

Industrial Automation Cybersecurity Market Forecasts to 2034 – Global Analysis By Deployment (On-Premise, Cloud-Based, and Hybrid), Security Type, Component, Service Type, Technology, Application, End User, and By Geography

<https://marketpublishers.com/r/I19574FB9A03EN.html>

Date: August 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: I19574FB9A03EN

Abstracts

According to Statistics MRC, the Global Industrial Automation Cybersecurity Market is accounted for \$5.8 billion in 2026 and is expected to reach \$13.7 billion by 2034 growing at a CAGR of 11.3% during the forecast period. Industrial automation cybersecurity refers to specialized security frameworks and technologies designed to protect operational technology environments, industrial control systems, and automated manufacturing infrastructure from cyber threats. These systems encompass network segmentation, intrusion detection, endpoint protection, and secure remote access solutions tailored for supervisory control and data acquisition, distributed control systems, and programmable logic controllers. The technology integrates threat intelligence, anomaly detection, and incident response mechanisms that address the unique vulnerabilities of industrial networks where safety and availability are paramount.

Market Dynamics:

Driver:

OT-IT convergence risks

The accelerating convergence of operational technology and information technology networks is exposing industrial control systems to sophisticated cyber threats previously confined to enterprise environments. Legacy industrial equipment designed without security considerations creates persistent vulnerabilities as connectivity expands. The

integration of cloud services, remote monitoring, and IoT sensors into production networks multiplies attack surfaces. End users recognize that traditional IT security approaches inadequately address operational technology requirements. Regulatory mandates for critical infrastructure protection sustain investment momentum.

Restraint:

Legacy system incompatibility

The incompatibility of modern cybersecurity solutions with legacy industrial equipment poses significant deployment challenges across manufacturing and process industries. Older control systems operate on proprietary protocols that resist standard security implementations. Patching and updating legacy devices risks operational disruption in continuous production environments. The extended operational lifecycles of industrial assets exceed cybersecurity product support periods. These compatibility constraints force customized integration approaches that increase cost and complexity.

Opportunity:

Zero trust architectures

The adoption of zero trust security architectures presents transformative opportunities for industrial automation cybersecurity by eliminating implicit trust within operational networks. Micro-segmentation strategies restrict lateral movement capabilities for threat actors. Continuous verification of every device, user, and transaction strengthens access controls. The framework accommodates remote workforce requirements without compromising operational integrity. Scalable implementation models allow phased deployment aligned with operational priorities.

Threat:

Nation-state attacks

The escalating frequency of nation-state sponsored cyberattacks targeting critical infrastructure threatens industrial automation cybersecurity investments and operational continuity. Advanced persistent threat groups develop specialized malware designed to disrupt industrial processes and cause physical damage. Geopolitical tensions increase targeting of energy, manufacturing, and transportation sectors. The sophistication of state-sponsored attacks outpaces defensive capabilities of individual organizations.

Insurance and liability exposure from catastrophic incidents creates risk aversion.

Covid-19 Impact:

The COVID-19 pandemic initially disrupted industrial cybersecurity deployments through remote work constraints and supply chain interruptions. However, the crisis dramatically expanded remote access requirements for industrial systems, creating new attack vectors that demanded enhanced security measures. Post-pandemic hybrid work models sustained elevated remote connectivity needs. The experience of pandemic-induced supply chain vulnerabilities reinforced the critical importance of resilient, secure operational technology infrastructure.

The on-premise segment is expected to be the largest during the forecast period

The on-premise segment is expected to account for the largest market share during the forecast period, due to stringent regulatory requirements and operational continuity demands in critical infrastructure environments. Large industrial enterprises maintain sensitive control system data within localized infrastructure while ensuring deterministic security response times. The segment benefits from established compliance frameworks and air-gapped network architectures. End users prefer direct control over security policy enforcement and threat monitoring. Integration with legacy supervisory control systems favors on-premise deployment models.

