Defense Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Defense Cyber Security Market Analysis

The Defense cyber security market size stood at USD 32.26 billion in 2025 and is projected to reach USD 46.51 billion by 2030, reflecting an 11.87% CAGR as the sector pivots toward "never-trust, always-verify" architectures across national security systems. Rapid institutionalization of zero-trust policies, the weaponization of operational technology, and mounting pressure to defend satellite and software-defined networks combine to elevate cyber operations to a full war-fighting domain on par with land, sea, air, and space. Mandates issued by the United States Department of Defense (DoD) to embed zero trust into every weapons platform by 2035 amplify demand for security solutions that operate at both enterprise and tactical echelons. At the same time, the shift to joint, all-domain operations under programs such as JADC2 and GCIA is propelling investment in secure cloud-edge fabrics capable of real-time data sharing in contested theaters.

Global Defense Cyber Security Market Trends and Insights

Rapid Deployment of Software-Defined & Satellite-Based Battlefield Networks in Asia

Asia-Pacific militaries are field-testing software-defined networks that let commanders reconfigure communications topologies in seconds, multiplying potential attack vectors that adversaries can exploit from space to shore. South Korea's 2024 doctrine now integrates offensive cyber options alongside zero-trust secure enclaves, signaling a regional transition from purely defensive postures. Japan's active cyber defense law takes effect by 2027 and permits government monitoring of critical infrastructure

traffic to flag anomalies, a marked expansion of state oversight. Coupling satellite links with terrestrial 5G nodes improves resilience, yet exposes spacecraft telemetry to spoofing and denial tactics. Exercises such as Talisman Sabre increasingly weave cyber objectives into kinetic war-games, underscoring how the Defense cyber security market is entwined with broader force-structure decisions.

Mandated Zero-Trust Architectures in U.S. & Five-Eyes Defence Procurement

Executive Order 14028 and National Security Memorandum 8 oblige every U.S. national-security system to embrace zero trust, fueling compliance-driven procurement that extends from enterprise IT to tactical weapon controls. The Pentagon's automation of assessment workflows accelerates accreditation without diluting rigor, a prerequisite for scaling across millions of endpoints. Five Eyes interoperability clauses now appear in request-for-proposal language, rewarding vendors that can satisfy multinational security-clearance thresholds. By 2035, zero trust must permeate launch-systems, avionics, and fire-control chains, demanding cryptographic agility and continuous identity verification even in communications-denied settings.

Fragmented Legacy Platforms Hindering End-to-End Encryption Roll-Out

Weapon systems built in the 1990s remain on duty, yet their processors and buses cannot handle modern cryptography without performance trade-offs. Each service branch still sustains platform-specific protocols, complicating any push for unified key-management. Commanders sometimes prefer mission uptime over exhaustive encryption, creating cultural resistance that matches the technical impasse. Because replacement cycles span decades, prime contractors must architect wrapper solutions that retrofit zero-trust principles without rewriting source code, a niche but growing slice of the Defense cyber security market.

Other drivers and restraints analyzed in the detailed report include:

Accelerated Digital-Twin & Autonomous Platform Adoption Demanding Real-Time OT-IT Security / Defense Cloud-Edge Migration Programmes (JADC2, GCIA) Driving Secure Data-Fabric Spend / Prolonged Security-Cleared Talent Gap in Classified Projects /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Solutions captured 67% revenue in 2024, reflecting steady refresh contracts for firewalls, secure-gateway appliances, and threat-intelligence platforms that anchor enterprise networks. That dominance translated into USD 21.6 billion of the Defense cyber security market size in the base year. Yet services are scaling faster, advancing at 11.8% CAGR, because militaries increasingly view security as a continuous practice rather than a one-off install.

Consulting teams now embed DevSecOps experts inside agile software factories to ensure code pipelines meet authority-to-operate standards from day one. Managed detection and response providers triage millions of daily alerts across the Air Force's global infrastructure, employing AI to suppress noise and elevate actionable threats. Training regimens covering zero-trust concepts, quantum-safe encryption, and adversarial AI are being delivered by private academies under indefinite-delivery contracts. These activities grow recurring revenue and tilt spending toward services, a pattern that will likely lift the Defense cyber security market share of services to one-third by 2030.

Network security remained the anchor at 42% in 2024, equivalent to USD 13.6 billion of the Defense cyber security market size. Firewalls, intrusion-prevention systems, and secure gateways still safeguard garrison networks, but cloud security is streaking ahead at 15.7% CAGR. JADC2 mandates multi-level security architectures that stretch from classified to coalition to commercial clouds, forcing procurement of identity, configuration, and data-loss-prevention controls tailored for infrastructure-as-code.

