

Global Cyber Security For Industrial Automation Market Size study, by Security Type (Enterprise Security, SCADA Security, Network Security, Device Security, Physical Security), by End Use (Automotive Manufacturing, Electronics and Telecommunication, Food & Beverage Processing, Pharmaceuticals, Others), by Type (Flexible Automation System, Integrated Automation System, Fixed Automation System, Programmable Automation System), by Tools or Technologies (Numerical Control (NC) Machine Tools, Programmable Logic Controllers (PLCs), Computer Numerical Control (CNC) Systems, Industrial Sensors) and Regional Forecasts 2022-2032

<https://marketpublishers.com/r/G5BCAD149843EN.html>

Date: July 2024

Pages: 200

Price: US\$ 4,950.00 (Single User License)

ID: G5BCAD149843EN

Abstracts

Global Cyber Security for Industrial Automation Market is valued approximately at USD 9.6 billion in 2023 and is anticipated to grow with a healthy growth rate of more than 8.9% over the forecast period 2024-2032. The integration of cybersecurity in industrial automation, often associated with Industry 4.0 and smart manufacturing, has become increasingly crucial. This focus on cybersecurity aims to protect critical infrastructure within the industrial sector, safeguarding sensitive information from cyber threats. Industrial automation systems, encompassing various control systems, sensors, and technologies, are frequently connected to networks, making them susceptible to cyber-attacks. Consequently, sectors such as energy, transportation, and manufacturing are implementing robust cybersecurity measures to protect their critical infrastructure from

unauthorized access and disruptions.

The growing demand for cybersecurity in detecting and responding to cyber threats, while maintaining data integrity and confidentiality, is expected to drive market growth. The intrusion detection systems and security monitoring tools are integral to identifying and mitigating potential cyber threats in real-time. This proactive approach minimizes the impact of security incidents and prevents data loss. Additionally, the importance of maintaining data integrity and confidentiality in industrial automation necessitates the implementation of cybersecurity measures such as data encryption and secure storage practices. These measures ensure the protection of sensitive data from unauthorized access and tampering. Furthermore, the focus of many legacy systems on integrity and availability rather than security complicates the digitalization of supply chain management processes. This disparity between legacy and modern IoT systems presents a significant challenge for implementing effective cybersecurity measures in the industrial sector. For instance, in October 2023, Dragos Inc., a company in cybersecurity for industrial control systems (ICS) and operational technology (OT) environments, expanded its collaborative capabilities with Rockwell Automation, enhancing threat detection for ICS/OT cybersecurity. However, the market faces challenges such as outdated legacy systems and compliance issues in integrating various cybersecurity tools and technologies. Legacy systems, often manufactured using different approaches, pose significant hurdles when adopting new cybersecurity technologies.

The key regions considered for the Global Hologram Market study include North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa. North America boasts a significant industrial base across various sectors including manufacturing, energy (oil and gas, utilities), transportation, and healthcare. These industries increasingly rely on interconnected systems and automation to enhance efficiency and productivity. The convergence of IT (Information Technology) and OT (Operational Technology) networks in industrial settings has exposed critical infrastructure to cyber threats such as ransomware, malware, and targeted attacks. These threats can disrupt operations, compromise safety, and cause financial losses. Regulatory bodies in North America, such as the Department of Homeland Security (DHS) in the US and similar agencies in Canada, have introduced cybersecurity frameworks and guidelines (e.g., NIST Cybersecurity Framework) to strengthen defenses against cyber threats in critical infrastructure sectors. The Asia-Pacific region is projected to experience the highest growth rate during the forecast period 2024-2032.

Major market players included in this report are:

IBM

ABB
Schneider Electric
Honeywell International Inc.
Siemens AG
Microsoft Corporation
Rockwell Automation Inc.
Palo Alto Networks
Cisco Systems, Inc.
Dell Inc.
Dragos Inc.
Fortinet, Inc.
Kaspersky Lab
CyberArk
Check Point Software Technologies Ltd.

The detailed segments and sub-segment of the market are explained below:

By Security Type:

Enterprise Security
SCADA Security (Supervisory Control and Data Acquisition)
Network Security
Device Security
Physical Security

By End Use:

Automotive Manufacturing
Electronics and Telecommunication
Food & Beverage Processing
Pharmaceuticals
Others

By Type:

Flexible Automation System
Integrated Automation System
Fixed Automation System
Programmable Automation System

By Tools or Technologies:

Numerical Control (NC) Machine Tools
Programmable Logic Controllers (PLCs)

Computer Numerical Control (CNC) Systems Industrial Sensors

By Region:

North America

U.S.