The cloud security segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud security segment is predicted to witness the highest growth rate, driven by the accelerating migration of industrial data and analytics workloads to cloud environments. Cloud-native security solutions offer centralized threat intelligence and automated policy management across distributed facilities. The scalability of cloud platforms accommodates fluctuating security monitoring demands. Hybrid cloud architectures enable secure data sharing between operational sites and enterprise systems. Subscription pricing models reduce upfront investment barriers for small and medium industrial enterprises.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to advanced critical infrastructure protection programs and early

adoption of industrial cybersecurity standards. The United States leads with significant government investment through the Cybersecurity and Infrastructure Security Agency. Major technology companies including Palo Alto Networks, Fortinet, and CrowdStrike maintain extensive industrial security portfolios. Regulatory frameworks such as NERC CIP mandate security compliance for energy infrastructure. The presence of leading industrial control system vendors creates ecosystem synergies.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, driven by rapid industrial digitalization and increasing cyber threat awareness in China, Japan, and India. Government programs supporting smart manufacturing prioritize cybersecurity investments alongside automation. The region's expanding critical infrastructure creates attack surfaces requiring protection. Growing regulatory requirements for data protection and operational resilience accelerate market development. Indigenous technology capabilities in network security and threat intelligence support market expansion.

Key players in the market

Some of the key players in Industrial Automation Cybersecurity Market include Palo Alto Networks, Inc., Fortinet, Inc., Cisco Systems, Inc., Check Point Software Technologies Ltd., CrowdStrike Holdings, Inc., Microsoft Corporation, IBM Corporation, Broadcom Inc., Honeywell International Inc., Schneider Electric SE, Siemens AG, Rockwell Automation, Inc., Nozomi Networks Inc., Claroty Ltd., Tenable Holdings, Inc., Trend Micro Incorporated and Darktrace plc..

Key Developments:

In June 2026, Palo Alto Networks, Inc. launched an updated Industrial OT Security platform with AI-driven anomaly detection and automated threat response for critical infrastructure protection.

In May 2026, CrowdStrike Holdings, Inc. expanded its Falcon platform with specialized OT endpoint protection modules for programmable logic controller and remote terminal unit environments.

In April 2026, Claroty Ltd. introduced enhanced continuous threat detection capabilities with deep packet inspection for proprietary industrial protocols and automated asset

discovery.

Deployments Covered:

On-Premise

Cloud-Based

Hybrid

Security Types Covered:

Network Security

Endpoint Security

Application Security

Cloud Security

Identity and Access Management

Security Monitoring

Components Covered:

Solutions

Services

Service Types Covered:

Consulting

Integration

Managed Security Services

Training and Support

Technologies Covered:

Artificial Intelligence

Machine Learning

Zero Trust Security

Industrial IoT Security

Threat Intelligence

Blockchain

Applications Covered:

Manufacturing

Energy and Utilities

Oil and Gas

Chemicals

Mining

Transportation

Pharmaceuticals

End Users Covered:

SCADA Security

ICS Security

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:

Market share assessments for the regional and country-level segments

Strategic recommendations for the new entrants

Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)

Strategic recommendations in key business segments based on the market estimations

Competitive landscaping mapping the key common trends

Company profiling with detailed strategies, financials, and recent developments

Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY DEPLOYMENT

- 5.1 On-Premise
- 5.2 Cloud-Based
- 5.3 Hybrid

6 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY SECURITY TYPE

- 6.1 Network Security
- 6.2 Endpoint Security
- 6.3 Application Security
- 6.4 Cloud Security
- 6.5 Identity and Access Management
- 6.6 Security Monitoring

7 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY COMPONENT

- 7.1 Solutions
- 7.2 Services

8 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY SERVICE TYPE

- 8.1 Consulting
- 8.2 Integration
- 8.3 Managed Security Services
- 8.4 Training and Support

9 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY TECHNOLOGY

- 9.1 Artificial Intelligence

- 9.2 Machine Learning
- 9.3 Zero Trust Security
- 9.4 Industrial IoT Security
- 9.5 Threat Intelligence
- 9.6 Blockchain

10 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY APPLICATION

- 10.1 SCADA Security
- 10.2 ICS Security
- 10.3 OT Network Security
- 10.4 Asset Protection
- 10.5 Remote Access Security
- 10.6 Compliance Management

11 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY END USER

- 11.1 Manufacturing
- 11.2 Energy and Utilities
- 11.3 Oil and Gas
- 11.4 Chemicals
- 11.5 Mining
- 11.6 Transportation
- 11.7 Pharmaceuticals

