

# **Military Cybersecurity 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): Global Opportunity Analysis and Industry Forecast, 2024-2033**

<https://marketpublishers.com/r/MA765BC0C1ADEN.html>

Date: April 2024

Pages: 323

Price: US\$ 3,570.00 (Single User License)

ID: MA765BC0C1ADEN

## **Abstracts**

The global military cybersecurity market was valued at \$15.7 billion in 2023, and is estimated to reach \$68.5 billion by 2033, growing at a CAGR of 15.4% from 2024 to 2033.

The safeguarding of military networks, systems, and data from cyber threats and attacks is known as military cybersecurity. It includes the methods, tools, procedures, and practices that armed forces use to protect their communications networks, command and control systems, IT infrastructure, and sensitive data assets from unwanted access, use, interference, or destruction by enemies.

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 military cyber security market.

In addition, the transition of conventional military aircraft into autonomous or unmanned systems also presents unique cybersecurity challenges. Ensuring the integrity and security of the communication links, command systems, and sensor data of these unmanned platforms is crucial to prevent potential exploitation or hijacking by adversaries. Moreover, the rise in cyber-attacks targeting not only military networks but also critical infrastructure, regulatory bodies, trade organizations, and individuals underscores the need for robust defense cybersecurity measures. Cyber threats can range from espionage and sabotage to data breaches and disruptive attacks, posing significant risks to national security, economic stability, and public safety.

Despite the growing recognition of the importance of cybersecurity in the defense sector, there are challenges that could impede its growth. Limited awareness among military personnel and decision-makers about cybersecurity best practices and threats may result in insufficient investment and attention to cybersecurity initiatives.

Furthermore, there is a shortage of skilled cybersecurity professionals and workforce within the defense sector, exacerbating the challenge of defending against sophisticated cyber threats. Recruiting, training, and retaining cybersecurity experts with specialized knowledge of military systems and operations are essential for maintaining a strong military cybersecurity. Moreover, the demand for military cybersecurity solutions is driven by factors such as increased IT expenditure, the transition to autonomous military platforms, and the proliferation of cyber threats, addressing challenges like awareness gaps and workforce shortages is crucial for effectively mitigating cyber risks and safeguarding military assets and operations.

The global military cybersecurity market was affected by the COVID-19 pandemic, which led to disturbances in the supply chain and production procedures. The dynamics of the market were impacted by fluctuating demand and economic uncertainty. Despite these obstacles, the market quickly rebounded due to the defense industry's increased investment in the purchase of aerial, land, and marine vehicles for its military cybersecurity.

The market is propelled by the collaboration among military organizations and defense contractors which is playing a crucial role in enhancing technical expertise and

capabilities in cybersecurity. Joint initiatives and partnerships facilitate the development of innovative cybersecurity solutions adapted to the unique requirements of military operations.

The military cybersecurity market is witnessing robust growth driven by the increasing sophistication of cyber threats, the adoption of advanced military technologies, and collaborative efforts aimed at enhancing defense cyber resilience. As defense organizations prioritize cybersecurity as a core component of their strategic initiatives, the market is poised for further expansion to meet the evolving cybersecurity needs of modern military operations.

For instance, in January 2023, NATO announced that they have signed contracts with IBM Belgium and King ICT Croatia to support the organization's cybersecurity. These contracts which are valued at USD 31.7 million will cover the integration of cyber defense capabilities and associated configuration services from February until 2025 with an additional two-year option. Such factors are propelling the need for military cybersecurity market during the forecast period of 2022-2032.

The military cybersecurity market is segmented into type, deployment, solution, and region. By type, the market is divided into endpoint security solutions, network security solutions, and content security solutions. As per deployment, the market is fragmented into on-premises 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.

