+44 20 8123 2220
info@marketpublishers.com

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

+44 20 8123 2220
info@marketpublishers.com

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.

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

CHAPTER 3. GLOBAL CYBER SECURITY FOR INDUSTRIAL AUTOMATION MARKET DYNAMICS

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

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

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

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

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

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+44 20 8123 2220
info@marketpublishers.com

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

+44 20 8123 2220
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

+44 20 8123 2220
info@marketpublishers.com

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

+44 20 8123 2220
info@marketpublishers.com

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

Custumer signature _____

+44 20 8123 2220
info@marketpublishers.com

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