+357 96 030922
info@marketpublishers.com

Industrial Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Hardware, Software and Services), Security Type, Solution Type, Deployment Mode, End User and By Geography

https://marketpublishers.com/r/I1380E342581EN.html
Date: October 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: I1380E342581EN

Abstracts

According to Stratistics MRC, the Global Industrial Cybersecurity Market is accounted for $54.48 billion in 2025 and is expected to reach $112.40 billion by 2032 growing at a CAGR of 10.9% during the forecast period. Industrial cybersecurity aims to safeguard essential industrial operations—including factories, energy infrastructure, and transport systems—against cyberattacks. The adoption of IoT devices, operational technology, and industrial control systems has increased exposure to security threats, heightening the need for protection. Key measures include identifying risks, segmenting networks, monitoring systems in real time, detecting threats, and training staff to prevent unauthorized access or operational disruptions. Ensuring adherence to regulations, preparing incident response strategies, and updating systems regularly are critical. As industries undergo digital transformation, strong cybersecurity frameworks are vital for maintaining continuous operations, protecting confidential information, and reducing potential financial and reputational damage from cyber threats.

According to the Data Security Council of India (DSCI), the Indian cybersecurity market reached ?17,200 crore (USD 2.07 billion) in 2023, with industrial and critical infrastructure sectors contributing significantly to demand due to increased digitization and threat exposure.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Growing adoption of IoT and industrial automation

The rise in IoT device deployment and industrial automation is fueling growth in the Industrial Cybersecurity market. Companies increasingly rely on connected sensors, smart devices, and automated control systems to improve efficiency, gather data, and streamline processes. However, such digital interconnectivity also increases vulnerability to cyberattacks, data leaks, and operational interruptions, making protective measures critical. The shift toward digital transformation in industrial environments amplifies the demand for cybersecurity solutions, including monitoring tools, threat detection systems, and endpoint protection. This growing necessity drives investments in securing industrial networks and ensures uninterrupted operations while safeguarding sensitive operational information from cyber threats.

Restraint:

High implementation costs

The expensive nature of implementing industrial cybersecurity solutions poses a major limitation for market expansion. Establishing advanced security measures, such as firewalls, intrusion detection systems, and endpoint protection, requires significant financial resources. Small and medium enterprises frequently face challenges in allocating adequate budgets for full-scale cybersecurity implementation. Beyond initial investments, ongoing costs for system monitoring, maintenance, and employee training further increase financial strain. These cost-related issues can slow adoption rates and restrict scalability, particularly among smaller industries. As a result, budget constraints remain a key barrier for organizations seeking to safeguard industrial networks, limiting widespread deployment of advanced cybersecurity solutions in various industrial domains.

Opportunity:

Adoption of advanced security technologies

The integration of advanced security technologies presents significant opportunities for the Industrial Cybersecurity market. Cutting-edge tools such as AI, machine learning, automated threat detection, and behavioral analytics allow industrial systems to identify and respond to cyber threats proactively. These technologies improve operational efficiency, speed up incident response, and reduce the consequences of cyberattacks. Industrial enterprises are increasingly adopting predictive cybersecurity solutions

+357 96 030922
info@marketpublishers.com

capable of detecting anomalies, preventing breaches, and ensuring regulatory compliance. The ongoing development of innovative security technologies offers solution providers the chance to design specialized tools, software, and services to safeguard industrial networks and critical infrastructure against increasingly complex cyber threats, enhancing overall system resilience.

Threat:

Increasing sophistication of cyberattacks

The rise in sophisticated cyberattacks represents a major threat to the Industrial Cybersecurity market. Attackers are utilizing advanced methods, including ransomware, malware, phishing, and persistent threats, to compromise industrial networks. With increased interconnectivity through IoT devices, automation, and cloud systems, industrial infrastructure faces growing exposure to vulnerabilities. Rapidly evolving cyber threats challenge organizations to implement up-to-date security technologies and maintain effective threat intelligence. Failure to address these advanced attacks can result in operational disruptions, financial setbacks, and reputational harm, directly impacting industrial productivity and highlighting the critical need for resilient cybersecurity strategies, making the threat landscape a major concern for market growth and stability.

Covid-19 Impact:

The COVID-19 crisis influenced the Industrial Cybersecurity market by accelerating the adoption of digital technologies and remote operations in industrial sectors. Lockdowns and safety restrictions led companies to implement cloud platforms, automated systems, and remote monitoring solutions to sustain productivity. Although these technologies improved operational efficiency, they also heightened vulnerability to cyberattacks, as remote access and interconnected devices created new security risks. In response, organizations increased spending on cybersecurity tools, threat intelligence, risk mitigation, and employee awareness programs. The pandemic underscored the importance of strong industrial cybersecurity frameworks to protect sensitive information, maintain continuous operations, and shield critical infrastructure from evolving cyber threats.

