+357 96 030922
info@marketpublishers.com

Cybersecurity for Industrial Control Systems Market Forecasts to 2032 – Global Analysis By Component (Solution and Service), Deployment Model (On-Premises, Cloud-Based and Hybrid), Security Type, System Type, Application and By Geography

https://marketpublishers.com/r/C15AC7DCE582EN.html
Date: July 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: C15AC7DCE582EN

Abstracts

According to Stratistics MRC, the Global Cybersecurity for Industrial Control Systems Market is accounted for $22.91 billion in 2025 and is expected to reach $42.18 billion by 2032 growing at a CAGR of 9.11% during the forecast period. Cybersecurity for Industrial Control Systems (ICS) is critical to ensuring the safe and reliable operation of essential infrastructure such as power plants, water treatment facilities, manufacturing systems, and transportation networks. ICS environments, such as Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, and Programmable Logic Controllers (PLCs), were once isolated but are now more frequently linked to corporate IT networks and the internet, which leaves them open to cyber attacks. Moreover, these systems are frequently based on antiquated technology with weak security features, making them vulnerable to ransom ware, malware intrusions, and nation-state exploits.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), in 2022 it published over 300 Advisories representing thousands of vulnerabilities in a variety of ICS/OT products, affecting sectors such as energy, water/wastewater, manufacturing, food/agriculture, and chemical.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Growing risks of cyber attacks on vital infrastructure

The market for ICS cybersecurity is largely driven by the increasing sophistication and frequency of cyber attacks on critical infrastructure. Threat actors have proven their ability to target physical processes, interfere with necessary services, and even put human life in danger through attacks like Stuxnet, BlackEnergy, TRITON, and Industroyer. In addition to resulting in monetary losses, these incidents have raised awareness of operational environments' vulnerabilities. Additionally, the rise of state-sponsored hackers and cybercriminal organizations that target industrial sectors—particularly power grids, oil refineries, chemical plants, and water utilities—continues to change the threat landscape.

Restraint:

High maintenance and deployment costs

Small and medium-sized businesses (SMEs) may find it expensive to implement complete cybersecurity solutions across industrial control systems. Expenses consist of the initial purchase of hardware and software tools, the employment of specialist cybersecurity staff, vulnerability assessments, and continuing maintenance and updates. Furthermore, security solutions for ICS environments might need to be vendor-specific or custom-built, which raises costs even more. In industries with limited operating budgets, cybersecurity projects frequently clash with other capital expenditures, making it challenging for businesses to set aside enough money. In emerging economies and less digitalized industries, in particular, this financial strain slows market penetration.

Opportunity:

Increasing need for threat intelligence and monitoring with an ICS focus

Demand for domain-specific threat intelligence, anomaly detection tools, and continuous monitoring services catered to industrial settings is rising as cyber threats targeting ICS become more complex. Because of operational limitations, system sensitivities, and protocol differences, traditional IT-centric security solutions frequently don't work for OT systems. Because of this gap, cybersecurity providers can create solutions that emphasize real-time response mechanisms, OT asset visibility, and behavioral analytics. Additionally, threat intelligence platforms that compile information on sector-specific indicators of compromise (IOCs), threat actor behavior, and ICS vulnerabilities

+357 96 030922
info@marketpublishers.com

are turning into crucial instruments for proactive defense tactics in industrial sectors.

Threat:

Threats are invisible in OT networks

The restricted visibility into OT network activity is one of the particular risks to ICS environments. Conventional IT security tools, like intrusion detection systems or antivirus software, frequently conflict with OT protocols and are unable to efficiently monitor or identify threats in real time. Numerous industrial systems use legacy devices and proprietary communication protocols that don't produce standard security logs. Because of this, malicious activity may go unnoticed for extended periods of time, giving attackers the opportunity to stay integrated into the system and conduct sabotage or intelligence gathering. Furthermore, ICS networks are susceptible to insider threats and external attacks due to their lack of granular monitoring capabilities.

Covid-19 Impact:

The COVID-19 pandemic accelerated digital transformation and revealed serious vulnerabilities, which had a substantial effect on the cybersecurity market for industrial control systems (ICS). The convergence of IT and OT systems grew more intense as industrial operations adjusted to remote work and greater automation, increasing vulnerability to cyber threats and expanding the attack surface. ICS environments were more susceptible to intrusion because remote access tools, which were hurriedly put in place to ensure operational continuity, frequently lacked adequate security controls. However, the spike in cyber attacks during the pandemic—particularly ransom ware that targeted critical infrastructure—inspired long-term investments in ICS cybersecurity and increased stakeholder awareness, making it a strategic priority for risk management and resilience in the post-pandemic era.

