-2034) (\$MN)

Table 26 Global Aerospace Cybersecurity Solutions Market Outlook, By End User (2023-2034) (\$MN)

Table 27 Global Aerospace Cybersecurity Solutions Market Outlook, By Commercial Aviation (2023-2034) (\$MN)

Table 28 Global Aerospace Cybersecurity Solutions Market Outlook, By Military & Defense Aviation (2023-2034) (\$MN)

Table 29 Global Aerospace Cybersecurity Solutions Market Outlook, By Space Agencies (2023-2034) (\$MN)

Table 30 Global Aerospace Cybersecurity Solutions Market Outlook, By Aerospace OEMs & Suppliers (2023-2034) (\$MN)

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

I would like to order

Product name: Aerospace Cybersecurity Solutions Market Forecasts to 2034 - Global Analysis By Solution Type (Network Security, Endpoint Security, Application Security, Cloud Security, Data Security, Identity & Access Management (IAM) and Security Information & Event Management (SIEM)), Deployment Mode, Security Offering, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/A70217967C98EN.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/A70217967C98EN.html>