# 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

## CHAPTER 2 EXECUTIVE SUMMARY

## CHAPTER 3 INDUSTRY INSIGHTS

## 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