

Jam-packed Opportunities for Investors | Cyber Security for Industrial Automation Market Reach USD 20.5 Billion by 2032

The integration of new technologies in industrial automation sector such as behavioral analytics and blockchain to generate market growth.

PORTLAND, PORTLAND, OR, UNITED STATE, August 26, 2024

/EINPresswire.com/ -- Allied Market Research published a new report, titled, "Jam-packed Opportunities for Investors | [Cyber Security for Industrial Automation Market](#) Reach USD 20.5 Billion by 2032." The report offers an

extensive analysis of key growth strategies, drivers, opportunities, key segment, Porter's Five Forces analysis, and competitive landscape. This study is a helpful source of information for market players, investors, VPs, stakeholders, and new entrants to gain thorough understanding of the industry and determine steps to be taken to gain competitive advantage.

The global cyber security for industrial automation market size was valued at USD 9 billion in 2022, and is projected to reach USD 20.5 billion by 2032, growing at a CAGR of 8.7% from 2023 to 2032.

Request Sample Report (Get Full Insights in PDF - 320 Pages) at:

<https://www.alliedmarketresearch.com/request-sample/A289338>

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. 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 market growth.



The cyber security for industrial automation market is segmented on the basis of type, tools or technologies, security type, end use, and region. By type, the market is divided into fixed automation system, programmable automation system, flexible automation system, and integrated automation system. By tools or technologies, the market is classified into numerical control (NC) machine tools, programmable logic controllers (PLCs), computer numerical control (CNC) systems, and industrial sensors. By security type, the market is analyzed across enterprise security, SCADA security (supervisory control and data acquisition), network security, device security, and physical security. By end use, the market is classified into automotive manufacturing, electronics & telecommunication, food & beverage processing, pharmaceuticals, and others. By region, the market is analyzed across North America, Europe, Asia-Pacific, and LAMEA.

If you have any questions, Please feel free to contact our analyst at:
<https://www.alliedmarketresearch.com/connect-to-analyst/A289338>

COVID-19 Scenario

□ 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.

□ 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.

Enquiry Before Buying: <https://www.alliedmarketresearch.com/purchase-enquiry/A289338>

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.

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.

The key players profiled in the cyber security for industrial automation market analysis report include IBM, ABB, Schneider Electric, Honeywell International Inc., Siemens AG, Microsoft Corporation, Rockwell Automation Inc., Palo Alto Networks, Cisco Systems, Inc., and Dell Inc.

Buy Now & Get Exclusive Discount on this Report (320 Pages PDF with Insights, Charts, Tables, and Figures) at: <https://www.alliedmarketresearch.com/cyber-security-for-industrial-automation-market/purchase-options>

Thanks for reading this article, you can also get an individual chapter-wise section or region-wise report versions like North America, Europe, or Asia.

If you have any special requirements, please let us know and we will offer you the report as per your requirements.

Lastly, this report provides market intelligence most comprehensively. The report structure has been kept such that it offers maximum business value. It provides critical insights into the market dynamics and will enable strategic decision-making for the existing market players as well as those willing to enter the market.

About Us:

Allied Market Research (AMR) is a market research and business-consulting firm of Allied Analytics LLP, based in Portland, Oregon. AMR offers market research reports, business solutions, consulting services, and insights on markets across 11 industry verticals. Adopting extensive research methodologies, AMR is instrumental in helping its clients to make strategic business decisions and achieve sustainable growth in their market domains. We are equipped with skilled analysts and experts and have a wide experience of working with many Fortune 500 companies and small & medium enterprises.

Pawan Kumar, the CEO of Allied Market Research, is leading the organization toward providing high-quality data and insights. We are in professional corporate relations with various

companies. This helps us dig out market data that helps us generate accurate research data tables and confirm utmost accuracy in our market forecasting. Every data company in the domain is concerned. Our secondary data procurement methodology includes deep presented in the reports published by us is extracted through primary interviews with top officials from leading online and offline research and discussion with knowledgeable professionals and analysts in the industry.

David Correa

Allied Market Research

+1 800-792-5285

[email us here](#)

Visit us on social media:

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/738379931>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.