Cyber Security For Industrial Automation Market to Grow at a CAGR of 8.7% and will Reach USD 20.5 billion by 2032

Rising cyber threats and tech advances in industrial automation will boost global cybersecurity market growth, led by Asia-Pacific by 2032.

Cyber Security For Industrial Automation Market Size

WILMINGTON, DE, UNITED STATES, July 23, 2025 /EINPresswire.com/ -- Cybersecurity for industrial automation implements a set of practices, tools, and technologies to protect the industrial systems, data, and network from cyber threats such as ransomware, malicious software's, emails, data breach, and others. Industrial automation, which is quite popular across industries namely automotive, pharmaceutical, food & beverage, and others involves the use of control systems, sensors, and other devices for managing the industrial processes. Furthermore, the integration of digital technologies and advanced connectivity has led to increase in cyber threats and related vulnerabilities that can expose the crucial data. In such cases, cyber security for industrial automation plays a major role in protecting the critical infrastructure present in industrial units as well as preventing unauthorized access, data breaches, and cyber threats.

Request Sample Report (Get Full Insights in PDF - 320 Pages) at:
https://www.alliedmarketresearch.com/request-sample/A289338

Cyber security in industrial automation implements set of measures such as network security, encryption, endpoint security, access control, regulatory compliance, physical security, and others to prevent cyber-attacks. For instance, in network security, the trained cyber security professionals implement firewalls, virtual private networks (VPNs), intrusion detection & prevention systems, and others to ensure network security. Cybersecurity for access control restricts or manages access to critical systems and data via various authorization mechanisms, authentication, and role-based access control. In addition, the end-point security is quite popular in the automotive and food & beverage sectors as it helps in securing individual devices, programmable logic controllers, and other devices.

According to the report, the global cyber security for industrial automation market generated $9 billion in 2022, and is anticipated to generate $20.5 billion by 2032, rising at a CAGR of 8.7% from 2023 to 2032.

The rising popularity of cyber security in detecting & responding to cyber threats, increased number of cyber threats, and the stringent regulations & standards mandating the implementation of cybersecurity in industrial automation are the factors expected to drive the growth of the global cyber security for industrial automation market in the forecast period from 2023 to 2032. However, the lack of expertise & skilled professionals and the outdated legacy systems and compliance issues may hamper market growth in the coming future.

On the contrary, the adoption of novel technologies in the industrial automation sector and the growing focus on cyber resilience and the development of incident response plans & business continuity are expected to offer remunerative opportunities for the expansion of the cyber security for industrial automation market during the forecast period.

Buy Now & Get Exclusive Report at: https://www.alliedmarketresearch.com/cyber-security-for-industrial-automation-market/purchase-options

COVID-19 Scenario

1. The COVID-19 pandemic outbreak had a significant impact on the global cyber security for industrial automation market's growth. The pandemic led to disruptions in global supply chains due to lockdowns, reduced manufacturing activities, and restrictions on international trade. These disruptions led to remote work culture that exposed several industries to cyber threats by compromising network security and leading to data breaches.

2. Moreover, industrial automation systems emerged as prime targets for cybercriminals amidst the COVID-19 pandemic, aiming to exploit vulnerabilities amid heightened dependence on digital technologies. Additionally, disruptions in global supply chains caused by the pandemic prompted greater scrutiny of supply chain security processes.

The SCADA security (Supervisory Control and Data Acquisition) sub-segment accounted for the largest global cyber security for industrial automation market share of 28.5% in 2022 and is expected to grow at the highest CAGR of 9.4% during the forecast period. This is majorly because SCADA systems play a crucial role in industrial automation by providing remote monitoring and control capabilities. The rising need to protect critical processes from cyber threats is another factor to boost the sub-segment's growth. Besides, SCADA's capability for efficient centralized process control is driving the demand for cyber security in industrial automation.

The food & beverage processing sub-segment accounted for the largest market share of 34.4% in 2022 and is expected to rise at the highest CAGR of 9.3% during the forecast period. This is

mainly because the food & beverage industry depends heavily on computer-controlled automation systems for its productivity. Besides, cybersecurity measures are significant to prevent downtime caused by cyberattacks. Moreover, in the food & beverage industry, intellectual property, such as formulations, proprietary recipes, and processes, is a valuable asset. A major factor to protect this intellectual property from unauthorized access or theft is cybersecurity.