The hardware segment is expected to be the largest during the forecast period

The hardware segment is expected to account for the largest market share during the

+357 96 030922
info@marketpublishers.com

forecast period due to its essential function in defending industrial operations against cyber threats. Key components such as firewalls, secure gateways, network appliances, and intrusion detection systems serve as the foundation of industrial cybersecurity frameworks. These devices protect sensitive operational technology and control systems by monitoring traffic, ensuring secure communication, and preventing unauthorized access. With the rising integration of automation, IoT, and interconnected industrial networks, the need for dependable and efficient hardware solutions has increased significantly. Companies focus on implementing robust hardware to protect critical infrastructure, ensure continuous operations, and reduce vulnerabilities to potential cyberattacks across industrial environments.

The energy & utilities segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the energy & utilities segment is predicted to witness the highest growth rate due to rapid digital transformation and automation of critical infrastructure. The adoption of smart grids, IoT devices, and cloud-based energy management solutions exposes power generation, transmission, and distribution networks to increased cyber risks. Ensuring protection against data breaches, operational failures, and regulatory violations has become a strategic priority. Rising investments in advanced cybersecurity technologies, including threat detection, monitoring, and risk mitigation, are supporting this growth. As energy and utility companies embrace innovative digital solutions, the demand for tailored industrial cybersecurity measures rises, driving substantial market expansion in this sector.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by its highly developed industrial base, rapid adoption of digital technologies, and strict regulatory standards. The region hosts numerous key industrial and energy players, extensive manufacturing operations, and critical infrastructure, which drives the requirement for comprehensive cybersecurity solutions. The increasing deployment of IoT, automation, and industrial control systems heightens vulnerability to cyber threats, prompting organizations to invest heavily in hardware, software, and services to protect operational data and ensure uninterrupted performance. Continuous technological innovation, proactive cybersecurity strategies, and heightened awareness of cyber risks reinforce North America’s leading market position, making it the largest contributor to the industrial cybersecurity sector globally.

+357 96 030922
info@marketpublishers.com

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, fueled by rapid industrial development, digitalization, and the integration of automation and IoT systems. Expanding manufacturing, energy, and transportation sectors in emerging economies face increasing cyber risks, driving demand for robust security solutions. Government policies, regulatory standards, and rising awareness about cybersecurity further support market growth. Companies in the region are prioritizing the protection of operational technology, industrial control systems, and critical infrastructure. The combination of accelerated industrial expansion, technology adoption, and focused cybersecurity investments makes Asia-Pacific the region with the highest CAGR, representing significant opportunities in the industrial cybersecurity sector.

Key players in the market

Some of the key players in Industrial Cybersecurity Market include Cisco Systems Inc., ABB Ltd., Fortinet Inc., Honeywell International Inc., Palo Alto Networks Inc., Schneider Electric SE, Rockwell Automation Inc., Dell Technologies Inc., Siemens AG, IBM Corporation, Check Point Software Technologies Ltd., Kaspersky Lab, Tenable Inc., Dragos Inc. and Nozomi Networks Inc.

Key Developments:

In March 2025, ABB has signed a Leveraged Procurement Agreement (LPA) to support as the automation partner for Dow’s Path2Zero project at Fort Saskatchewan in Alberta, Canada. According to Dow, the project, which is currently under construction, will create the world’s first net-zero Scope 1 and 2 greenhouse gas emissions ethylene and derivatives complex1, producing the essential building blocks needed for many of the materials and products that society relies on.

In December 2024, Fortinet has just completed the acquisition of Perception Point, a leader in advanced collaboration and email security. This strategic acquisition will enhance its mission to provide end-to-end cybersecurity by extending protection beyond email into the broader modern workspace. While the companies did not disclose the deal's value, media reports estimated to be around $100 million.

In December 2024, Honeywell announced the signing of a strategic agreement with Bombardier, a global leader in aviation and manufacturer of world-class business jets,

+357 96 030922
info@marketpublishers.com

to provide advanced technology for current and future Bombardier aircraft in avionics, propulsion and satellite communications technologies.

Components Covered:

- Hardware
- Software
- Services

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Physical Security Integration

Solution Types Covered:

- Antivirus/Malware Protection
- Firewall & Perimeter Defense
- Data Loss Prevention (DLP)
- SCADA Security
- Security Information and Event Management (SIEM)
- Identity and Access Management (IAM)

+357 96 030922
info@marketpublishers.com

DDoS Mitigation

Deployment Modes Covered:

On-premise

Cloud

End Users Covered:

Energy & Utilities

Discrete Manufacturing

Process Manufacturing

Transportation & Logistics

Other End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

+357 96 030922
info@marketpublishers.com

- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- 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

+357 96 030922
info@marketpublishers.com

Qatar

South Africa

Rest of Middle East & Africa

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

+357 96 030922
info@marketpublishers.com

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

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+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: Industrial Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Hardware, Software and Services), Security Type, Solution Type, Deployment Mode, End User and By Geography

Product link: https://marketpublishers.com/r/I1380E342581EN.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/I1380E342581EN.html