Region wise, the military cybersecurity market trends are analyzed across North America (U.S., Canada, and Mexico), Europe (UK, Germany, France, Russia, Italy, Spain, and rest of Europe), Asia-Pacific (China, India, Japan, Australia, South Korea, and rest of Asia-Pacific), Latin America (Brazil, Argentina, and Rest of Latin America) and Middle East and Africa (Saudi Arabia, UAE, Israel, and Africa).

Competitive analysis and profiles of the major global military cybersecurity market players that have been provided in the report include 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., SentinelOne, Secureworks, Inc., and Thales Group. The key strategies adopted by the major players of the global market are product launch, mergers, and acquisitions.

## Key Benefits For Stakeholders

This report provides a quantitative analysis of the market segments, current trends, estimations, and dynamics of the military cybersecurity market analysis from 2023 to 2033 to identify the prevailing military cybersecurity market opportunities.

The market research is offered along with information related to key drivers, restraints, and opportunities.

Porter's five forces analysis highlights the potency of buyers and suppliers to enable stakeholders make profit-oriented business decisions and strengthen their supplier-buyer network.

In-depth analysis of the military cybersecurity market segmentation assists to determine the prevailing market opportunities.

Major countries in each region are mapped according to their revenue contribution to the global market.

Market player positioning facilitates benchmarking and provides a clear understanding of the present position of the market players.

The report includes the analysis of the regional as well as global military cybersecurity market trends, key players, market segments, application areas, and market growth strategies.

Additional benefits you will get with this purchase are:

Quarterly Update and\* (only available with a corporate license, on listed price)

5 additional Company Profile of client Choice pre- or Post-purchase, as a free update.

Free Upcoming Version on the Purchase of Five and Enterprise User License.

16 analyst hours of support\* (post-purchase, if you find additional data requirements upon review of the report, you may receive support amounting to 16 analyst hours to solve questions, and post-sale queries)

15% Free Customization\* (in case the scope or segment of the report does not match your requirements, 15% is equivalent to 3 working days of free work, applicable once)

Free data Pack on the Five and Enterprise User License. (Excel version of the report)

Free Updated report if the report is 6-12 months old or older.

24-hour priority response\*

Free Industry updates and white papers.

Possible Customization with this report (with additional cost and timeline, please talk to the sales executive to know more)

Product Benchmarking / Product specification and applications

Regulatory Guidelines

Import Export Analysis/Data

Key Market Segments

By Deployment

On-Premises

Cloud

By Type

*Military Cybersecurity Market By Type (Endpoint Security Solutions, Network Security Solutions, Content Securi...*

Endpoint Security Solutions

Network Security Solutions

Content Security Solutions

## 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 Region

North America

U.S.

Canada

Mexico

Asia-Pacific

China

Japan

India

South Korea

Rest of Asia-Pacific

Europe

UK

Germany

France

Italy

Rest of Europe

LAMEA

Latin America

Middle East

Africa

Key Market Players

North Grumman Corporation

Lockhead Martin Corporation

BAE Systems

Thales

Intel Corporation

AT&T Inc.

Cisco Systems Inc.

IBM Corporation

SecureWorks Corp.

General Dynamics Corporation



## Contents

### **CHAPTER 1: INTRODUCTION**

- 1.1. Report Description
- 1.2. Key market segments
- 1.3. Key benefits to the stakeholders
- 1.4. Research methodology
  - 1.4.1. Primary research
  - 1.4.2. Secondary research
  - 1.4.3. Analyst tools and models

### **CHAPTER 2: EXECUTIVE SUMMARY**

- 2.1. CXO perspective

### **CHAPTER 3: MARKET OVERVIEW**

- 3.1. Market definition and scope
- 3.2. Key findings
  - 3.2.1. Top impacting factors
  - 3.2.2. Top investment pockets
- 3.3. Porter's Five Forces Analysis
- 3.4. Market dynamics
  - 3.4.1. Drivers
  - 3.4.2. Restraints
  - 3.4.3. Opportunities