If you have any special requirements, Request customization:
https://www.alliedmarketresearch.com/request-for-customization/A289338

The programmable automation system sub-segment of the global market accounted for the highest share of 35.6% in 2022 and is projected to continue to maintain its dominance in terms of market share during the forecast period. This is primarily because the programmable automation systems offer a high degree of flexibility and adaptability in manufacturing processes. Besides, the nature of programmable automation systems is well-suited for batch production processes, especially in industries producing similar items using the same automated steps and tools. Furthermore, the programmable automation systems enable the seamless implementation of new processes through modification of the control program.

The programmable logic controllers (PLCs) sub-segment of the global market accounted for the largest cyber security for industrial automation market share of 32.6% in 2022 and is anticipated to rise at the highest CAGR of 9.5% by 2032. This is primarily owing to the efficient adaptation to evolving cybersecurity requirements offered by the flexibility of programmable logic controllers (PLCs) in industrial automation. Besides, PLCs offer robust operation and enhanced reliability compared to traditional relay-based control systems. The design of PLCs to operate in harsh industrial environments, along with built-in protection against temperature extremes, electrical noise, and dependable performance, ensures dependable and consistent performance.

The cyber security for industrial automation market in the Asia-Pacific region accounted for the largest share of 38.2% in 2022 and is predicted to rise at the highest CAGR of 9.2% during the forecast period. This growth is mainly owing to the significant rise in cyber threats. Besides, the rapid digitalization, geopolitical tensions, and the increased Internet penetration are other factors driving the regional market growth. Moreover, several countries in the Asia-Pacific region, such as India, South Korea, Japan, China, and others are actively pursuing digital transformation initiatives to enhance the productivity and efficiency of industrial processes.

Cybersecurity for industrial automation industry has witnessed significant technological advancements in the recent years. This includes the development of zero trust architecture that offers a proactive approach to address the cyber threats and growing emphasis on endpoint security to ensure data integrity & prevent unauthorized access. Also, the cloud-based security solutions and the implementation of artificial intelligence (AI) and machine learning (ML) in the industrial automation for analyzing the anomalies and potential security threats are being widely adopted.

Get More Information Before Buying: https://www.alliedmarketresearch.com/purchase-enquiry/A289338

Leading Players in the Cyber Security for Industrial Automation Market:

Microsoft Corporation
Siemens AG
Cisco Systems, Inc.
ABB
Dell Inc.
Schneider Electric
Honeywell International Inc.
IBM
Rockwell Automation Inc.
Palo Alto Networks, Inc.

The report provides a detailed analysis of the key players of the global cyber security for industrial automation market. These players have adopted different strategies, such as new product launches, collaborations, expansion, joint ventures, agreements, and others to increase their market share and maintain their dominance in different regions. The report is valuable in highlighting business performance, operating segments, product portfolio, and strategic moves of market players to showcase the competitive scenario.

Other Trending Report:

1. Content Moderation Services Market
https://www.alliedmarketresearch.com/content-moderation-services-market-A31650

2. Surface & Field Analytics Market
https://www.alliedmarketresearch.com/surface-&-field-analytics-market-A31577

3. Network and Location Analytics Market
https://www.alliedmarketresearch.com/network-and-location-analytics-market-A31571

About Us:

Allied Market Research (AMR) is a full-service market research and business-consulting wing of Allied Analytics LLP, based in Portland, Oregon. AMR provides global enterprises as well as medium and small businesses with unmatched quality "Market Research Reports" and "Business Intelligence Solutions." AMR has a targeted view of providing business insights and consulting to assist its clients in making strategic business decisions and achieving sustainable growth in their respective market domains.

AMR launched its user-based online library of reports and company profiles, on Avenue. An e-access library is accessible from any device, anywhere, and at any time for entrepreneurs, stakeholders, researchers, and students at universities. With reports on more than 60,000 niche markets with data comprising 600,000 pages along with company profiles on more than 12,000 firms, Avenue offers access to the entire repository of information through subscriptions. A hassle-free solution to clients' requirements is complemented with analyst support and customization requests.

Contact:
David Correa
1209 Orange Street,
Corporation Trust Center,
Wilmington, New Castle,
Delaware 19801 USA.
Int'l: +1-503-894-6022
Toll Free: + 1-800-792-5285
UK: +44-845-528-1300
India (Pune): +91-20-66346060
Fax: +1-800-792-5285
help@alliedmarketresearch.com

David Correa
Allied Market Research
+ 1 800-792-5285
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
