+44 20 8123 2220
info@marketpublishers.com

Industrial Control Systems Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution, Service), By Security (Network Security, Application Security, Endpoint Security, Database Security), By System (Supervisory Control & Data Acquisition System, Distributed Control System, Programmable Logic Controller, Machine Execution System (MES), Product Lifecycle Management (PLM), Enterprise Resource Planning (ERP), Human Machine Interface (HMI), Others), By End User (Automotive, Chemical & Petrochemical, Oil & Gas, Utilities, Pharmaceutical, Food & Beverage, Others), By Region, and By Competition, 2019-2029F

https://marketpublishers.com/r/IDB649131906EN.html
Date: April 2024
Pages: 185
Price: US$ 4,900.00 (Single User License)
ID: IDB649131906EN

Abstracts

The Global Industrial Control Systems (ICS) Security Market was valued at USD 17.36 billion in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 7.59% through 2029.The Global Industrial Control Systems (ICS) Security Market is witnessing robust growth driven by the escalating threat landscape, technological advancements, and the critical importance of securing industrial processes. With industries increasingly digitizing their operations and relying on interconnected systems, the demand for comprehensive ICS security solutions is at an all-time high. Key drivers include the growing frequency of cyber threats to critical

+44 20 8123 2220
info@marketpublishers.com

infrastructure, the rapid adoption of Industrial Internet of Things (IIoT) technologies, and regulatory mandates emphasizing cybersecurity compliance. Network Security emerges as a dominant segment, playing a pivotal role in safeguarding interconnected industrial environments. The Oil Gas sector stands out as a significant end-user, given its strategic importance, expansive infrastructure, and vulnerability to cyber threats. While ICS security solutions, such as advanced threat detection and artificial intelligence integration, address evolving challenges, the market faces obstacles like integration of legacy systems, limited awareness, and resource constraints. The global landscape is shaped by North America's leadership, driven by its developed critical infrastructure, proactive regulatory environment, and concentration of cybersecurity expertise. As industries navigate the complexities of securing industrial control systems, the ICS Security market is poised for sustained growth, fueling innovations to counter the dynamic cyber threat landscape.

Key Market Drivers

Increasing Cyber Threats to Critical Infrastructure:

A primary driver in the global Industrial Control Systems (ICS) Security market is the escalating frequency and sophistication of cyber threats targeting critical infrastructure. With industries becoming more digitized and interconnected, the vulnerabilities of industrial control systems have become prominent targets for malicious actors. High-profile cyber-attacks on critical infrastructure, such as power grids, water treatment facilities, and manufacturing plants, have underscored the urgency of bolstering ICS security. This driver compels organizations to invest in robust cybersecurity solutions to safeguard against cyber threats that could have severe consequences on public safety, economic stability, and national security.

Rapid Adoption of Industrial Internet of Things (IIoT) Technologies:

The rapid adoption of Industrial Internet of Things (IIoT) technologies serves as a significant driver propelling the ICS Security market. As industries embrace digital transformation, the integration of smart sensors, connected devices, and data analytics in industrial environments enhances operational efficiency but also introduces new cyber risks. The proliferation of IIoT devices expands the attack surface, necessitating comprehensive security measures to protect against unauthorized access, data breaches, and potential disruptions to critical processes. Security solutions that cater to the unique challenges of securing IIoT ecosystems become crucial drivers for the ICS Security market's growth.

+44 20 8123 2220
info@marketpublishers.com

Regulatory Mandates and Compliance Requirements:

The increasing focus on regulatory mandates and compliance requirements is a key driver shaping the ICS Security market. Governments and regulatory bodies worldwide are enacting stringent cybersecurity regulations to ensure the protection of critical infrastructure. Compliance frameworks such as NIST, ISA/IEC 62443, and regional cybersecurity standards mandate organizations to implement robust security measures for industrial control systems. This driver compels industries to invest in cybersecurity solutions that align with regulatory requirements, fostering a proactive approach to mitigating cyber risks and ensuring adherence to established standards.

