

Defense Cybersecurity Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 – 2034

<https://marketpublishers.com/r/D070AC74135DEN.html>

Date: January 2025

Pages: 210

Price: US\$ 4,850.00 (Single User License)

ID: D070AC74135DEN

Abstracts

The Global Defense Cybersecurity Market, valued at USD 38.8 billion in 2024, is expected to expand at a CAGR of 9.8% from 2025 to 2034. As defense organizations face increasingly sophisticated cyber threats, there is an urgent need to protect critical, classified data from evolving risks. This heightened demand for advanced cybersecurity solutions across defense and aerospace sectors is driving market growth. The integration of cutting-edge security technologies, such as artificial intelligence (AI), machine learning (ML), and cloud-based infrastructure, is further accelerating this shift. With rising concerns over cyber-attacks targeting national security, defense systems worldwide are prioritizing investments in robust cybersecurity frameworks. In turn, this is fueling the adoption of next-gen security tools, providing comprehensive protection against both internal and external threats.

The market is divided into several segments, including software and services, hardware, and security types such as network security, endpoint security, application security, and cloud security. The software and services segment, which represented 62.5% of the market share in 2024, is expected to see significant growth. The growing adoption of cloud infrastructure among defense organizations is contributing to this trend, as cloud-native security solutions offer scalability and seamless integration with existing systems. These solutions are designed to respond quickly to emerging threats, making them a critical component in defense cybersecurity strategies.

In terms of security types, the network security segment is predicted to grow at a CAGR of 10.5% over the next decade. The increasing implementation of zero-trust security models, which continuously verify user and device identities, is a key factor driving this growth. By enforcing stringent access controls, defense organizations are better

equipped to safeguard sensitive data from cyber-attacks. Additionally, AI and ML are transforming network security, allowing systems to proactively identify and mitigate potential threats before they escalate. These advancements ensure that defense agencies stay ahead of increasingly sophisticated cybercriminals and state-sponsored cyber-attacks.

North America is set to dominate the defense cybersecurity market, generating USD 34 billion by 2034. The region's growth is driven by substantial investments in protecting critical defense infrastructure, as well as compliance with stringent regulations like the Cybersecurity Maturity Model Certification (CMMC). Organizations in North America are increasingly turning to zero-trust architectures and AI-powered security solutions to defend against complex cyber threats, including those posed by nation-state actors. This shift is reinforcing North America's position as a leader in the global defense cybersecurity market, and the demand for advanced cybersecurity solutions is only expected to increase in the coming years.

Contents

CHAPTER 1 METHODOLOGY & SCOPE

- 1.1 Market scope & definitions
- 1.2 Base estimates & calculations
- 1.3 Forecast calculations
- 1.4 Data sources
 - 1.4.1 Primary
 - 1.4.2 Secondary
 - 1.4.2.1 Paid sources
 - 1.4.2.2 Public sources

CHAPTER 2 EXECUTIVE SUMMARY

- 2.1 Industry synopsis, 2021-2034

CHAPTER 3 INDUSTRY INSIGHTS

- 3.1 Industry ecosystem analysis
 - 3.1.1 Factor affecting the value chain
 - 3.1.2 Profit margin analysis
 - 3.1.3 Disruptions
 - 3.1.4 Future outlook
 - 3.1.5 Manufacturers
 - 3.1.6 Distributors
- 3.2 Supplier landscape
- 3.3 Profit margin analysis
- 3.4 Key news & initiatives
- 3.5 Regulatory landscape
- 3.6 Impact forces
 - 3.6.1 Growth drivers
 - 3.6.1.1 Growing sophistication of cyberattacks targeting defense networks
 - 3.6.1.2 Integration of AI and machine learning in cybersecurity solutions
 - 3.6.1.3 Expansion of interconnected IoT devices and OT systems in military and defense
 - 3.6.1.4 Rising geopolitical tensions and ongoing defense modernization
 - 3.6.1.5 Increasing reliance on satellites and space technologies in military operations
 - 3.6.2 Industry pitfalls & challenges

