Government And Public Sector Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 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:

Government And Public Sector Cybersecurity Market Analysis

The Government And Public Sector Cybersecurity Market was valued at USD 75.14 billion in 2025 and estimated to grow from USD 84.61 billion in 2026 to reach USD 153.35 billion by 2031, at a CAGR of 12.62% during the forecast period (2026-2031).

Escalating state-sponsored attacks, fast-tracking of zero-trust mandates, and quantum-resistant encryption projects are reshaping procurement priorities across every tier of government. NATO's pledge to spend 1.5% of GDP on cyber resilience is diverting defence resources toward new threat-intelligence platforms, while federal budgets in the United States, the European Union, and key Asia-Pacific economies are earmarking multi-year allocations that favour end-to-end managed security services. Spending is shifting from reactive perimeter protection to proactive detection powered by artificial intelligence, augmented by workforce outsourcing to offset talent shortages. As a result, the government and public sector cybersecurity market is experiencing broader vendor consolidation, deeper public-private partnerships, and longer contract tenures anchored in performance-based service-level agreements.

Global Government And Public Sector Cybersecurity Market Trends and Insights

Escalating State-Sponsored Cyber-Attacks on Critical Public Infrastructure

State-linked groups such as Salt Typhoon have breached federal networks and telecom infrastructure, demonstrating how adversaries leverage supply-chain compromises to gain persistent access to multiple government domains. Security teams now prioritise continuous monitoring, threat hunting, and forensic readiness, replacing periodic "point-in-time" scans. High-profile water-utility disruptions in 2024 revealed that operational technology environments can be weaponised to cause real-world service outages, prompting agencies to adopt cross-domain security architectures. Budget allocations, therefore, increasingly favour threat-intelligence feeds, endpoint detection, and 24 7 incident-response retainers. The cumulative effect is sustained demand for integrated solutions that shorten detection-to-containment cycles across federal, state, and local layers.

Government Zero-Trust Funding Mandates and Compliance Deadlines

The United States Defense Information Systems Agency is rolling out a zero-trust framework that requires identity verification, device hygiene, and micro-segmentation for every transaction across Department of Defense networks. Failure to meet timeline targets risks budget forfeiture, so agencies accelerate multi-factor authentication and continuous diagnostics deployments. State and local bodies align with federal standards to unlock matching funds, evident in California's USD 22.6 million grant pool that prioritises zero-trust implementations. Vendors offering consolidated platforms spanning identity, endpoint, and cloud workloads gain a competitive advantage in crowded tenders, while integrators differentiate through reference architectures that map legacy assets to zero-trust maturity models. As deadlines converge in 2026, procurement pipelines are filling rapidly with multi-year, performance-based contracts.

Legacy System Integration and Technical Debt

Decades of incremental upgrades have left agencies with siloed mainframes, proprietary protocols, and undocumented interfaces that complicate modernisation projects. Implementing zero-trust across such heterogeneous environments often demands costly data migrations and parallel operations, inflating budgets beyond initial estimates. In Michigan, ransomware actors exploited outdated authentication controls in municipal servers, paralysing essential operations and illustrating the direct link between technical debt and operational risk. Federal audits estimate individual legacy-system overhauls can cost more than USD 100 million, forcing agencies to stage rollouts and rely on compensating controls that add further complexity. These constraints slow the adoption of advanced security frameworks and dilute the immediate impact on threat-mitigation metrics.

Other drivers and restraints analyzed in the detailed report include:

Rapid Cloud Migration of Citizen-Facing ServicesAI-Augmented Citizen Services Expanding Attack SurfaceCyber-Talent Shortage and Public-Sector Pay Gap

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

Segment Analysis

Network Security recorded USD 21.27 billion in 2025 and defended a 28.31% government and public sector cybersecurity market share on the strength of entrenched perimeter firewalls and intrusion-prevention systems that remain baseline procurement line items. Budget line continuity reflects audit mandates that still prioritise perimeter visibility despite known limitations against lateral movement. Yet Cloud Security generated only USD 13.34 billion but is forecast to grow faster at a 13.05% CAGR through 2031 as agencies transition citizen services into FedRAMP and ENISA-certified hosting. Identity and Access Management is also scaling as zero-trust checkpoints redistribute security emphasis toward user verification and continuous authentication. Rising endpoint investments underpin secure telework policies, while application-layer testing enjoys uplift from large-scale digital-service overhauls.

