Industrial Control Systems Security - 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:

Industrial Control Systems Security Market Analysis

Industrial Control Systems Security Market size in 2026 is estimated at USD 20.55 billion, growing from 2025 value of USD 19.24 billion with 2031 projections showing USD 28.57 billion, growing at 6.83% CAGR over 2026-2031.

Board-level prioritization of operational technology cyber-resilience, convergence of IT-OT networks, and escalating ransomware activity underpin sustained demand. North America retains leadership thanks to regulations such as NERC CIP-013 and the rapid incident-reporting mandate in CIRCIA. Asia-Pacific delivers the steepest growth as utilities and discrete manufacturers modernize SCADA assets and connect IIoT devices at scale. Solutions remain the revenue backbone, yet double-digit expansion of managed security services shows enterprises shifting toward 24/7 outsourced monitoring amid an acute OT-skilled labor shortage. Network segmentation and deep-packet inspection dominate current deployments, while cloud/remote-access protection gains momentum with the rise of hosted historians and remote maintenance portals.

Global Industrial Control Systems Security Market Trends and Insights

Accelerating IIoT-driven OT Connectivity Transforms Manufacturing Security

One-third of the 75 billion connected devices expected in 2025 will sit inside factories, exposing legacy production lines to unprecedented cyber risk. European and Japanese discrete manufacturers are integrating vision systems, robotics, and

predictive-maintenance sensors that require east-west traffic inspection and zero-trust segmentation. This intensified data flow strains traditional perimeter defenses and forces deployment of protocol-aware detection tools inside Ethernet/IP, PROFINET, and Modbus networks. Vendors respond with lightweight agents for resource-constrained controllers and DPI sensors that parse proprietary industrial frames without disrupting cycle times. As IT and OT teams co-manage assets, demand rises for unified dashboards that map Purdue levels 0-3 and automate policy rollouts. Budget holders increasingly tie security spend to overall equipment effectiveness metrics, reinforcing ROI narratives around avoided downtime.

Regulatory Compliance Drives Critical-Infrastructure Security Investment

NERC CIP-013 in North America and the EU's NIS2 Directive impose binding obligations ranging from supply-chain risk management to 72-hour incident reporting. Utilities, transport networks, and chemical plants accelerate procurements to avoid fines that can exceed 2% of annual turnover. The regulations also elevate cyber discussions from engineering teams to executive committees, compressing sales cycles for vendors offering audit-ready reporting and evidence collection. Integrators bundle asset-discovery, configuration-monitoring, and secure-file-transfer capabilities to meet both standards concurrently, simplifying multi-jurisdiction compliance. Momentum in the ICS security market is further boosted by insurers demanding proof of ICS segmentation before renewing coverage or lowering premiums.

Legacy System Integration Challenges Hinder Security Implementation

Modern firewalls and anomaly-detection engines must adapt to 20-year-old PLCs that lack encrypted firmware or role-based access controls. Retrofitting often requires staged shutdowns that jeopardize output quotas and contractual service-level agreements. Forty-six percent of asset owners need up to six months to patch a critical vulnerability, prolonging exposure windows. Cost-benefit debates delay full micro-segmentation projects, pushing some operators toward partial implementations like read-only passive monitoring, which offers visibility yet leaves write-access pathways unguarded.

Other drivers and restraints analyzed in the detailed report include:

Aging Infrastructure Modernization Creates Security ImperativesRansomware Targeting Critical Infrastructure Drives Security UrgencyCybersecurity Talent Gap Constrains Security Implementation

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

Segment Analysis

In 2025, the industrial control systems security market size attributed USD 12.96 billion to solutions, equal to a 67.35% revenue share. Firewalls, protocol-aware IPS, identity gateways, and vulnerability scanners formed the backbone of first-wave deployments. Spending grows steadily as vendors embed artificial-intelligence analytics that cut signature-update cycles and flag zero-day behaviors in real time. The industrial control systems security market now witnesses converged platforms that ingest logs across Purdue levels, enriching context for quicker root-cause correlation.