12 GLOBAL INDUSTRIAL AUTOMATION CYBERSECURITY MARKET, BY GEOGRAPHY

- 12.1 North America
 - 12.1.1 United States
 - 12.1.2 Canada
 - 12.1.3 Mexico
- 12.2 Europe
 - 12.2.1 United Kingdom
 - 12.2.2 Germany
 - 12.2.3 France
 - 12.2.4 Italy

- 12.2.5 Spain
- 12.2.6 Netherlands
- 12.2.7 Belgium
- 12.2.8 Sweden
- 12.2.9 Switzerland
- 12.2.10 Poland
- 12.2.11 Rest of Europe
- 12.3 Asia Pacific
 - 12.3.1 China
 - 12.3.2 Japan
 - 12.3.3 India
 - 12.3.4 South Korea
 - 12.3.5 Australia
 - 12.3.6 Indonesia
 - 12.3.7 Thailand
 - 12.3.8 Malaysia
 - 12.3.9 Singapore
 - 12.3.10 Vietnam
 - 12.3.11 Rest of Asia Pacific
- 12.4 South America
 - 12.4.1 Brazil
 - 12.4.2 Argentina
 - 12.4.3 Colombia
 - 12.4.4 Chile
 - 12.4.5 Peru
 - 12.4.6 Rest of South America
- 12.5 Rest of the World (RoW)
 - 12.5.1 Middle East
 - 12.5.1.1 Saudi Arabia
 - 12.5.1.2 United Arab Emirates
 - 12.5.1.3 Qatar
 - 12.5.1.4 Israel
 - 12.5.1.5 Rest of Middle East
 - 12.5.2 Africa
 - 12.5.2.1 South Africa
 - 12.5.2.2 Egypt
 - 12.5.2.3 Morocco
 - 12.5.2.4 Rest of Africa

13 STRATEGIC MARKET INTELLIGENCE

- 13.1 Industry Value Network and Supply Chain Assessment
- 13.2 White-Space and Opportunity Mapping
- 13.3 Product Evolution and Market Life Cycle Analysis
- 13.4 Channel, Distributor, and Go-to-Market Assessment

14 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

- 14.1 Mergers and Acquisitions
- 14.2 Partnerships, Alliances, and Joint Ventures
- 14.3 New Product Launches and Certifications
- 14.4 Capacity Expansion and Investments
- 14.5 Other Strategic Initiatives

14 COMPANY PROFILES

- 14.1 Palo Alto Networks, Inc.
- 14.2 Fortinet, Inc.
- 14.3 Cisco Systems, Inc.
- 14.4 Check Point Software Technologies Ltd.
- 14.5 CrowdStrike Holdings, Inc.
- 14.6 Microsoft Corporation
- 14.7 IBM Corporation
- 14.8 Broadcom Inc.
- 14.9 Honeywell International Inc.
- 14.10 Schneider Electric SE
- 14.11 Siemens AG
- 14.12 Rockwell Automation, Inc.
- 14.13 Nozomi Networks Inc.
- 14.14 Claroty Ltd.
- 14.15 Tenable Holdings, Inc.
- 14.16 Trend Micro Incorporated
- 14.17 Darktrace plc

List Of Tables

LIST OF TABLES

Table 1 Global Industrial Automation Cybersecurity Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Industrial Automation Cybersecurity Market Outlook, By Deployment (2023-2034) (\$MN)

Table 3 Global Industrial Automation Cybersecurity Market Outlook, By On-Premise (2023-2034) (\$MN)

Table 4 Global Industrial Automation Cybersecurity Market Outlook, By Cloud-Based (2023-2034) (\$MN)

Table 5 Global Industrial Automation Cybersecurity Market Outlook, By Hybrid (2023-2034) (\$MN)

Table 6 Global Industrial Automation Cybersecurity Market Outlook, By Security Type (2023-2034) (\$MN)

Table 7 Global Industrial Automation Cybersecurity Market Outlook, By Network Security (2023-2034) (\$MN)

Table 8 Global Industrial Automation Cybersecurity Market Outlook, By Endpoint Security (2023-2034) (\$MN)

Table 9 Global Industrial Automation Cybersecurity Market Outlook, By Application Security (2023-2034) (\$MN)

Table 10 Global Industrial Automation Cybersecurity Market Outlook, By Cloud Security (2023-2034) (\$MN)