- 3.6.2.1 High costs of advanced security solutions
- 3.6.2.2 Integration with legacy systems
- 3.7 Growth potential analysis
- 3.8 Porter's analysis
- 3.9 PESTEL analysis

CHAPTER 4 COMPETITIVE LANDSCAPE, 2024

- 4.1 Introduction
- 4.2 Company market share analysis
- 4.3 Competitive positioning matrix
- 4.4 Strategic outlook matrix

CHAPTER 5 MARKET ESTIMATES & FORECAST, BY SECURITY TYPE, 2021-2034 (USD MILLION)

- 5.1 Key trends
- 5.2 Network security
 - 5.2.1 Firewall and security appliance
 - 5.2.2 Intrusion Detection System (IDS)
 - 5.2.3 Intrusion Prevention System (IPS)
 - 5.2.4 Secure network infrastructure
- 5.3 Endpoint security
 - 5.3.1 Antivirus/antimalware solution
 - 5.3.2 Encryption tool
 - 5.3.3 Biometric device
- 5.4 Application security
 - 5.4.1 Encryption device
 - 5.4.2 Secure development tool
 - 5.4.3 Application security testing
- 5.5 Cloud security
 - 5.5.1 Secure cloud server and storage device
 - 5.5.2 Cloud encryption software
 - 5.5.3 Cloud Access Security Broker (CASB)

CHAPTER 6 MARKET ESTIMATES & FORECAST, BY OFFERING, 2021-2034 (USD MILLION)

- 6.1 Key trends

6.2 Hardware

6.3 Software and services

CHAPTER 7 MARKET ESTIMATES & FORECAST, BY APPLICATION, 2021-2034 (USD MILLION)

7.1 Key trends

7.2 Critical infrastructure protection

7.3 Data protection and encryption

7.4 Incident response and forensics

7.5 Identity and access management

7.6 Secure communications system

CHAPTER 8 MARKET ESTIMATES & FORECAST, BY END-USER, 2021-2034 (USD MILLION)

8.1 Key trends

8.2 Army

8.3 Navy

8.4 Air force

CHAPTER 9 MARKET ESTIMATES & FORECAST, BY REGION, 2021-2034 (USD MILLION)

9.1 Key trends

9.2 North America

9.2.1 U.S.

9.2.2 Canada

9.3 Europe

9.3.1 UK

9.3.2 Germany

9.3.3 France

9.3.4 Italy

9.3.5 Spain

9.3.6 Russia

9.4 Asia Pacific

9.4.1 China

9.4.2 India

9.4.3 Japan

9.4.4 South Korea

9.4.5 Australia

9.5 Latin America

9.5.1 Brazil

9.5.2 Mexico

9.6 MEA

9.6.1 South Africa

9.6.2 Saudi Arabia

9.6.3 UAE

CHAPTER 10 COMPANY PROFILES

10.1 Airbus

10.2 BAE Systems

10.3 Boeing

10.4 CACI International

10.5 Carlyle Group

10.6 Cisco

10.7 CrowdStrike

10.8 General Dynamics

10.9 Hanwha Systems

10.10 IBM

10.11 Israel Aerospace Industries

10.12 L3Harris Technologies

10.13 Leonardo

10.14 Lockheed Martin

10.15 ManTech International

10.16 Northrop Grumman

10.17 Palo Alto

10.18 Rafael Advanced Defense Systems

10.19 Raytheon Technologies

10.20 Rheinmetall

10.21 Saab

10.22 SAIC

10.23 Salient CRGT

10.24 Thales

I would like to order

Product name: Defense Cybersecurity Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 – 2034

Product link: <https://marketpublishers.com/r/D070AC74135DEN.html>

Price: US\$ 4,850.00 (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/D070AC74135DEN.html>