

Defense Cyber Security Market in Defense Industry Anticipated to Surge to \$43.4 Billion by 2031

OREGAON, PORTLAND, UNITED STATES , January 12, 2024

/EINPresswire.com/ -- Allied Market Research published a report, titled,

"[Defense Cyber Security Market](#) by Type (Endpoint Security Solutions, Network Security Solutions, Content Security Solutions), by Deployment (On-Premises, Cloud), by Solution (Threat intelligence and Response Management, Identity and Access Management, Data Loss Prevention Management, Security and Vulnerability Management, Unified Threat Management, Enterprise Risk and Compliance, Managed Security, Others), by Application (Military, Public Utilities, Communication Networks, Others): Global Opportunity Analysis and Industry Forecast, 2022-2031."

According to the report, the global defense cyber security industry generated \$21.3 billion in 2021, and is estimated to reach \$43.4 billion by 2031, witnessing a CAGR of 7.7% from 2022 to 2031. The report offers a detailed analysis of changing market trends, top segments, key investment pockets, value chain, regional landscape, and competitive scenario.



Defense Cyber Security Market Trend

Request a sample report - <https://www.alliedmarketresearch.com/request-sample/10092>

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.

For more information, contact: info@alliedmarketresearch.com

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.

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 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.

For more information on the defense cyber security market, visit <https://www.alliedmarketresearch.com/defense-cyber-security-market/purchase-options>

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 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.

For more information on the defense cyber security market, visit <https://www.alliedmarketresearch.com/defense-cyber-security-market/purchase-options>

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.

For more information, please contact: <https://www.alliedmarketresearch.com/purchase-enquiry/10092>

For more information, please contact:

Intel Corporation
AT&T Inc.
Northrop Grumman
IBM Corporation
Lockheed Martin Corporation
BAE Systems plc
Thales
Eclectiq B.V.
SentinelOne
Boeing
DXC Technology Company
Cisco Systems, Inc.
Raytheon Technologies Corporation
Secureworks, Inc.
Privacera, Inc.

David Correa
Allied Market Research
+1 800-792-5285
[email us here](#)
Visit us on social media:
[Facebook](#)
[Twitter](#)
[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/680855885>

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.

