Critical Infrastructure Protection (CIP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 150 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:

Critical Infrastructure Protection (CIP) Market Analysis

The Critical Infrastructure Protection market size is valued at USD 154.32 billion in 2025 and is projected to reach USD 187.03 billion by 2030, reflecting a 3.92% CAGR over the forecast horizon. This balanced expansion shows how cybersecurity and physical security are converging into unified programs that protect energy, transportation, water, and communications assets. Heightened state-backed attacks, expanding regulatory mandates, and rapid digitization of operational technology (OT) are increasing demand for threat monitoring, incident reporting, and zero-trust access solutions. North American investments remain dominant, yet Asia-Pacific growth is accelerating as 5G, edge computing, and smart-grid deployments widen the attack surface. Services revenue is rising faster than traditional hardware and software because operators are outsourcing continuous monitoring to managed security providers. Meanwhile, talent gaps and legacy OT interoperability issues temper deployment speed even as artificial-intelligence-driven analytics unlock predictive protection models.

Global Critical Infrastructure Protection (CIP) Market Trends and Insights

Growing Government Mandates Drive Compliance-Led Market Expansion

Mandatory regulations are reshaping Critical Infrastructure Protection market purchasing patterns. The EU NIS-2 directive extends obligatory cybersecurity to 18 sectors and any organization with more than 50 employees and EUR 10 million (USD 10.9 million) revenue, enlarging the addressable base. In the United States, CISA's proposed CIRCIA rule compels roughly 316,000 entities to

report cyber incidents within 72 hours and ransomware payments within 24 hours. Alignment around ISA/IEC 62443 standards simplifies vendor certification and drives bulk procurement, while entities that previously relied on voluntary guidelines now accelerate investments to meet penalties and audit thresholds.

State-Backed Cyber Campaigns Target Operational Technology Systems

Nation-state groups are prioritizing long-dwell infiltration of OT networks that run power, water, and transport systems. Chinese actor Volt Typhoon remained in U.S. infrastructure for over five years aiming for disruptive capability rather than espionage. Similar campaigns against U.S. water facilities and Japanese aerospace organizations underscore the shift from IT-centric data theft to OT-level sabotage. These threats exploit aged protocols such as Modbus that lack authentication, spurring investment in specialized intrusion detection and network segmentation tools.

Legacy OT Systems Create Persistent Interoperability Challenges

Industrial assets often run for decades on protocols without basic encryption. Modbus and OPC Classic cannot be patched without downtime, requiring costly compensating controls such as data diodes and virtual patching. The FBI labels end-of-life systems the "Achilles' heel" of infrastructure security, indicating that many upgrades depend on multi-year capital planning. These barriers slow the Critical Infrastructure Protection market even as compliance dates loom.

Other drivers and restraints analyzed in the detailed report include:

Smart-Grid Modernization Integrates Physical and Cyber Protection / 5G Network Expansion Creates New Attack Surfaces in Telecom Infrastructure / Acute Workforce Shortages Limit Deployment Capabilities /

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

Segment Analysis

Solutions generated 66.0% of 2024 revenue; however, Services are projected to expand at a 5.7% CAGR as organizations confront mounting complexity. Managed detection and response, compliance auditing, and incident recovery are bundled into subscription contracts that transfer operational risk. Cloud Security Alliance guidance notes that zero-trust rollouts in OT require specialized road-mapping and 24/7 monitoring, workloads most enterprises lack in-house.

The Critical Infrastructure Protection market benefits as managed providers consolidate expertise through acquisitions such as GardaWorld's integration of OnSolve for critical-event management. Dragos' purchase of Network Perception adds continuous visualization of firewall rules to its industrial platform, broadening cross-sell potential. These moves illustrate how scale and breadth of service accelerate competitive advantage and underpin long-run recurring revenue.

Physical Safety and Security retained 56.9% of 2024 spend through perimeter surveillance, access control, and screening technologies. Yet the Cybersecurity segment is advancing 5.9% annually as threat actors migrate to IT-OT convergence points. The Critical Infrastructure Protection market size for SCADA/OT security is expected to rise sharply given new zero-trust baselines, while network micro-segmentation products isolate legacy assets without plant shutdowns.

Automatic response suites such as Siemens SIBERprotect isolate compromised nodes within milliseconds, demonstrating how machine-speed defense reshapes incident containment. Identity-and-access platforms built for air-gapped systems prevent credential sprawl. As capital planners seek integrated dashboards combining CCTV analytics with cyber alerts, convergence software continues to erode the historical divide between physical and digital safeguards.

Critical Infrastructure Protection Market is Segmented by Component (Solutions, Services), Security Type (Physical Safety and Security, Cybersecurity), Deployment Mode (On-Premise, Cloud/X-as-a-Service), Vertical (Energy and Power, BFSI, and More), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America maintained 36.1% of 2024 revenue, underpinned by CISA's performance-goal road map that aligns 16 sectors with mandatory reporting. Schneider Electric's USD 700 million manufacturing expansion demonstrates sustained capital inflows that localize supply chains and shorten response times for grid customers. The Department of Homeland Security's AI safety framework further standardizes risk posture, fostering home-market strength for domestic vendors.

Asia-Pacific posts the fastest regional CAGR at 4.2% to 2030. Japan's Active Cyber Defense Bill enables pre-emptive threat hunting, while the KDDI-NEC alliance scales managed supply-chain protection for industrial customers. ASEAN economies collectively budget USD 171 billion for cybersecurity by 2025, stimulating demand for localized SOCs and language-aware threat analytics. China's national programs and India's digital-public-infrastructure model broaden vendor opportunity, though unique encryption rules require country-specific product variants.

List of Companies Covered in this Report:

BAE Systems PLC / Honeywell International Inc. / Lockheed Martin Corporation / General Dynamics Corporation / Northrop Grumman Corp. / Hexagon AB / Airbus SE / General Electric Company / Kaspersky Lab Inc. / Waterfall Security Solutions Ltd. / Ericsson AB / Claroty / Cisco Systems Inc. / IBM Corporation / ABB Ltd. / Schneider Electric SE / Raytheon Technologies Corp. / Palo Alto Networks Inc. / Siemens AG / Johnson Controls International / Thales Group / Trellix / Booz Allen Hamilton / Darktrace PLC / Fortinet / Dragos /

Additional Benefits:

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

Table of Contents:

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 Rest of South America
5.5.3 Europe
5.5.3.1 United Kingdom
5.5.3.2 Germany
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 New Zealand
5.5.4.6 Rest of Asia-Pacific
5.5.5 Middle East and Africa
5.5.5.1 Middle East
5.5.5.1.1 GCC
5.5.5.1.2 Turkey
5.5.5.1.3 Israel
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 Egypt
5.5.5.2.4 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 BAE Systems PLC
6.4.2 Honeywell International Inc.
6.4.3 Lockheed Martin Corporation
6.4.4 General Dynamics Corporation
6.4.5 Northrop Grumman Corp.
6.4.6 Hexagon AB
6.4.7 Airbus SE
6.4.8 General Electric Company

Critical Infrastructure Protection (CIP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 150 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