Growing Awareness of Industrial Cybersecurity Risks:

A notable driver influencing the ICS Security market is the growing awareness of industrial cybersecurity risks among organizations and industry stakeholders. High-profile cyber-attacks on industrial facilities have heightened awareness regarding the potential consequences of inadequate cybersecurity measures. This increased awareness prompts organizations to prioritize cybersecurity initiatives, invest in advanced security technologies, and conduct comprehensive risk assessments. The recognition of the interconnected nature of cyber and physical risks amplifies the demand for ICS security solutions that provide holistic protection against evolving threats.

Integration of Artificial Intelligence (AI) and Machine Learning (ML):

The integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies serves as a driving force in the evolution of the ICS Security market. AI and ML empower security solutions to enhance threat detection, anomaly identification, and predictive analytics in real-time. These technologies enable ICS security systems to adapt and respond dynamically to emerging cyber threats. The ability of AI and ML to analyze vast datasets and recognize patterns contributes to the development of proactive and intelligent cybersecurity measures. This driver reflects a shift towards more sophisticated, adaptive security solutions that can effectively counter evolving cyber threats in industrial environments.

Key Market Challenges

Evolving and Sophisticated Cyber Threats:

+44 20 8123 2220
info@marketpublishers.com

The global Industrial Control Systems (ICS) Security market faces a formidable challenge in the form of evolving and sophisticated cyber threats. Cyber adversaries continually adapt their tactics, techniques, and procedures to exploit vulnerabilities in industrial control systems. This challenge necessitates a proactive and adaptive security posture to effectively counter emerging threats. Organizations must stay ahead of cybercriminals by implementing advanced threat intelligence, continuous monitoring, and robust cybersecurity measures that can evolve in tandem with the dynamic threat landscape.

Integration of Legacy Systems and New Technologies:

A significant challenge in the ICS Security market stems from the integration of legacy systems with new technologies. Many industrial environments still rely on legacy control systems that were not originally designed with cybersecurity in mind. The coexistence of these legacy systems with modern technologies, such as the Industrial Internet of Things (IIoT) and cloud computing, creates a complex security landscape. Bridging the gap between old and new systems poses challenges in terms of interoperability, security updates, and ensuring that security measures are uniformly applied across diverse technologies within industrial control environments.

Lack of Standardization and Interoperability:

The absence of standardization and interoperability poses a considerable challenge in the ICS Security market. Industrial control systems vary widely across industries, and the lack of standardized security protocols complicates efforts to implement consistent cybersecurity measures. This challenge is further exacerbated by the diversity of vendors and the proprietary nature of some control systems. The industry needs concerted efforts to establish common standards, ensuring interoperability between different ICS components and facilitating the implementation of robust, standardized security measures across the spectrum.

Limited Security Awareness and Training:

An ongoing challenge in the ICS Security market revolves around the limited security awareness and training among personnel responsible for managing and operating industrial control systems. Human error remains a significant contributor to cybersecurity incidents, emphasizing the importance of cultivating a cybersecurity-aware culture within organizations. Addressing this challenge requires comprehensive

training programs, awareness campaigns, and skill-building initiatives for employees, engineers, and operators to recognize and respond to security threats effectively. Bridging the gap in security knowledge within the industrial workforce is critical for establishing a strong defense against cyber threats.

Resource Constraints and Budgetary Limitations:

Resource constraints and budgetary limitations represent a pervasive challenge in the ICS Security market. Organizations often face the dilemma of allocating limited resources to cybersecurity initiatives while balancing other operational priorities. The implementation of robust security measures, regular security assessments, and the deployment of advanced technologies require significant financial investments. This challenge is especially pronounced in critical infrastructure sectors, where aging systems and limited budgets may hinder the timely adoption of comprehensive cybersecurity measures. Overcoming resource constraints involves strategic planning, risk assessment, and advocacy for increased investment in ICS security to safeguard critical infrastructure against cyber threats.

Key Market Trends

Growing Threat Landscape and Focus on Cybersecurity:

The global Industrial Control Systems (ICS) Security market is witnessing a significant trend marked by the growing threat landscape targeting critical infrastructure. As industrial systems become more interconnected, cyber threats pose substantial risks to the stability and safety of essential sectors. This trend is driving increased investments in ICS security solutions, with organizations recognizing the need to fortify their systems against cyber-attacks. The focus on cybersecurity encompasses advanced threat detection, incident response, and the development of resilient architectures to safeguard critical industrial processes.