Endpoint and application security segments gain incremental traction as every drone, radar, and combat vehicle morphs into a node on the defense network. Quantum-random-number-generation and AI-enabled threat hunting are emerging sub-segments attracting venture capital and EDF grants. Vendors capable of spanning traditional perimeter defenses and containerized micro-services in cloud environments will consolidate share in the Defense cyber security market.

The Defense Cyber Security Market is Segmented by Component (Solutions, Services), Security Type (Network Security, Endpoint Security, Application Security, Cloud Security, Other Security Types), Deployment Mode (On-Premises, Cloud and Hybrid), End-User (Land Force, Naval Force. Air Force), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America retained the lead with 38% revenue in 2024 as congressional appropriations embedded cybersecurity line-items in every major acquisition program. Compliance regimes such as CMMC 2.0 obligate the entire defense industrial base-from primes to sub-tier suppliers-to implement controls before bidding, enlarging addressable demand beyond uniformed customers. Canada follows U.S. frameworks to preserve Five Eyes interoperability, while Mexico's procurement ties gain momentum through cross-border defense technology transfers.

Asia-Pacific is expanding at 11.4% CAGR through 2030 on the strength of accelerated cyber doctrine in Japan and South Korea, India's trilateral partnerships with Australia and the United States, and South-East Asian fleet upgrades designed to monitor contested waterways. Sovereign-cloud mandates coupled with satellite network investments make the region the most dynamic theater for vendors targeting forward-deployed, software-defined capabilities within the Defense cyber security market.

Europe benefits from EUR 8 billion (USD 8.5 billion) in EDF funding for 2021-2027, plus the DIANA accelerator that marries NATO demand signals with venture capital. The European Investment Bank's June 2025 tranche of EUR 8.9 billion (USD 9.4 billion) earmarked for security technologies underlines how public-finance tools are funneling capital into sovereign cyber resilience projects. Meanwhile, the Middle East and Africa register healthy but lower growth as budgets prioritize kinetic systems first; nonetheless, adoption of NATO-aligned standards creates latent demand that global integrators aim to unlock.

List of Companies Covered in this Report:

CACI International Inc. / SAIC Inc. / Raytheon Technologies Corp. / Lockheed Martin Corp. / General Dynamics Corp. / L3Harris Technologies Inc. / BAE Systems plc / Northrop Grumman Corp. / Booz Allen Hamilton Holding Corp. / Leidos Holdings Inc. / Thales Group / Airbus Defence and Space / Leonardo S.p.A / QinetiQ Group plc / Palantir Technologies Inc. / Darktrace plc / Viasat Inc. / IBM Corporation / DXC Technology / Rohde and Schwarz Cybersecurity /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

5.5.1.2 Canada
5.5.1.3 Mexico
5.5.2 Europe
5.5.2.1 United Kingdom
5.5.2.2 Germany
5.5.2.3 France
5.5.2.4 Italy
5.5.2.5 Spain
5.5.2.6 Rest of Europe
5.5.3 Asia-Pacific
5.5.3.1 China
5.5.3.2 India
5.5.3.3 Japan
5.5.3.4 South Korea
5.5.3.5 Rest of Asia-Pacific
5.5.4 South America
5.5.4.1 Brazil
5.5.4.2 Chile
5.5.4.3 Colombia
5.5.4.4 Rest of South America
5.5.5 Middle East
5.5.5.1 Saudi Arabia
5.5.5.2 United Arab Emirates
5.5.5.3 Israel
5.5.5.4 Qatar
5.5.5.5 Turkey
5.5.5.6 Rest of Middle East
5.5.6 Africa
5.5.6.1 South Africa
5.5.6.2 Nigeria
5.5.6.3 Rest of Africa

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves (Partnerships, JVs, RandD)
6.3 Market Share Analysis
6.4 Company Profiles (includes Global Level Overview, Market Level Overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)
6.4.1 CACI International Inc.
6.4.2 SAIC Inc.
6.4.3 Raytheon Technologies Corp.
6.4.4 Lockheed Martin Corp.
6.4.5 General Dynamics Corp.
6.4.6 L3Harris Technologies Inc.
6.4.7 BAE Systems plc
6.4.8 Northrop Grumman Corp.
6.4.9 Booz Allen Hamilton Holding Corp.

Defense Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-03
		Signature