Industrial Cybersecurity Market Report: USD 15.84 Billion Valuation in 2019 to USD 51.58 Billion by 2032 at 8.9% CAGR

Key Companies covered in helicopter market are Honeywell International Inc., Microsoft Corporation, Siemens AG, IBM Corporation, ABB Ltd., & others.

PUNE, MAHARASHTRA, INDIA, March 24, 2025 /EINPresswire.com/ -- Market Overview

Industrial Cybersecurity Market 2032

The global Industrial Cybersecurity Market was valued at USD 15.84 billion in 2019 and is anticipated to expand to USD 51.58 billion by 2032, reflecting a robust compound annual growth rate (CAGR) of 8.9% during the forecast period. The increasing digitization of industrial operations combined with the growing frequency and sophistication of cyberattacks on critical infrastructure is driving significant investment in cybersecurity solutions. North America currently leads the market, with a strong presence in both public and private sectors due to advanced industrial infrastructure and stringent regulatory mandates.

> "The U.S. industrial cybersecurity market is set for significant growth, expected to reach USD 9.49 billion by 2032, driven by rising government demand for cybersecurity products."
> *Fortune Business Insights*

Market Highlights:

• Rapid Digital Transformation: Industrial facilities are increasingly adopting automation and IoT, making cybersecurity a critical priority.
• Heightened Threat Landscape: Rising cyber threats, including ransomware and advanced persistent threats (APTs), are pushing industries to invest in proactive defense mechanisms.
• Regulatory Compliance: Governments worldwide are mandating robust cybersecurity measures to protect critical infrastructure, further bolstering market growth.

Get a Free Sample Research Report:
https://www.fortunebusinessinsights.com/enquiry/sample/industrial-cybersecurity-market-104557

Key Companies Covered in the Industrial Cybersecurity Market

- IBM Corporation (New York, United States)
- ABB Ltd. (Switzerland)
- Check Point Software Technologies Ltd. (Israel)
- Schneider Electric (Rueil-Malmaison, France)
- Mcafee, LLc (Intel Security) (California, United States)
- Cisco Systems, Inc. (California, United States)
- Honeywell International Inc. (North Carolina, United States)
- Microsoft Corporation (Washington, United States)
- Siemens AG (Munich, Germany)
- Trend Micro, Inc. (Tokyo, Japan)
- Splunk Inc. (California, United States)
- Rockwell Automation, Inc. (Wisconsin, United States)
- Bayshore Networks, Inc. (North Carolina, United States)
- Broadcom Inc. (California, United States)
- Kaspersky Lab (Moscow, Russia)
- Dell Inc. (Texas, United States)
- Proofpoint, Inc. (California, United States)
- FireEye, Inc. (California, United States)
- Symantec Corporation (NortonLifeLock Inc.) (Arizona, United States)
- Palo Alto Networks (California, United States)

Segmentation Analysis

By Component

- Hardware: Security appliances such as firewalls and intrusion detection systems tailored for industrial control systems.
- Software: Advanced cybersecurity software including threat detection, endpoint protection, and monitoring tools.
- Services: Consulting, implementation, and managed security services focused on continuous monitoring and threat intelligence.

By Industry Vertical

- Energy & Utilities: Protecting critical infrastructure like power plants and smart grids from cyber intrusions.

• Manufacturing: Securing industrial control systems and automation networks that drive production processes.
• Transportation: Ensuring the cybersecurity of logistics and supply chain operations including rail, road, and air traffic systems.
• Oil & Gas: Safeguarding exploration, production, and distribution networks against cyber threats.
• Others: Sectors such as chemicals, pharmaceuticals, and water treatment facilities are also increasingly adopting industrial cybersecurity solutions.

By Deployment Mode

• On-Premise: Traditional security systems installed within the industrial facility, preferred for critical infrastructure with high customization needs.
• Cloud-Based: Solutions offering scalability and cost-effectiveness, gaining traction among mid-sized industrial operations.

Ask for Customization: https://www.fortunebusinessinsights.com/enquiry/ask-for-customization/industrial-cybersecurity-market-104557

Key Drivers & Restraints

Drivers:

• Evolving Cyber Threats: The escalating number and complexity of cyberattacks on industrial operations necessitate advanced cybersecurity measures.
• Digitalization & IoT Integration: The integration of IoT devices in industrial operations increases vulnerabilities, driving the demand for robust cybersecurity.
• Regulatory Pressures: Stricter compliance requirements across regions are compelling organizations to enhance their cybersecurity frameworks.
Restraints:
• High Implementation Costs: Significant capital investment for deploying and maintaining cybersecurity solutions can be a barrier, especially for small- to medium-sized enterprises.
• Legacy Systems: Many industrial facilities operate with legacy systems that are difficult to integrate with modern cybersecurity technologies.
• Shortage of Skilled Professionals: A lack of cybersecurity expertise can impede the effective implementation and management of cybersecurity measures.

Regional Insights

• North America: Dominates the industrial cybersecurity market with advanced industrial networks and significant investment in cybersecurity infrastructure.
• Europe: Maintains a strong market presence driven by regulatory compliance and the presence of key industry players.

• Asia Pacific: Expected to be the fastest-growing region due to rapid industrialization, increasing digital transformation, and a surge in cyberattacks on emerging industrial hubs.
• Rest of the World: Regions such as Latin America and the Middle East & Africa are gradually embracing industrial cybersecurity solutions as they modernize their industrial sectors.

Competitive Landscape

The market is characterized by intense competition among global and regional players. Major companies are adopting strategic initiatives such as mergers and acquisitions, new product launches, and collaborations to maintain market leadership. For instance:
• Product Innovation: Companies are investing in research and development to offer innovative cybersecurity solutions that integrate artificial intelligence (AI) and machine learning (ML) for predictive threat detection.
• Strategic Partnerships: Collaborations between technology providers and industrial firms are on the rise, ensuring seamless integration of cybersecurity protocols into existing industrial infrastructures.
• Geographical Expansion: Firms are expanding their global footprint to tap into emerging markets with increasing industrial cybersecurity needs.

Get a Quote Now: https://www.fortunebusinessinsights.com/enquiry/get-a-quote/industrial-cybersecurity-market-104557

Key Industry Development

• June 2020: Microsoft Corporation completed the acquisition of CyberX, provider of industrial IoT, Operational Technology and infrastructure solutions. The acquisition assisted the company to boost the adoption and secure users' IoT deployments.
• February 2020: Rockwell Automation, Inc., completed acquisition of Kalypso, an Ohio-based company. The acquisition assisted Rockwell to develop and offer a full suite of security solutions across consulting, business process management, and enterprise technologies.

Read Related Insights:
Facilities Management Market Size, Share, Growth and Industry Forecast Report, 2032
SCADA Market Size, Share, Growth and Industry Forecast Report, 2032

Ashwin Arora
Fortune Business Insights™ Pvt. Ltd.
+1 833-909-2966
sales@fortunebusinessinsights.com
Visit us on social media:
Facebook
X
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/796372869