### **CHAPTER 4: MILITARY CYBERSECURITY MARKET, BY TYPE**

- 4.1. Overview
  - 4.1.1. Market size and forecast
- 4.2. Endpoint Security Solutions
  - 4.2.1. Key market trends, growth factors and opportunities
  - 4.2.2. Market size and forecast, by region
  - 4.2.3. Market share analysis by country
- 4.3. Network Security Solutions
  - 4.3.1. Key market trends, growth factors and opportunities
  - 4.3.2. Market size and forecast, by region

- 4.3.3. Market share analysis by country
- 4.4. Content Security Solutions
  - 4.4.1. Key market trends, growth factors and opportunities
  - 4.4.2. Market size and forecast, by region
  - 4.4.3. Market share analysis by country

## **CHAPTER 5: MILITARY CYBERSECURITY MARKET, BY DEPLOYMENT**

- 5.1. Overview
  - 5.1.1. Market size and forecast
- 5.2. On-Premises
  - 5.2.1. Key market trends, growth factors and opportunities
  - 5.2.2. Market size and forecast, by region
  - 5.2.3. Market share analysis by country
- 5.3. Cloud
  - 5.3.1. Key market trends, growth factors and opportunities
  - 5.3.2. Market size and forecast, by region
  - 5.3.3. Market share analysis by country

## **CHAPTER 6: MILITARY CYBERSECURITY MARKET, BY SOLUTION**

- 6.1. Overview
  - 6.1.1. Market size and forecast
- 6.2. Threat Intelligence and Response Management
  - 6.2.1. Key market trends, growth factors and opportunities
  - 6.2.2. Market size and forecast, by region
  - 6.2.3. Market share analysis by country
- 6.3. Identity and Access Management
  - 6.3.1. Key market trends, growth factors and opportunities
  - 6.3.2. Market size and forecast, by region
  - 6.3.3. Market share analysis by country
- 6.4. Data Loss Prevention Management
  - 6.4.1. Key market trends, growth factors and opportunities
  - 6.4.2. Market size and forecast, by region
  - 6.4.3. Market share analysis by country
- 6.5. Security and Vulnerability Management
  - 6.5.1. Key market trends, growth factors and opportunities
  - 6.5.2. Market size and forecast, by region
  - 6.5.3. Market share analysis by country

- 6.6. Unified Threat Management
  - 6.6.1. Key market trends, growth factors and opportunities
  - 6.6.2. Market size and forecast, by region
  - 6.6.3. Market share analysis by country
- 6.7. Enterprise Risk and Compliance
  - 6.7.1. Key market trends, growth factors and opportunities
  - 6.7.2. Market size and forecast, by region
  - 6.7.3. Market share analysis by country
- 6.8. Managed Security
  - 6.8.1. Key market trends, growth factors and opportunities
  - 6.8.2. Market size and forecast, by region
  - 6.8.3. Market share analysis by country
- 6.9. Others
  - 6.9.1. Key market trends, growth factors and opportunities
  - 6.9.2. Market size and forecast, by region
  - 6.9.3. Market share analysis by country

## **CHAPTER 7: MILITARY CYBERSECURITY MARKET, BY REGION**

- 7.1. Overview
  - 7.1.1. Market size and forecast By Region
- 7.2. North America
  - 7.2.1. Key market trends, growth factors and opportunities
  - 7.2.2. Market size and forecast, by Type
  - 7.2.3. Market size and forecast, by Deployment
  - 7.2.4. Market size and forecast, by Solution
  - 7.2.5. Market size and forecast, by country
    - 7.2.5.1. U.S.
      - 7.2.5.1.1. Market size and forecast, by Type
      - 7.2.5.1.2. Market size and forecast, by Deployment
      - 7.2.5.1.3. Market size and forecast, by Solution
    - 7.2.5.2. Canada
      - 7.2.5.2.1. Market size and forecast, by Type
      - 7.2.5.2.2. Market size and forecast, by Deployment
      - 7.2.5.2.3. Market size and forecast, by Solution
    - 7.2.5.3. Mexico
      - 7.2.5.3.1. Market size and forecast, by Type
      - 7.2.5.3.2. Market size and forecast, by Deployment
      - 7.2.5.3.3. Market size and forecast, by Solution