The services segment, valued at USD 6.28 billion in 2025, records the fastest 10.86% CAGR through 2031. Managed detection and response offerings combine remote tier-1 triage and on-site incident-handlers, allowing plants to maintain uptime while meeting 72-hour reporting mandates. Integration and deployment partners bridge heterogeneous vendor stacks, mapping asset inventories against ISA/IEC 62443 zones before configuring layered controls. Consulting teams benchmark maturity via kill-chain simulations, then craft phased roadmaps tied to capex refresh cycles. Support and maintenance contracts secure firmware updates and periodic rule-set tuning, reducing mean time to patch by more than 30% in highly regulated energy utilities.

Network security anchors 36.55% of 2025 revenues as operators prioritize physical and virtual segmentation appliances that filter protocol commands and mirror traffic to passive collectors. Zero-trust architectures isolate HMIs, historians, and engineering workstations, preventing lateral movement from IT subnets. Threat-intelligence feeds inject industrial IOCs, helping SOC teams block malicious OT-specific command sequences.

Cloud/remote-access security posts a 12.01% forecast CAGR, the highest among categories, as plants adopt digital twins and vendor-assisted maintenance portals. Multi-factor identity gateways, just-in-time session brokers, and continuous posture assessment counter the heightened risk from internet-exposed endpoints. Endpoint security tools harden PLCs, RTUs, and sensors with agentless monitoring that tracks firmware states and memory integrity. Application-layer defenses use dynamic code analysis to spot unsafe calls within MES and batch-execution software, while database firewalls safeguard time-series operational data against exfiltration.

The Industrial Control Systems ICS Security Market Report is Segmented by Component (Solutions, Services), Security Type (Network Security, Endpoint Security, Application Security, and More), Control System Type (SCADA, Distributed Control System (DCS), and More), End-User Industry (Automotive, Chemical & Petrochemical, Power and Utilities, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America generated 32.60% of 2025 global revenue. Federal scrutiny intensified after headline breaches, prompting asset owners to adopt CISA's Shields-Up advisories and submit vulnerability reports within stipulated windows. Investments accelerate around secure remote access for sparsely staffed pumping stations and wind farms. Canada's National Cyber Threat Assessment warns that hostile states could disrupt energy exports, pushing provincial regulators to align with NERC CIP frameworks.

Asia-Pacific records the highest 8.15% CAGR from 2026 to 2031. China scales cyber-hygiene across thousands of new substations, blending domestic firewall brands with global analytics engines. Japan upgrades robot-dense automotive lines, coupling deep-packet inspection appliances with OT-aware SIEM integrations. South Korea leverages its 5G backbone, necessitating encryption and identity overlays for millisecond-latency control commands. India replaces serial-to-Ethernet converters in hydro projects, inserting inspection taps that feed national-level SOCs. ASEAN SMEs rely on vendor-hosted SOCs as local talent pipelines mature.

Europe remains a pivotal market as NIS2 expands enforcement to medium-sized critical entities. Germany's BSI drives cross-sector vulnerability advisory sharing, while France's ANSSI prescribes segmentation checklists. United Kingdom utilities pilot AI-based predictive anomaly engines to meet Ofgem resilience targets. Renewable-energy growth in Spain and Italy sparks demand for authentication brokers that manage inverter OEMs during field maintenance. Latin America and Middle East & Africa steadily adopt defenses; Brazilian utilities implement supply-chain attestation for PLC firmware, and Gulf pipeline operators deploy deception grids to deter reconnaissance.

List of Companies Covered in this Report:

Honeywell International Inc. Cisco Systems Inc. IBM Corporation Fortinet Inc. ABB Ltd. Rockwell Automation Inc. Dragos Inc. Nozomi Networks Inc. Palo Alto Networks Inc. Check Point Software Technologies Ltd. Darktrace Holdings Limited Broadcom Inc. (Symantec) Trellix Schneider Electric SE Siemens AG Kaspersky Lab GE Vernova (GE Digital) Claroty Ltd. Trend Micro Inc. AhnLab Inc.

Additional Benefits:

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

Table of Contents:

Industrial Control Systems Security - 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	2026-03-03
		Signature