Canada

Europe

UK

Germany

France

Spain

Italy

ROE

Asia Pacific

China

India

Japan

Australia

South Korea

RoAPAC

Latin America

Brazil

Mexico

Rest of Latin America

Middle East & Africa

Saudi Arabia

South Africa

RoMEA

Years considered for the study are as follows:

Historical year – 2022

Base year – 2023

Forecast period – 2024 to 2032

Key Takeaways:

Market Estimates & Forecast for 10 years from 2022 to 2032.

Annualized revenues and regional level analysis for each market segment.

Detailed analysis of geographical landscape with Country level analysis of major regions.

Competitive landscape with information on major players in the market.

Analysis of key business strategies and recommendations on future market approach.

Analysis of competitive structure of the market.

Demand side and supply side analysis of the market.

Contents

CHAPTER 1. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET EXECUTIVE SUMMARY

- 1.1. Global Cyber Security For Industrial Automation Market Size & Forecast (2022-2032)
- 1.2. Regional Summary
- 1.3. Segmental Summary
 - 1.3.1. By Security Type
 - 1.3.2. By End Use
 - 1.3.3. By Type
 - 1.3.4. By Tools or Technologies
- 1.4. Key Trends
- 1.5. Recession Impact
- 1.6. Analyst Recommendation & Conclusion

CHAPTER 2. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET DEFINITION AND RESEARCH ASSUMPTIONS

- 2.1. Research Objective
- 2.2. Market Definition
- 2.3. Research Assumptions
 - 2.3.1. Inclusion & Exclusion
 - 2.3.2. Limitations
 - 2.3.3. Supply Side Analysis
 - 2.3.3.1. Availability
 - 2.3.3.2. Infrastructure
 - 2.3.3.3. Regulatory Environment
 - 2.3.3.4. Market Competition
 - 2.3.3.5. Economic Viability (Consumer's Perspective)
 - 2.3.4. Demand Side Analysis
 - 2.3.4.1. Regulatory frameworks
 - 2.3.4.2. Technological Advancements
 - 2.3.4.3. Environmental Considerations
 - 2.3.4.4. Consumer Awareness & Acceptance
- 2.4. Estimation Methodology
- 2.5. Years Considered for the Study
- 2.6. Currency Conversion Rates

CHAPTER 3. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET DYNAMICS

3.1. Market Drivers

- 3.1.1. Growing Popularity of Cyber Security Measures
- 3.1.2. Rising Cyber Threats in Industrial Automation
- 3.1.3. Increasing Integration of Advanced Technologies

3.2. Market Challenges

- 3.2.1. Outdated Legacy Systems
- 3.2.2. Compliance Issues

3.3. Market Opportunities

- 3.3.1. Integration of Behavioral Analytics
- 3.3.2. Adoption of Blockchain Technology

CHAPTER 4. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET INDUSTRY ANALYSIS

4.1. Porter's 5 Force Model

- 4.1.1. Bargaining Power of Suppliers
- 4.1.2. Bargaining Power of Buyers
- 4.1.3. Threat of New Entrants
- 4.1.4. Threat of Substitutes
- 4.1.5. Competitive Rivalry
- 4.1.6. Futuristic Approach to Porter's 5 Force Model
- 4.1.7. Porter's 5 Force Impact Analysis

4.2. PESTEL Analysis

- 4.2.1. Political
- 4.2.2. Economical
- 4.2.3. Social
- 4.2.4. Technological
- 4.2.5. Environmental
- 4.2.6. Legal

4.3. Top investment opportunity

4.4. Top winning strategies

4.5. Disruptive Trends

4.6. Industry Expert Perspective

4.7. Analyst Recommendation & Conclusion

CHAPTER 5. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET SIZE & FORECASTS BY SECURITY TYPE 2022-2032

5.1. Segment Dashboard

5.2. Global Cyber Security For Industrial Automation Market: Security Type Revenue Trend Analysis, 2022 & 2032 (USD Billion)

5.2.1. Enterprise Security

5.2.2. SCADA Security (Supervisory Control and Data Acquisition)

5.2.3. Network Security

5.2.4. Device Security

5.2.5. Physical Security

CHAPTER 6. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET SIZE & FORECASTS BY END USE 2022-2032

6.1. Segment Dashboard

6.2. Global Cyber Security For Industrial Automation Market: End Use Revenue Trend Analysis, 2022 & 2032 (USD Billion)

6.2.1. Automotive Manufacturing

6.2.2. Electronics and Telecommunication

6.2.3. Food & Beverage Processing

6.2.4. Pharmaceuticals

6.2.5. Others

CHAPTER 7. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET SIZE & FORECASTS BY TYPE 2022-2032

