

Defense Cyber Security Market is Booming with a 7.7% CAGR, Projected Reach \$43.4 Bn by 2031

The network security solutions segment dominated the global Defense Cyber Security market in terms of growth rate during the forecast period.

WILMINGTON, DE, UNITED STATES, March 4, 2025 /EINPresswire.com/ -- According to a new report published by Allied Market Research, titled, "[Defense Cyber Security Market](#) Size, Share, Competitive Landscape and Trend Analysis Report, by Type, by Deployment, by Solution, by

Application : Global Opportunity Analysis and Industry Forecast, 2021-2031" The research provides a current evaluation of the global market landscape, highlighting recent trends, key drivers, and the overall market environment. The study examines the main factors influencing industry expansion, analyzing both its growth drivers and restraints. Additionally, it sheds light on factors expected to offer promising opportunities for development of industry in the future.

“

The cloud segment dominated the global defense cyber security market in terms of growth rate during the forecast period.”

Roshan Deshmukh

Download Sample Report:

<https://www.alliedmarketresearch.com/request-sample/A09727>

A growing risk of cyber threat to critical infrastructures by structured criminal groups, technological improvement in the cyber security industry, increase in demand for

defense IT expenditure, transition of conventional military aircrafts into autonomous aircrafts, and increased dependency of military organizations on the internet drive the [growth of the global defense cyber security market](#). However, limited awareness related to cyber security and lack of cyber security professionals or workforce hamper the global market growth. On the other hand, increase in threats and warnings related to cyber-attack on officials and adoption of IoT in



cyber security technology present new growth opportunities for the global market in the coming years.

The concept of defense cyber security is typically attributed to a series of security protocols and controls that are layered throughout an IT network to preserve the integrity and privacy of defense organizations. Every organization has vulnerabilities that an attacker can exploit to gain access and cause damage. Hence, the in depth strategy of defense cyber security is to protect against a wide range of threats and close all of an organization's security holes in order to protect it effectively against cyber threats.

In addition, the defense cyber security market has witnessed significant growth in recent years, owing to the increased dependency of military organizations on the internet network, growing advancements in information technology, and increasing government initiatives to secure critical data. For instance, in March 2021, the government announced its plans regarding National Cyber Force and set up a Cyber Corridor in north of England. This is expected to set out the importance of cyber security to the country's defense, extending from cyber enhanced battlefield capabilities for the armed forces to internet security for household users.

The factors such as increase in demand for defense IT expenditure, transition, of conventional military aircraft into autonomous aircraft, and growth in cyber-attacks on the regulatory, trade and individuals supplement the growth of the defense cyber security market. However, limited awareness related to cyber security and lack of cyber security professionals or workforce are the factors expected to hamper the growth of the defense cyber security market. In addition, increasing threats and warnings related to cyber-attack on officials and adoption of IoT in cyber security technology creates market opportunities for the key players operating in the defense cyber security market.

The defense cyber security market is segmented into application, type, deployment, solution and region. By type, the market is divided into endpoint security solutions, network security solutions, and content security solutions. By deployment, the market is fragmented into on-premise and cloud. By solution, it is categorized into threat intelligence & response management, identity & access management, data loss prevention management, security & vulnerability management, unified threat management, enterprise risk & compliance, managed security, and others. By application, the market is classified into military, public utilities, communication networks, and others. By region, it is analyzed across North America, Europe, Asia-Pacific, and LAMEA.

Buy This Research Report: <https://www.alliedmarketresearch.com/checkout-final/344d952cc1257f3c46714c38ee03a7f9>

Based on application, the military segment was the largest market in 2021, contributing to more than one-third of the global defense cyber security market share, and is expected to maintain its leadership status during the forecast period. This is due to the growing frequency and

sophistication of cyber-attacks due to the increasing dependency of military organizations on the internet network. To counter all these vulnerabilities, there is a major focus on adopting cyber security solutions in the defense sector. On the other hand, the communication networks segment is projected to witness the fastest CAGR of 9.0% from 2022 to 2031. This is due to the fact that different sectors adopt more technologies to improve their communications and infrastructure, and there is a parallel rise in cyber threats to these networks.