Rise of IIoT and Convergence of IT/OT Networks:

The trend of the Industrial Internet of Things (IIoT) is reshaping the ICS Security market. The convergence of Information Technology (IT) and Operational Technology (OT) networks introduces new complexities and vulnerabilities. As industries embrace digital transformation, the integration of sensors, devices, and smart technologies creates a broader attack surface. ICS security trends are adapting to address these challenges, emphasizing the need for robust security measures that extend from traditional OT

+44 20 8123 2220
info@marketpublishers.com

environments to interconnected IT/OT networks. Solutions encompass secure edge computing, network segmentation, and comprehensive risk assessments to manage the evolving threat landscape.

Regulatory Compliance and Industry Standards:

Regulatory compliance and adherence to industry standards are becoming integral to the ICS Security landscape. Governments and regulatory bodies globally are recognizing the critical importance of securing industrial control systems, leading to the development and enforcement of stringent cybersecurity regulations. This trend is driving organizations to align their security practices with established standards such as NIST, ISA/IEC 62443, and others. Compliance frameworks guide the implementation of robust security measures, ensuring a standardized approach to ICS security across various industries.

Advanced Threat Detection and Incident Response:

The market trend in ICS security emphasizes the need for advanced threat detection and efficient incident response capabilities. Traditional security measures are evolving to incorporate Artificial Intelligence (AI) and Machine Learning (ML) technologies to detect sophisticated cyber threats. The ability to swiftly respond to incidents and minimize the impact on critical industrial processes is crucial. Security solutions are integrating real-time monitoring, anomaly detection, and automated incident response mechanisms to fortify ICS environments against both known and emerging cyber threats.

Collaboration and Information Sharing:

The trend of collaboration and information sharing is gaining prominence in the ICS Security market. Recognizing the collective challenge of securing critical infrastructure, industries are fostering collaboration between public and private sectors. Information sharing platforms, threat intelligence exchanges, and collaborative initiatives facilitate the dissemination of cybersecurity insights and best practices. This trend enhances the collective defense against cyber threats by creating a community-driven approach to ICS security. Collaborative efforts extend beyond individual organizations to industry consortiums, enabling the sharing of threat intelligence and the development of unified strategies to mitigate evolving cyber risks in the industrial sector.

Segmental Insights

+44 20 8123 2220
info@marketpublishers.com

Component Insights

Solution segmentdominates in the global industrial control systems security market in 2023.ICS security solutions are tailored to address the unique challenges posed by industrial environments, including the integration of advanced threat detection, anomaly identification, and real-time monitoring capabilities. These solutions provide a robust defense mechanism against cyber threats that target industrial control systems, such as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. The Solution segment includes technologies such as firewalls, intrusion detection systems, secure remote access solutions, and encryption protocols specifically designed to safeguard the integrity and availability of industrial processes.

The dominance of the Solution segment is further accentuated by the continual evolution of cyber threats that necessitate sophisticated and adaptive security measures. Industrial environments are increasingly exposed to advanced persistent threats, ransomware attacks, and other cyber-attacks that demand innovative solutions for timely detection and mitigation. ICS security solutions, rooted in advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML), enable proactive threat identification, enabling organizations to stay ahead of emerging cyber risks.

Moreover, the significance of the Solution segment lies in its capacity to provide a holistic and integrated approach to ICS security. These solutions are often tailored to address the specific needs of industrial sectors, offering a unified platform that encompasses threat intelligence, incident response, and vulnerability management. The Solution segment empowers organizations to create a robust security posture that aligns with industry standards and compliance requirements, ensuring a comprehensive and standardized approach to securing industrial control systems.