7.1. Segment Dashboard

7.2. Global Cyber Security For Industrial Automation Market: Type Revenue Trend Analysis, 2022 & 2032 (USD Billion)

7.2.1. Flexible Automation System

7.2.2. Integrated Automation System

7.2.3. Fixed Automation System

7.2.4. Programmable Automation System

CHAPTER 8. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET SIZE & FORECASTS BY TOOLS OR TECHNOLOGIES 2022-2032

8.1. Segment Dashboard

8.2. Global Cyber Security For Industrial Automation Market: Tools or Technologies Revenue Trend Analysis, 2022 & 2032 (USD Billion)

- 8.2.1. Numerical Control (NC) Machine Tools
- 8.2.2. Programmable Logic Controllers (PLCs)
- 8.2.3. Computer Numerical Control (CNC) Systems
- 8.2.4. Industrial Sensors

CHAPTER 9. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET SIZE & FORECASTS BY REGION 2022-2032

9.1. North America Cyber Security For Industrial Automation Market

9.1.1. U.S. Cyber Security For Industrial Automation Market

- 9.1.1.1. Security Type breakdown size & forecasts, 2022-2032
- 9.1.1.2. End Use breakdown size & forecasts, 2022-2032
- 9.1.1.3. Type breakdown size & forecasts, 2022-2032
- 9.1.1.4. Tools or Technologies breakdown size & forecasts, 2022-2032

9.1.2. Canada Cyber Security For Industrial Automation Market

- 9.1.2.1. Security Type breakdown size & forecasts, 2022-2032
- 9.1.2.2. End Use breakdown size & forecasts, 2022-2032
- 9.1.2.3. Type breakdown size & forecasts, 2022-2032
- 9.1.2.4. Tools or Technologies breakdown size & forecasts, 2022-2032

9.2. Europe Cyber Security For Industrial Automation Market

9.2.1. U.K. Cyber Security For Industrial Automation Market

9.2.2. Germany Cyber Security For Industrial Automation Market

9.2.3. France Cyber Security For Industrial Automation Market

9.2.4. Spain Cyber Security For Industrial Automation Market

9.2.5. Italy Cyber Security For Industrial Automation Market

9.2.6. Rest of Europe Cyber Security For Industrial Automation Market

9.3. Asia-Pacific Cyber Security For Industrial Automation Market

9.3.1. China Cyber Security For Industrial Automation Market

9.3.2. India Cyber Security For Industrial Automation Market

9.3.3. Japan Cyber Security For Industrial Automation Market

9.3.4. Australia Cyber Security For Industrial Automation Market

9.3.5. South Korea Cyber Security For Industrial Automation Market

9.3.6. Rest of Asia Pacific Cyber Security For Industrial Automation Market

9.4. Latin America Cyber Security For Industrial Automation Market

9.4.1. Brazil Cyber Security For Industrial Automation Market

9.4.2. Mexico Cyber Security For Industrial Automation Market

9.4.3. Rest of Latin America Cyber Security For Industrial Automation Market

9.5. Middle East & Africa Cyber Security For Industrial Automation Market

9.5.1. Saudi Arabia Cyber Security For Industrial Automation Market

9.5.2. South Africa Cyber Security For Industrial Automation Market

9.5.3. Rest of Middle East & Africa Cyber Security For Industrial Automation Market

CHAPTER 10. COMPETITIVE INTELLIGENCE

10.1. Key Company SWOT Analysis

10.1.1. Company

10.1.2. Company

10.1.3. Company

10.2. Top Market Strategies

10.3. Company Profiles

10.3.1. IBM

10.3.1.1. Key Information

10.3.1.2. Overview

10.3.1.3. Financial (Subject to Data Availability)

10.3.1.4. Product Summary

10.3.1.5. Market Strategies

10.3.2. ABB

10.3.3. Schneider Electric

10.3.4. Honeywell International Inc.

10.3.5. Siemens AG

10.3.6. Microsoft Corporation

10.3.7. Rockwell Automation Inc.

10.3.8. Palo Alto Networks

10.3.9. Cisco Systems, Inc.

10.3.10. Dell Inc.

10.3.11. Dragos Inc.

10.3.12. Fortinet, Inc.

10.3.13. Kaspersky Lab

10.3.14. CyberArk

10.3.15. Check Point Software Technologies Ltd.

CHAPTER 11. RESEARCH PROCESS

11.1. Research Process

11.1.1. Data Mining

11.1.2. Analysis

- 11.1.3. Market Estimation
- 11.1.4. Validation
- 11.1.5. Publishing
- 11.2. Research Attributes