Table 11 Global Industrial Automation Cybersecurity Market Outlook, By Identity and Access Management (2023-2034) (\$MN)

Table 12 Global Industrial Automation Cybersecurity Market Outlook, By Security Monitoring (2023-2034) (\$MN)

Table 13 Global Industrial Automation Cybersecurity Market Outlook, By Component (2023-2034) (\$MN)

Table 14 Global Industrial Automation Cybersecurity Market Outlook, By Solutions (2023-2034) (\$MN)

Table 15 Global Industrial Automation Cybersecurity Market Outlook, By Services (2023-2034) (\$MN)

Table 16 Global Industrial Automation Cybersecurity Market Outlook, By Service Type (2023-2034) (\$MN)

Table 17 Global Industrial Automation Cybersecurity Market Outlook, By Consulting (2023-2034) (\$MN)

Table 18 Global Industrial Automation Cybersecurity Market Outlook, By Integration

(2023-2034) (\$MN)

Table 19 Global Industrial Automation Cybersecurity Market Outlook, By Managed Security Services (2023-2034) (\$MN)

Table 20 Global Industrial Automation Cybersecurity Market Outlook, By Training and Support (2023-2034) (\$MN)

Table 21 Global Industrial Automation Cybersecurity Market Outlook, By Technology (2023-2034) (\$MN)

Table 22 Global Industrial Automation Cybersecurity Market Outlook, By Artificial Intelligence (2023-2034) (\$MN)

Table 23 Global Industrial Automation Cybersecurity Market Outlook, By Machine Learning (2023-2034) (\$MN)

Table 24 Global Industrial Automation Cybersecurity Market Outlook, By Zero Trust Security (2023-2034) (\$MN)

Table 25 Global Industrial Automation Cybersecurity Market Outlook, By Industrial IoT Security (2023-2034) (\$MN)

Table 26 Global Industrial Automation Cybersecurity Market Outlook, By Threat Intelligence (2023-2034) (\$MN)

Table 27 Global Industrial Automation Cybersecurity Market Outlook, By Blockchain (2023-2034) (\$MN)

Table 28 Global Industrial Automation Cybersecurity Market Outlook, By Application (2023-2034) (\$MN)

Table 29 Global Industrial Automation Cybersecurity Market Outlook, By SCADA Security (2023-2034) (\$MN)

Table 30 Global Industrial Automation Cybersecurity Market Outlook, By ICS Security (2023-2034) (\$MN)

Table 31 Global Industrial Automation Cybersecurity Market Outlook, By OT Network Security (2023-2034) (\$MN)

Table 32 Global Industrial Automation Cybersecurity Market Outlook, By Asset Protection (2023-2034) (\$MN)

Table 33 Global Industrial Automation Cybersecurity Market Outlook, By Remote Access Security (2023-2034) (\$MN)

Table 34 Global Industrial Automation Cybersecurity Market Outlook, By Compliance Management (2023-2034) (\$MN)

Table 35 Global Industrial Automation Cybersecurity Market Outlook, By End User (2023-2034) (\$MN)

Table 36 Global Industrial Automation Cybersecurity Market Outlook, By Manufacturing (2023-2034) (\$MN)

Table 37 Global Industrial Automation Cybersecurity Market Outlook, By Energy and Utilities (2023-2034) (\$MN)

Table 38 Global Industrial Automation Cybersecurity Market Outlook, By Oil and Gas (2023-2034) (\$MN)

Table 39 Global Industrial Automation Cybersecurity Market Outlook, By Chemicals (2023-2034) (\$MN)

Table 40 Global Industrial Automation Cybersecurity Market Outlook, By Mining (2023-2034) (\$MN)

Table 41 Global Industrial Automation Cybersecurity Market Outlook, By Transportation (2023-2034) (\$MN)

Table 42 Global Industrial Automation Cybersecurity Market Outlook, By Pharmaceuticals (2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) Regions are also represented in the same manner as above.

I would like to order

Product name: Industrial Automation Cybersecurity Market Forecasts to 2034 – Global Analysis By Deployment (On-Premise, Cloud-Based, and Hybrid), Security Type, Component, Service Type, Technology, Application, End User, and By Geography

Product link: <https://marketpublishers.com/r/l19574FB9A03EN.html>

Price: US\$ 4,150.00 (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/l19574FB9A03EN.html>