Based on type, the endpoint security segment held the largest market share of more than two-fifths of the global defense cyber security market in 2021 and is expected to maintain its dominance during the forecast period. This is due to the fact that endpoint security solutions are one of the most important assets of the defense sector. The high penetration of the segment is attributed to the increasing use of automation and behavioral analysis for threat detection, growing amount of data across verticals, and rising investments by key players. On the other hand, the network security solutions segment is projected to witness the largest CAGR of 8.5% from 2022 to 2031. This is due to the rise in frequency and sophistication of cyber-attacks owing to the increasing dependency of military organizations on the internet network. To counter all these vulnerabilities, there is a major focus on adopting network security solutions in the defense sector.

Based on region, North America was the largest market in 2021, capturing nearly one-third of the global defense cyber security market share, owing to increasing investment in cyber security services by many companies in the region. However, Asia-Pacific is expected to lead in terms of revenue and manifest the fastest CAGR of 9.2% during the forecast period. This is due to the high rate of modernization of police force, increased annual budgetary spending on homeland security, and rise in instances of terrorist activities in the region.

The leading players operating in the defense cyber security market are AT&T, BAE Systems, Boeing, Cisco Systems, Inc., DXC Technology Company, EclecticIQ B.V., IBM Corporation, Intel Corporation, Lockheed Martin Corporation, Northrop Grumman Corporation, Privacera, Inc., Raytheon Technologies Corporation, SentinelOne, Secureworks, Inc., and Thales Group.

Key Benefits For Stakeholders:

- This study presents analytical depiction of the global defense cyber security market analysis along with current trends and future estimations to depict imminent investment pockets.
- The overall defense cyber security market opportunity is determined by understanding profitable trends to gain a stronger foothold.
- The report presents information related to the key drivers, restraints, and opportunities of the global defense cyber security market with a detailed impact analysis.
- The current defense cyber security market is quantitatively analyzed from 2022 to 2031 to benchmark the financial competency.
- Porter's five forces analysis illustrates the potency of the buyers and suppliers in the industry.

Enquiry About Report: <https://www.alliedmarketresearch.com/purchase-enquiry/A09727>

Frequently Asked Questions:

- What is the defense cyber security market?
- Why is cyber security important in defense?
- What are the key components of the defense cyber security market?
- What are the main drivers of the defense cyber security market?
- What challenges does the defense cyber security market face?
- Which regions lead the defense cyber security market in 2025?
- What technologies are driving the defense cyber security market?
- Who are the key players in the defense cyber security market?

Explore AMR's Extensive ongoing Coverage on Aerospace and Defense Domain:

□ Space Launch Services Market Opportunity Analysis and Industry Forecast, 2023-2032
<https://www.alliedmarketresearch.com/space-launch-services-market>

□ Small Arms Market Opportunity Analysis and Industry Forecast, 2023-2032
<https://www.alliedmarketresearch.com/small-arms-market>

□ Aviation Blockchain Market Opportunity Analysis and Industry Forecast, 2021-2030
<https://www.alliedmarketresearch.com/aviation-blockchain-market-A06275>

□ Air Defense Systems Market Opportunity Analysis and Industry Forecast, 2021-2031
<https://www.alliedmarketresearch.com/air-defense-systems-market-A07789>

□ Defense Cyber Security Market Opportunity Analysis and Industry Forecast, 2021-2031
<https://www.alliedmarketresearch.com/defense-cyber-security-market-A09727>

□ Space Robotics Market Opportunity Analysis and Industry Forecast, 2021-2031
<https://www.alliedmarketresearch.com/space-robotics-market-A07165>

□ Satellite Manufacturing Market Opportunity Analysis and Industry Forecast, 2021-2031
<https://www.alliedmarketresearch.com/satellite-manufacturing-market-A13678>

□ Drone Software Market Opportunity Analysis and Industry Forecast, 2021-2031
<https://www.alliedmarketresearch.com/drone-software-market-A09617>

David Correa

Allied Market Research

+ 1 800-792-5285

[email us here](#)

Visit us on social media:

[Facebook](#)

[X](#)

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/791035382>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.