By 2031, Cloud Security is projected to claim a material share of the government and public sector cybersecurity market size, illustrating how hybrid architectures elevate demand for data-centric controls alongside flexible policy orchestration. Encryption and data-security upgrades accelerate as post-quantum migration deadlines approach, influencing procurement specifications to demand NIST-validated algorithms. Vendors are bundling key management as-a-service with analytics to simplify deployment across multi-cloud environments. In parallel, application-security gateways incorporate API posture management to police interactions with third-party contractors and software supply-chain dependencies. Combined, these shifts underscore a transition from single-point products to layered, interoperable security suites that map neatly to evolving architecture roadmaps.

On-premises systems retained USD 39.18 billion in revenue and 52.15% government and public sector cybersecurity market share during 2025. Sensitive workloads such as defence command-and-control and citizen identity repositories remain anchored in agency-controlled data centres, but the narrative is changing as risk-based classification models free less critical data for cloud processing. Cloud deployments, valued at USD 19.68 billion, are advancing at a 12.78% CAGR, fuelled by consumption-based pricing and the operational flexibility needed for elastic service demand during emergencies. Hybrid strategies bridge compliance with efficiency: agencies adopt containerised micro-services for new applications while gradually retiring monoliths.

As cloud confidence builds, hybrid architectures are forecast to add USD 16.1 billion to the government and public sector cybersecurity market size by 2031, requiring unified policy engines that span identity, data, and network controls. Secure access service edge solutions emerge as the connective tissue, routing traffic through inspection nodes regardless of hosting location. Vendors differentiate by offering pre-packaged reference designs that accelerate accreditation under FedRAMP Moderate and NIS2 compliance tracks. Meanwhile, funding frameworks now earmark modernisation grants specifically for orchestration platforms that normalise compliance reporting across mixed environments, signalling that hybrid will dominate new awards through the forecast window.

Government and Public Sector Cybersecurity Market Report is Segmented by Solution Type (Network Security, Endpoint Security, and More), Deployment Model (On-Premises, Cloud, and Hybrid), Government Level (National/Federal Agencies, Defense and Intelligence, and More), Security Service Type (Consulting and Advisory, Managed Security Services, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America contributed USD 28.64 billion and retained 38.12% of the government and public sector cybersecurity market in 2025 on the back of robust federal directives, sustained grant programmes, and active public-private information sharing. Treasury Department's USD 20 billion PROTECTS framework illustrates contract scale and an inclination for platform-based solutions. Canada is setting up the BOREALIS agency to advance quantum and AI security, further solidifying regional leadership. State-level regulation, such as California's IoT Cyber Trust Mark, creates harmonised baselines that streamline vendor certification pipelines.

Europe stood at USD 20.2 billion in 2025, propelled by the Digital Europe Programme's EUR 390 million cybersecurity budget and the forthcoming enforcement of NIS2 directives. EU-wide reciprocity efforts with U.S. FedRAMP align certification schemes, accelerating cross-border vendor consolidation. Individual member states, notably Germany and France, are allocating sovereign-cloud grants to ensure data localisation while benefitting from hyperscale efficiencies. These initiatives push the region toward integrated security suites that embed compliance reporting and zero-trust blueprints.

Asia-Pacific clocked USD 15.57 billion and is projected to record the highest 12.94% CAGR, adding significant heft to the government and public sector cybersecurity market by 2031. Japan's Active Cyber Defense bill authorises proactive threat hunting, while South Korea targets AI-enabled detection for critical infrastructure. Australia's Cyber Security Strategy emphasises regional partnerships, expanding opportunities for shared intelligence platforms. Simultaneously, emerging economies in Southeast Asia are setting up national CSIRTs, funnelling donor and domestic funds into core monitoring capabilities. Middle East and Africa, though smaller today, are quickly scaling post-oil diversification budgets to protect smart-city and energy projects, signalling an upcoming wave of tenders for operational-technology segmentation and encryption gateways.

