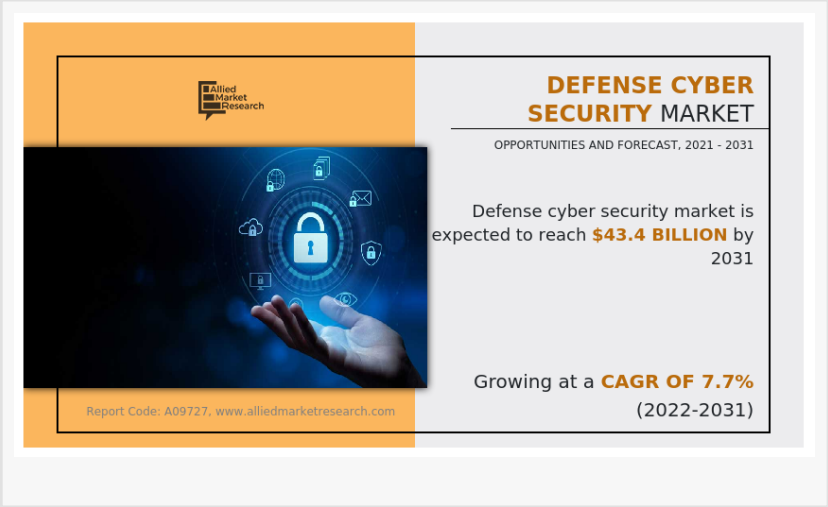
Defense Cyber Security Market to Grow at CAGR of 7.7% to Reach US$ 43.4 Billion by 2031

global defense cyber security industry is estimated to reach US$ 43.4 billion by 2031, witnessing a CAGR of 7.7% during the forecast period.



PORTLAND, OREGON, UNITED STATES, November 22, 2023 / 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 US$ 21.3 billion in 2021, and is estimated to reach US$ 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.

Get inside scoop of the report, request sample - https://www.alliedmarketresearch.com/request-sample/10092

Here are some key applications of defense cybersecurity:

Protection of National Security Information:
Defense cybersecurity is essential for safeguarding classified and sensitive information related to national security. This includes military plans, intelligence data, and other critical information that, if compromised, could pose a significant threat to a country's defense capabilities.

Critical Infrastructure Protection:
Many critical infrastructures, such as power grids, communication networks, and transportation systems, rely on digital systems. Defense cybersecurity helps prevent cyber attacks that could disrupt these critical infrastructures, ensuring the continued functionality of essential services.

Military Operations Security (OPSEC):
Cybersecurity is integrated into military operations to protect the confidentiality, integrity, and availability of information. This includes securing communication channels, ensuring the integrity of command and control systems, and preventing unauthorized access to military networks.

Defense Against Cyber Espionage:
Nation-states and other adversaries may engage in cyber espionage to gather intelligence on a country's defense capabilities. Defense cybersecurity is crucial for detecting and preventing cyber espionage activities, including unauthorized access to military databases and systems.

Prevention of Cyber Attacks on Weapon Systems:
Modern military systems, including weapons and communication systems, are increasingly reliant on digital technologies. Defense cybersecurity is necessary to prevent cyber attacks that could compromise the functionality and effectiveness of these systems.

Ensuring the Integrity of Defense Supply Chains:
Defense organizations often source components and technologies from various suppliers. Cybersecurity measures are needed to ensure the integrity of the supply chain, preventing the insertion of malicious hardware or software that could compromise the security of defense systems.

Deterrence and Cyber Warfare:
A robust defense cybersecurity posture can serve as a deterrent against cyber attacks. Nations with strong cybersecurity capabilities are less likely to be targeted, as potential adversaries are aware of the challenges they would face in penetrating and disrupting their systems.

Incident Response and Recovery:
In the event of a cyber attack, defense cybersecurity includes effective incident response and recovery plans. This involves identifying and mitigating the impact of the attack, restoring systems to normal operation, and learning from the incident to improve future cybersecurity measures.

Collaboration with Allies:
International cooperation is essential in addressing cyber threats that transcend national borders. Defense cybersecurity efforts involve collaborating with allies to share threat intelligence, coordinate responses to cyber incidents, and collectively strengthen global cybersecurity.

Continuous Adaptation and Innovation:
Defense cybersecurity is an ever-evolving field, as cyber threats constantly evolve. It requires continuous adaptation, innovation, and investment in research and development to stay ahead of emerging cyber threats and technologies.

Drivers, Restraints, and Opportunities

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.

Covid-19 Scenario

The outbreak of the COVID-19 pandemic rendered the military sectors in some nations to meet with shortfalls of the looming budget.
Nevertheless, various governments worldwide adopted cyber security automation solutions for their military applications by focusing on minimizing the operating expenditures (OPEX) while taking appropriate measures against cyber threats.

For instance, in June 2020, the Australian government allocated $1.35 billion towards enhancing the nation's cyber security capabilities over the next decade, under the Cyber Enhanced Situational Awareness and Response (CESAR) package. Under this CESAR, $35 million is allocated toward a new cyber threat-sharing platform which assists government to share intelligence about cyber activity and block emerging threats in the future.

The military segment to rule the roost during the forecast period

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 size, 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.

The endpoint security segment to maintain its dominance during the forecast period

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.

Make a Purchase Inquiry - https://www.alliedmarketresearch.com/purchase-enquiry/10092

Asia-Pacific to achieve the largest revenue and fastest growth by 2031

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.

Leading Market Players

Intel Corporation
AT&T Inc.
Northrop Grumman
IBM Corporation
Lockheed Martin Corporation
BAE Systems plc
Thales
EclecticIQ B.V.
SentinelOne
Boeing
DXC Technology Company

Cisco Systems, Inc.
Raytheon Technologies Corporation
Secureworks, Inc.
Privacera, Inc.

□□□□□□□□ □□□□□□□□ □□ □□□□ □□ □□□□□□□□□□ □□□□□□□□□ :

Aerospace Cyber Security Market - https://www.alliedmarketresearch.com/aerospace-cyber-security-market-A09068

Aerospace Bearings Market - https://www.alliedmarketresearch.com/aerospace-bearings-market-A14120

Aerospace Artificial Intelligence Market - https://www.alliedmarketresearch.com/aerospace-artificial-intelligence-market-A11337

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