While the Service segment, which includes offerings such as consulting, risk assessments, and managed security services, plays a vital role in complementing the implementation and optimization of ICS security solutions, it is the Solution segment that forms the foundational technology backbone driving the market's growth. The increasing complexity of cyber threats, coupled with the imperative to secure critical infrastructure, positions ICS security solutions as indispensable assets for organizations across diverse industrial sectors. As the global reliance on industrial control systems continues to grow, the dominance of the Solution segment is expected to persist, catalyzing innovations and advancements that fortify industrial environments against the ever-evolving landscape of cyber threats.

+44 20 8123 2220
info@marketpublishers.com

Security Insights

Network Security segmentdominates in the global industrial control systems security market in 2023.The dominance of Network Security within the ICS Security market is rooted in its overarching responsibility to protect the critical communication networks that underpin industrial processes. As industries increasingly embrace digital transformation and the Industrial Internet of Things (IIoT), the reliance on interconnected networks becomes more pronounced. Network Security, therefore, takes center stage in defending these communication channels against unauthorized access, cyber intrusions, and potential disruptions to industrial control systems.

Network Security encompasses a suite of technologies and protocols specifically designed to secure the network infrastructure within industrial environments. This includes robust firewalls, intrusion detection and prevention systems, Virtual Private Networks (VPNs), and secure communication protocols tailored to the unique requirements of industrial control systems. These technologies collectively form a formidable barrier against cyber threats, ensuring the integrity, confidentiality, and availability of data flowing across the industrial network.

The dominance of Network Security is further accentuated by its role in addressing the distinctive challenges posed by industrial control environments. With the integration of legacy systems, smart devices, and remote access capabilities, industrial networks become increasingly complex and susceptible to cyber risks. Network Security solutions are specifically engineered to provide granular control over network traffic, monitor for anomalies, and enforce access policies critical for protecting the underlying industrial control infrastructure.

Moreover, the emphasis on Network Security aligns with the broader industry focus on securing the perimeter of industrial networks. As cyber threats continue to evolve, network-centric security measures become paramount in preventing unauthorized access to critical components such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS). The robustness of Network Security solutions is crucial for maintaining the continuous and secure operation of industrial processes, minimizing the risk of disruptions and ensuring the reliability of critical infrastructure.

Regional Insights

+44 20 8123 2220
info@marketpublishers.com

North Americadominates the Global Industrial Control Systems Security Market in 2023.North America boasts a highly developed industrial landscape with a vast and interconnected critical infrastructure. The region hosts numerous key industries, including energy, manufacturing, and utilities, which heavily rely on industrial control systems. The criticality of these sectors makes them primary targets for cyber threats, driving a heightened focus on securing industrial control systems. Consequently, organizations in North America are more inclined to invest significantly in advanced ICS security solutions to protect their critical infrastructure.

United States, in particular, has been proactive in establishing stringent cybersecurity regulations and standards. Regulatory bodies such as the National Institute of Standards and Technology (NIST) have played a crucial role in shaping cybersecurity frameworks, including guidelines specifically tailored for ICS security (e.g., NIST SP 800-82). The emphasis on compliance and adherence to these standards encourages organizations to prioritize cybersecurity measures, contributing to the overall dominance of North America in the ICS Security Market.

North America is home to a multitude of cybersecurity companies, research institutions, and technology hubs, including Silicon Valley. The concentration of expertise and innovation in the region fosters the development of cutting-edge ICS security solutions. These solutions often leverage emerging technologies like Artificial Intelligence (AI) and Machine Learning (ML) to provide advanced threat detection and response capabilities. The robust ecosystem of cybersecurity professionals and technological innovators positions North America as a global leader in shaping the direction of ICS security solutions.

The awareness of the evolving cybersecurity landscape and the increasing sophistication of cyber threats is notably high in North America. Organizations in the region are quick to adopt and implement the latest security measures to stay ahead of potential risks. This proactive stance, coupled with a willingness to invest in cybersecurity infrastructure, further solidifies North America's dominance in the ICS Security Market.

Recent Developments

In March 2023,With devices like the FortiGate 70F Rugged NGFW, FortiDeceptor Rugged 100G breach detection device, FortiPAM Privileged Access Management, and FortiSIEM upgrades, Fortinet Inc. increased the scope of its OT security solutions. These solutions combine threat analysis tools with real-time reaction and privileged

+44 20 8123 2220
info@marketpublishers.com

access management to strengthen OT defense.