List Of Tables

LIST OF TABLES

- TABLE 1. Global Cyber Security For Industrial Automation market, report scope
- TABLE 2. Global Cyber Security For Industrial Automation market estimates & forecasts by Region 2022-2032 (USD Billion)
- TABLE 3. Global Cyber Security For Industrial Automation market estimates & forecasts by Security Type 2022-2032 (USD Billion)
- TABLE 4. Global Cyber Security For Industrial Automation market estimates & forecasts by End Use 2022-2032 (USD Billion)
- TABLE 5. Global Cyber Security For Industrial Automation market estimates & forecasts by Type 2022-2032 (USD Billion)
- TABLE 6. Global Cyber Security For Industrial Automation market estimates & forecasts by Tools or Technologies 2022-2032 (USD Billion)
- TABLE 7. Global Cyber Security For Industrial Automation market by segment, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 8. Global Cyber Security For Industrial Automation market by region, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 9. Global Cyber Security For Industrial Automation market by segment, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 10. Global Cyber Security For Industrial Automation market by region, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 11. Global Cyber Security For Industrial Automation market by segment, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 12. Global Cyber Security For Industrial Automation market by region, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 13. Global Cyber Security For Industrial Automation market by segment, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 14. Global Cyber Security For Industrial Automation market by region, estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 15. U.S. Cyber Security For Industrial Automation market estimates & forecasts, 2022-2032 (USD Billion)
- TABLE 16. U.S. Cyber Security For Industrial Automation market estimates & forecasts by segment 2022-2032 (USD Billion)
- TABLE 17. U.S. Cyber Security For Industrial Automation market estimates & forecasts by segment 2022-2032 (USD Billion)
- TABLE 18. Canada Cyber Security For Industrial Automation market estimates & forecasts, 2022-2032 (USD Billion)

TABLE 19. Canada Cyber Security For Industrial Automation market estimates & forecasts by segment 2022-2032 (USD Billion)

TABLE 20. Canada Cyber Security For Industrial Automation market estimates & forecasts by segment 2022-2032 (USD Billion)

.....

This list is not complete, final report does contain more than 100 tables. The list may be updated in the final deliverable.

List Of Figures

LIST OF FIGURES

FIG 1. Global Cyber Security For Industrial Automation market, research methodology

FIG 2. Global Cyber Security For Industrial Automation market, market estimation techniques

FIG 3. Global market size estimates & forecast methods.

FIG 4. Global Cyber Security For Industrial Automation market, key trends 2023

FIG 5. Global Cyber Security For Industrial Automation market, growth prospects 2022-2032

FIG 6. Global Cyber Security For Industrial Automation market, porters 5 force model

FIG 7. Global Cyber Security For Industrial Automation market, PESTEL analysis

FIG 8. Global Cyber Security For Industrial Automation market, value chain analysis

FIG 9. Global Cyber Security For Industrial Automation market by segment, 2022 & 2032 (USD Billion)

FIG 10. Global Cyber Security For Industrial Automation market by segment, 2022 & 2032 (USD Billion)

FIG 11. Global Cyber Security For Industrial Automation market by segment, 2022 & 2032 (USD Billion)

FIG 12. Global Cyber Security For Industrial Automation market by segment, 2022 & 2032 (USD Billion)

FIG 13. Global Cyber Security For Industrial Automation market by segment, 2022 & 2032 (USD Billion)

FIG 14. Global Cyber Security For Industrial Automation market, regional snapshot 2022 & 2032

FIG 15. North America Cyber Security For Industrial Automation market 2022 & 2032 (USD Billion)

FIG 16. Europe Cyber Security For Industrial Automation market 2022 & 2032 (USD Billion)

FIG 17. Asia pacific Cyber Security For Industrial Automation market 2022 & 2032 (USD Billion)

FIG 18. Latin America Cyber Security For Industrial Automation market 2022 & 2032 (USD Billion)

FIG 19. Middle East & Africa Cyber Security For Industrial Automation market 2022 & 2032 (USD Billion)

FIG 20. Global Cyber Security For Industrial Automation market, company market share analysis (2023)

.....

This list is not complete, final report does contain more than 50 figures. The list may be updated in the final deliverable.

I would like to order

Product name: Global Cyber Security For Industrial Automation Market Size study, by Security Type (Enterprise Security, SCADA Security, Network Security, Device Security, Physical Security), by End Use (Automotive Manufacturing, Electronics and Telecommunication, Food & Beverage Processing, Pharmaceuticals, Others), by Type (Flexible Automation System, Integrated Automation System, Fixed Automation System, Programmable Automation System), by Tools or Technologies (Numerical Control (NC) Machine Tools, Programmable Logic Controllers (PLCs), Computer Numerical Control (CNC) Systems, Industrial Sensors) and Regional Forecasts 2022-2032

Product link: <https://marketpublishers.com/r/G5BCAD149843EN.html>

Price: US\$ 4,950.00 (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/G5BCAD149843EN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:

Last name:

Email:

Company:

Address:

City:

Zip code:

Country:

Tel:

Fax:

Your message:

****All fields are required**

Customer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970