### 7.3. Asia-Pacific

7.3.1. Key market trends, growth factors and opportunities

7.3.2. Market size and forecast, by Type

7.3.3. Market size and forecast, by Deployment

7.3.4. Market size and forecast, by Solution

7.3.5. Market size and forecast, by country

7.3.5.1. China

7.3.5.1.1. Market size and forecast, by Type

7.3.5.1.2. Market size and forecast, by Deployment

7.3.5.1.3. Market size and forecast, by Solution

7.3.5.2. Japan

7.3.5.2.1. Market size and forecast, by Type

7.3.5.2.2. Market size and forecast, by Deployment

7.3.5.2.3. Market size and forecast, by Solution

7.3.5.3. India

7.3.5.3.1. Market size and forecast, by Type

7.3.5.3.2. Market size and forecast, by Deployment

7.3.5.3.3. Market size and forecast, by Solution

7.3.5.4. South Korea

7.3.5.4.1. Market size and forecast, by Type

7.3.5.4.2. Market size and forecast, by Deployment

7.3.5.4.3. Market size and forecast, by Solution

7.3.5.5. Rest of Asia-Pacific

7.3.5.5.1. Market size and forecast, by Type

7.3.5.5.2. Market size and forecast, by Deployment

7.3.5.5.3. Market size and forecast, by Solution

### 7.4. Europe

7.4.1. Key market trends, growth factors and opportunities

7.4.2. Market size and forecast, by Type

7.4.3. Market size and forecast, by Deployment

7.4.4. Market size and forecast, by Solution

7.4.5. Market size and forecast, by country

7.4.5.1. UK

7.4.5.1.1. Market size and forecast, by Type

7.4.5.1.2. Market size and forecast, by Deployment

7.4.5.1.3. Market size and forecast, by Solution

7.4.5.2. Germany

7.4.5.2.1. Market size and forecast, by Type

7.4.5.2.2. Market size and forecast, by Deployment

7.4.5.2.3. Market size and forecast, by Solution

7.4.5.3. France

7.4.5.3.1. Market size and forecast, by Type

7.4.5.3.2. Market size and forecast, by Deployment

7.4.5.3.3. Market size and forecast, by Solution

7.4.5.4. Italy

7.4.5.4.1. Market size and forecast, by Type

7.4.5.4.2. Market size and forecast, by Deployment

7.4.5.4.3. Market size and forecast, by Solution

7.4.5.5. Rest of Europe

7.4.5.5.1. Market size and forecast, by Type

7.4.5.5.2. Market size and forecast, by Deployment

7.4.5.5.3. Market size and forecast, by Solution

7.5. LAMEA

7.5.1. Key market trends, growth factors and opportunities

7.5.2. Market size and forecast, by Type

7.5.3. Market size and forecast, by Deployment

7.5.4. Market size and forecast, by Solution

7.5.5. Market size and forecast, by country

7.5.5.1. Latin America

7.5.5.1.1. Market size and forecast, by Type

7.5.5.1.2. Market size and forecast, by Deployment

7.5.5.1.3. Market size and forecast, by Solution

7.5.5.2. Middle East

7.5.5.2.1. Market size and forecast, by Type

7.5.5.2.2. Market size and forecast, by Deployment

7.5.5.2.3. Market size and forecast, by Solution

7.5.5.3. Africa

7.5.5.3.1. Market size and forecast, by Type

7.5.5.3.2. Market size and forecast, by Deployment

7.5.5.3.3. Market size and forecast, by Solution

## **CHAPTER 8: COMPETITIVE LANDSCAPE**

8.1. Introduction

8.2. Top winning strategies

8.3. Product mapping of top 10 player

8.4. Competitive dashboard

8.5. Competitive heatmap

## 8.6. Top player positioning, 2023

### **CHAPTER 9: COMPANY PROFILES**

#### 9.1. North Grumman Corporation

- 9.1.1. Company overview
- 9.1.2. Key executives
- 9.1.3. Company snapshot
- 9.1.4. Operating business segments
- 9.1.5. Product portfolio
- 9.1.6. Business performance
- 9.1.7. Key strategic moves and developments