In May 2023,In order to provide the manufacturing, electric utility, and transportation sectors with a reliable Zero Trust OT Security Solution, Wipro and Palo Alto Networks expanded their collaboration.

In December 2022,Dragos and Cisco collaborated to improve cybersecurity for industrial networks. Their integrated solution strengthens security against changing threats by combining the Dragos Platform with Cisco ASA firewalls to provide comprehensive visibility, threat prevention, and compliance for IT and OT environments.

In November 2022,Advanced Monitoring and Incident Response (AMIR), a complete cybersecurity solution for industrial control systems, was introduced by Honeywell. By utilizing Honeywell's proficiency in security and automation, AMIR improves security monitoring, incident response, and threat identification.

In September 2022, Dragos and Palo Alto Networks collaborated to include the Dragos Platform. Customers working together will benefit from its proactive assistance in thwarting unforeseen cybersecurity threats that affect IT and OT settings.

Key Market Players

IBM Corporation

Cisco Systems Inc.

Honeywell International Inc.

Broadcom Inc.

Rockwell Automation Inc.

Palo Alto Networks, Inc.

BAE Systems plc.

Raytheon Technologies Corporation

Trellix Corporation

+44 20 8123 2220
info@marketpublishers.com

Check Point Software Technologies Ltd.

Report Scope:

In this report, the Global Industrial Control Systems Security Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Industrial Control Systems Security Market,By Component:

oSolution

oService

Industrial Control Systems Security Market,By Security:

oNetwork Security

oApplication Security

oEndpoint Security

oDatabase Security

Industrial Control Systems Security Market,By System:

oSupervisory Control Data Acquisition System

oDistributed Control System

oProgrammable Logic Controller

oMachine Execution System (MES)

oProduct Lifecycle Management (PLM)

oEnterprise Resource Planning (ERP)

+44 20 8123 2220
info@marketpublishers.com

oHuman Machine Interface (HMI)

oOthers

Industrial Control Systems Security Market,By End User:

oAutomotive

oChemical Petrochemical

oOil Gas

oUtilities

oPharmaceutical

oFood Beverage

oOthers

Industrial Control Systems Security Market, By Region:

oNorth America

United States

Canada

Mexico

oEurope

Germany

France

United Kingdom

+44 20 8123 2220
info@marketpublishers.com

Italy

Spain

oSouth America

Brazil

Argentina

Colombia

oAsia-Pacific

China

India

Japan

South Korea

Australia

oMiddle East Africa

Saudi Arabia

UAE

South Africa

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global

+44 20 8123 2220
info@marketpublishers.com

Industrial Control Systems Security Market.

Available Customizations:

Global Industrial Control Systems Security Market report with the given market data, Tech Sci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

6.NORTH AMERICA INDUSTRIAL CONTROL SYSTEMS SECURITY MARKETOUTLOOK

+44 20 8123 2220
info@marketpublishers.com

7.EUROPE INDUSTRIAL CONTROL SYSTEMS SECURITY MARKETOUTLOOK

+44 20 8123 2220
info@marketpublishers.com

8.SOUTH AMERICA INDUSTRIAL CONTROL SYSTEMS SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

9.MIDDLE EAST AFRICA INDUSTRIAL CONTROL SYSTEMS SECURITY MARKETOUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10.ASIA PACIFIC INDUSTRIAL CONTROL SYSTEMS SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Industrial Control Systems Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution, Service), By Security (Network Security, Application Security, Endpoint Security, Database Security), By System (Supervisory Control & Data Acquisition System, Distributed Control System, Programmable Logic Controller, Machine Execution System (MES), Product Lifecycle Management (PLM), Enterprise Resource Planning (ERP), Human Machine Interface (HMI), Others), By End User (Automotive, Chemical & Petrochemical, Oil & Gas, Utilities, Pharmaceutical, Food & Beverage, Others), By Region, and By Competition, 2019-2029F

Product link: https://marketpublishers.com/r/IDB649131906EN.html

Price: US$ 4,900.00 (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/IDB649131906EN.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