

Industrial Control Systems Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-09-01 | 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:

Industrial Control Systems Security Market Analysis

The Industrial Control Systems Security Market size is estimated at USD 19.24 billion in 2025, and is expected to reach USD 26.86 billion by 2030, at a CAGR of 6.90% during the forecast period (2025-2030).

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

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

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 Imperatives / Ransomware Targeting Critical Infrastructure Drives Security Urgency / Cybersecurity Talent Gap Constrains Security Implementation /

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

Segment Analysis

In 2024, the industrial control systems security market size attributed USD 13.1 billion to solutions, equal to a 68% 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 6.1 billion in 2024, records the fastest 11.2% CAGR through 2030. 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.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Network security anchors 37% of 2024 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 12.5% 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 33% of 2024 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 8.3% CAGR from 2025 to 2030. 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:

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

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

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 Accelerating IIoT-driven OT Connectivity in Discrete Manufacturing (EU and Japan)
 - 4.2.2 Mandatory NERC CIP-013 and EU NIS2 Compliance for Critical Infrastructure Operators
 - 4.2.3 Modernization of Ageing SCADA/DCS Assets in Asian Power and Water Utilities
 - 4.2.4 Surge in Ransomware Attacks on Oil and Gas Pipelines (US and Middle East)
 - 4.2.5 Growth of Distributed Renewables Requiring Remote-Access Protection
 - 4.2.6 Adoption of Cloud-hosted Historians and Remote Maintenance Platforms
- 4.3 Market Restraints
 - 4.3.1 High Retrofit Costs and Downtime for Legacy PLCs
 - 4.3.2 OT-Skilled Cyber-Talent Shortage in Mid-size ASEAN Manufacturers
 - 4.3.3 Limited Interoperability of Proprietary Industrial Protocols
 - 4.3.4 Procurement Delays from IT/OT Tool-Stack Overlap ("Security Fatigue")
- 4.4 Value / Supply-Chain Analysis
- 4.5 Regulatory and Technological Outlook
- 4.6 Porter's Five Forces Analysis
 - 4.6.1 Bargaining Power of Suppliers
 - 4.6.2 Bargaining Power of Buyers
 - 4.6.3 Threat of New Entrants
 - 4.6.4 Threat of Substitutes
 - 4.6.5 Intensity of Competitive Rivalry
- 4.7 Investment Analysis

5 MARKET SIZE AND GROWTH FORECASTS (VALUE)

- 5.1 By Component
 - 5.1.1 Solutions
 - 5.1.1.1 Firewall and IPS
 - 5.1.1.2 Identity and Access Management
 - 5.1.1.3 Antivirus and Antimalware
 - 5.1.1.4 Security and Vulnerability Management
 - 5.1.1.5 Data Loss Prevention and Recovery
 - 5.1.1.6 Other Solutions
 - 5.1.2 Services
 - 5.1.2.1 Consulting and Assessment

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 5.1.2.2 Integration and Deployment
- 5.1.2.3 Support and Maintenance
- 5.1.2.4 Managed Security Services
- 5.2 By Security Type
 - 5.2.1 Network Security
 - 5.2.2 Endpoint Security
 - 5.2.3 Application Security
 - 5.2.4 Database Security
 - 5.2.5 Cloud/Remote Access Security
- 5.3 By Control System Type
 - 5.3.1 Supervisory Control and Data Acquisition (SCADA)
 - 5.3.2 Distributed Control System (DCS)
 - 5.3.3 Programmable Logic Controller (PLC)
 - 5.3.4 Other Control Systems
- 5.4 By End-user Industry
 - 5.4.1 Automotive
 - 5.4.2 Chemical and Petrochemical
 - 5.4.3 Power and Utilities
 - 5.4.4 Oil and Gas
 - 5.4.5 Food and Beverage
 - 5.4.6 Pharmaceuticals
 - 5.4.7 Water and Wastewater
 - 5.4.8 Mining and Metals
 - 5.4.9 Transportation and Logistics
 - 5.4.10 Other Industries
- 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 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 Rest of Europe
 - 5.5.3 Asia-Pacific
 - 5.5.3.1 China
 - 5.5.3.2 Japan
 - 5.5.3.3 India
 - 5.5.3.4 South Korea
 - 5.5.3.5 Rest of Asia-Pacific
 - 5.5.4 Middle East
 - 5.5.4.1 Israel
 - 5.5.4.2 Saudi Arabia
 - 5.5.4.3 United Arab Emirates
 - 5.5.4.4 Turkey

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 5.5.4.5 Rest of Middle East
- 5.5.5 Africa
 - 5.5.5.1 South Africa
 - 5.5.5.2 Egypt
 - 5.5.5.3 Rest of Africa
- 5.5.6 South America
 - 5.5.6.1 Brazil
 - 5.5.6.2 Argentina
 - 5.5.6.3 Rest of South America

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, Strategic Information, Market Rank/Share, Products and Services, Recent Developments)
 - 6.4.1 Honeywell International Inc.
 - 6.4.2 Cisco Systems Inc.
 - 6.4.3 IBM Corporation
 - 6.4.4 Fortinet Inc.
 - 6.4.5 ABB Ltd.
 - 6.4.6 Rockwell Automation Inc.
 - 6.4.7 Dragos Inc.
 - 6.4.8 Nozomi Networks Inc.
 - 6.4.9 Palo Alto Networks Inc.
 - 6.4.10 Check Point Software Technologies Ltd.
 - 6.4.11 Darktrace Holdings Limited
 - 6.4.12 Broadcom Inc. (Symantec)
 - 6.4.13 Trellix
 - 6.4.14 Schneider Electric SE
 - 6.4.15 Siemens AG
 - 6.4.16 Kaspersky Lab
 - 6.4.17 GE Vernova (GE Digital)
 - 6.4.18 Claroty Ltd.
 - 6.4.19 Trend Micro Inc.
 - 6.4.20 AhnLab Inc.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK

- 7.1 White-space and Unmet-Need Assessment

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Industrial Control Systems Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-09-01 | 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	2026-03-04
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com