#### 9.2. Lockheed Martin Corporation

- 9.2.1. Company overview
- 9.2.2. Key executives
- 9.2.3. Company snapshot
- 9.2.4. Operating business segments
- 9.2.5. Product portfolio
- 9.2.6. Business performance
- 9.2.7. Key strategic moves and developments

#### 9.3. BAE Systems

- 9.3.1. Company overview
- 9.3.2. Key executives
- 9.3.3. Company snapshot
- 9.3.4. Operating business segments
- 9.3.5. Product portfolio
- 9.3.6. Business performance
- 9.3.7. Key strategic moves and developments

#### 9.4. Thales

- 9.4.1. Company overview
- 9.4.2. Key executives
- 9.4.3. Company snapshot
- 9.4.4. Operating business segments
- 9.4.5. Product portfolio
- 9.4.6. Business performance
- 9.4.7. Key strategic moves and developments

#### 9.5. Intel Corporation

- 9.5.1. Company overview
- 9.5.2. Key executives

- 9.5.3. Company snapshot
- 9.5.4. Operating business segments
- 9.5.5. Product portfolio
- 9.5.6. Business performance
- 9.5.7. Key strategic moves and developments
- 9.6. AT&T Inc.
  - 9.6.1. Company overview
  - 9.6.2. Key executives
  - 9.6.3. Company snapshot
  - 9.6.4. Operating business segments
  - 9.6.5. Product portfolio
  - 9.6.6. Business performance
  - 9.6.7. Key strategic moves and developments
- 9.7. Cisco Systems Inc.
  - 9.7.1. Company overview
  - 9.7.2. Key executives
  - 9.7.3. Company snapshot
  - 9.7.4. Operating business segments
  - 9.7.5. Product portfolio
  - 9.7.6. Business performance
  - 9.7.7. Key strategic moves and developments
- 9.8. IBM Corporation
  - 9.8.1. Company overview
  - 9.8.2. Key executives
  - 9.8.3. Company snapshot
  - 9.8.4. Operating business segments
  - 9.8.5. Product portfolio
  - 9.8.6. Business performance
  - 9.8.7. Key strategic moves and developments
- 9.9. SecureWorks Corp.
  - 9.9.1. Company overview
  - 9.9.2. Key executives
  - 9.9.3. Company snapshot
  - 9.9.4. Operating business segments
  - 9.9.5. Product portfolio
  - 9.9.6. Business performance
  - 9.9.7. Key strategic moves and developments
- 9.10. General Dynamics Corporation
  - 9.10.1. Company overview

- 9.10.2. Key executives
- 9.10.3. Company snapshot
- 9.10.4. Operating business segments
- 9.10.5. Product portfolio
- 9.10.6. Business performance
- 9.10.7. Key strategic moves and developments



## I would like to order

Product name: Military Cybersecurity 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): Global Opportunity Analysis and Industry Forecast, 2024-2033

Product link: <https://marketpublishers.com/r/MA765BC0C1ADEN.html>

Price: US\$ 3,570.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/MA765BC0C1ADEN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:  
Last name:  
Email:  
Company:  
Address:  
City:  
Zip code:  
Country:  
Tel:  
Fax:  
Your message:

**\*\*All fields are required**

Customer signature \_\_\_\_\_

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms

& Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below  
and fax the completed form to +44 20 7900 3970