List of Companies Covered in this Report:

Palo Alto Networks, Inc. CrowdStrike Holdings, Inc. Fortinet, Inc. Check Point Software Technologies Ltd. Zscaler, Inc. Okta, Inc. Splunk Inc. Tenable Holdings, Inc. CyberArk Software Ltd. Rapid7, Inc. Darktrace plc Mandiant LLC (Google Cloud) Trellix Corporation Booz Allen Hamilton Holding Corporation BAE Systems plc Thales S.A. Elastic N.V. Proofpoint, Inc. Ivanti, Inc. Cohesity, Inc.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION
1.1 Study Assumptions and Market Definition
1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET LANDSCAPE
4.1 Market Overview
4.2 Market Drivers
4.2.1 Escalating state-sponsored cyber-attacks on critical public infrastructure
4.2.2 Government "zero-trust" funding mandates and compliance deadlines
4.2.3 Rapid cloud migration of citizen-facing services
4.2.4 AI-augmented citizen services expanding attack surface
4.2.5 NATO pledge of 1.5 % GDP on cyber and critical-infra protection
4.2.6 NIS2 / FedRAMP reciprocity accelerating vendor consolidation
4.3 Market Restraints
4.3.1 Legacy system integration and technical debt
4.3.2 Cyber-talent shortage and public-sector pay gap
4.3.3 Multi-cloud data-sovereignty conflicts
4.3.4 Fragmented procurement and elongated sales cycles
4.4 Value Chain Analysis
4.5 Regulatory Landscape
4.6 Technological Outlook
4.7 Porter's Five Forces Analysis
4.7.1 Threat of New Entrants
4.7.2 Bargaining Power of Suppliers
4.7.3 Bargaining Power of Buyers
4.7.4 Threat of Substitutes
4.7.5 Intensity of Competitive Rivalry

4.8 Impact of Macroeconomic Factors on the Market

5 MARKET SIZE AND GROWTH FORECASTS (VALUES)
5.1 By Solution Type
5.1.1 Network Security
5.1.2 Endpoint Security
5.1.3 Cloud Security
5.1.4 Application Security
5.1.5 Identity and Access Management (IAM)
5.1.6 Data Security and Encryption
5.2 By Deployment Model
5.2.1 On-premises
5.2.2 Cloud
5.2.3 Hybrid
5.3 By Government Level
5.3.1 National/Federal Agencies
5.3.2 Defense and Intelligence
5.3.3 State/Provincial Departments
5.3.4 Local/Municipal Bodies
5.3.5 Critical Infrastructure Authorities
5.4 By Security Service Type
5.4.1 Consulting and Advisory
5.4.2 Managed Security Services (MSS)
5.4.3 Incident Response and Forensics
5.4.4 Training and Awareness
5.5 By Geography
5.5.1 North America
5.5.1.1 United States
5.5.1.2 Canada
5.5.1.3 Mexico
5.5.2 South America
5.5.2.1 Brazil
5.5.2.2 Argentina
5.5.2.3 Chile
5.5.2.4 Rest of South America
5.5.3 Europe
5.5.3.1 Germany
5.5.3.2 United Kingdom
5.5.3.3 France
5.5.3.4 Italy
5.5.3.5 Spain
5.5.3.6 Rest of Europe
5.5.4 Asia-Pacific
5.5.4.1 China
5.5.4.2 Japan
5.5.4.3 India
5.5.4.4 South Korea

5.5.4.5 Australia
5.5.4.6 Singapore
5.5.4.7 Malaysia
5.5.4.8 Rest of Asia-Pacific
5.5.5 Middle East and Africa
5.5.5.1 Middle East
5.5.5.1.1 Saudi Arabia
5.5.5.1.2 United Arab Emirates
5.5.5.1.3 Turkey
5.5.5.1.4 Rest of Middle East
5.5.5.2 Africa
5.5.5.2.1 South Africa
5.5.5.2.2 Nigeria
5.5.5.2.3 Rest of Africa

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves
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 Palo Alto Networks, Inc.
6.4.2 CrowdStrike Holdings, Inc.
6.4.3 Fortinet, Inc.
6.4.4 Check Point Software Technologies Ltd.
6.4.5 Zscaler, Inc.
6.4.6 Okta, Inc.
6.4.7 Splunk Inc.
6.4.8 Tenable Holdings, Inc.
6.4.9 CyberArk Software Ltd.
6.4.10 Rapid7, Inc.
6.4.11 Darktrace plc
6.4.12 Mandiant LLC (Google Cloud)
6.4.13 Trellix Corporation
6.4.14 Booz Allen Hamilton Holding Corporation
6.4.15 BAE Systems plc
6.4.16 Thales S.A.
6.4.17 Elastic N.V.
6.4.18 Proofpoint, Inc.
6.4.19 Ivanti, Inc.
6.4.20 Cohesity, Inc.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK
7.1 White-space and Unmet-Need Assessment

Government And Public Sector Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 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	2026-02-13
		Signature	