The on-premises segment is expected to be the largest during the forecast period

The on-premises segment is expected to account for the largest market share during the forecast period, largely because it is widely used in vital infrastructure sectors like manufacturing, utilities, energy, and defense. Data privacy, system control, and operational continuity are top priorities for these industries' organizations, and on-premises deployment provides superior support for these goals. More customization, stricter security measures, and less vulnerability to online threats are all made possible by these solutions, which make them particularly appropriate for air-gapped and legacy

+357 96 030922
info@marketpublishers.com

ICS environments. Moreover, the need for stringent regulatory compliance and low network exposure continues to propel the dominance of on-premises cybersecurity solutions in ICS environments, despite the growing interest in cloud and hybrid models.

The endpoint security segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the endpoint security segment is predicted to witness the highest growth rate. Endpoint security guards against malware, tampering, and unwanted access to vital industrial assets, including engineering workstations, HMIs, PLCs, RTUs, and sensors. These devices are becoming more vulnerable to attacks that can spread laterally within industrial environments as a result of the merging of IT and OT networks. Furthermore, there is a significant increase in demand for endpoint defenses tailored to ICS, such as host-based intrusion prevention, application white listing, secure configurations, and real-time monitoring.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by its strict cybersecurity laws, high automation technology adoption, and sophisticated industrial infrastructure. The need for strong ICS security solutions has increased due to the existence of important critical infrastructure sectors, including manufacturing, transportation, energy, and water, as well as the frequency of cyber attacks that target these sectors. Investment in cybersecurity has also been boosted by frameworks like NERC CIP and NIST, as well as regulatory organizations like the U.S. Cybersecurity and Infrastructure Security Agency. Moreover, North America is a global leader in ICS cybersecurity adoption and innovation due to its abundance of top cybersecurity vendors and solid public-private partnerships.

Region with highest CAGR:

Over the forecast period, the Asia-Pacific region is anticipated to exhibit the highest CAGR, fueled by rising investments in vital infrastructure in nations like China, India, Japan, and South Korea, as well as by fast industrialization and the expanding use of smart manufacturing. The demand for strong ICS cybersecurity has increased as these economies implement Industrial Internet of Things (IIoT) technologies and speed up their digital transformation. Governments and businesses in the region are strengthening their security postures as a result of growing cyber threats and regulatory pressures. Additionally, Asia-Pacific is the fastest-growing regional market for ICS

+357 96 030922
info@marketpublishers.com

cybersecurity solutions due to rising urbanization, rising energy demands, and the expansion of industries like power generation, transportation, and oil and gas.

Key players in the market

Some of the key players in Cybersecurity for Industrial Control Systems Market include IBM Corporation, Fortinet, Rockwell Automation Inc., ABB, Cisco, Palo Alto Networks, Check Point, Honeywell, Schneider Electric, BAE Systems, Darktrace Inc, Siemens AG, Microsoft, Lockheed Martin, Nozomi Networks Inc, Claroty Inc and Raytheon Technologies.

Key Developments:

In May 2025, IBM is working with Oracle to bring the power of watsonx, IBM's flagship portfolio of AI products, to Oracle Cloud Infrastructure (OCI). Leveraging OCI's native AI services, the latest milestone in IBM's technology partnership with Oracle is designed to fuel a new era of multi-agentic, AI-driven productivity and efficiency across the enterprise.

In April 2025, Rockwell Automation and Amazon Web Services, Inc. (AWS) announced a collaboration to help support manufacturers in accelerating their digital transformation journeys. The initiative brings together Rockwell Automation's operational technology (OT) and AWS's cloud services to provide more secure, scalable solutions that help to improve asset performance, enhance visibility, and convert operational data into actionable insights.

In October 2024, Fortinet and CrowdStrike announced a partnership. This collaboration merges CrowdStrike's Falcon platform with Fortinet's FortiGate next-generation firewalls, aiming to offer seamless, end-to-end protection that spans networks, applications, and devices.

Components Covered:

- Solution
- Service

Deployment Models Covered:

+357 96 030922
info@marketpublishers.com

On-Premises

Cloud-Based

Hybrid

Security Types Covered:

Network Security

Endpoint Security

Application Security

Database Security

System Types Covered:

Supervisory Control and Data Acquisition (SCADA)

Distributed Control System (DCS)

Programmable Logic Controller (PLC)

Human Machine Interface (HMI)

Other System Types

Applications Covered:

Power and Energy

Critical Manufacturing

Mining

+357 96 030922
info@marketpublishers.com

- Oil & Gas
- Water Utility
- Transportation
- Pharmaceuticals
- Chemical
- Other Applications

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain
  - Rest of Europe
- Asia Pacific

+357 96 030922
info@marketpublishers.com

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

- Saudi Arabia
- UAE
- Qatar
- South Africa
- Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments

+357 96 030922
info@marketpublishers.com

- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cybersecurity for Industrial Control Systems Market Forecasts to 2032 – Global Analysis By Component (Solution and Service), Deployment Model (On-Premises, Cloud-Based and Hybrid), Security Type, System Type, Application and By Geography

Product link: https://marketpublishers.com/r/C15AC7DCE582EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/C15AC7DCE582EN.html