+357 96 030922
info@marketpublishers.com

Energy System Cyber-Physical Security Market Forecasts to 2032 – Global Analysis By Security Layer (Network Security, Device & Endpoint Security, Application Security, Data Integrity Protection, Control System Security and Physical Asset Protection), Threat Type, Energy Infrastructure, Application, End User and By Geography

https://marketpublishers.com/r/E30F4C44321CEN.html
Date: February 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: E30F4C44321CEN

Abstracts

According to Stratistics MRC, the Global Energy System Cyber-Physical Security Market is accounted for $19.6 billion in 2025 and is expected to reach $39.2 billion by 2032 growing at a CAGR of 10.4% during the forecast period. Energy System Cyber-Physical Security encompasses measures to protect critical energy infrastructure (power grids, pipelines, renewables) from cyber-attacks, physical threats, and combined hybrid risks. It integrates IT network security with physical access controls and real-time monitoring of operational technology (OT). The goal is to ensure the availability, integrity, and resilience of energy supply systems against sabotage, espionage, or ransomware that could cause widespread disruption.

Market Dynamics:

Driver:

Rising cyber threats to grids

Rising cyber threats to grids are significantly increasing demand for cyber-physical security solutions as energy systems become more interconnected and digitized. Integration of smart meters, IoT sensors, and distributed energy resources expands the

+357 96 030922
info@marketpublishers.com

attack surface across power networks. Utilities face growing risks of operational disruption, data breaches, and physical damage caused by cyber intrusions. These risks are driving investments in advanced security architectures designed to protect grid reliability, operational continuity, and critical infrastructure integrity.

Restraint:

Complex integration with legacy systems

Complex integration with legacy systems restrains adoption of cyber-physical security solutions across energy networks. Many utilities operate aging infrastructure with limited cybersecurity capabilities and incompatible communication protocols. Retrofitting security controls into legacy environments increases deployment complexity, costs, and operational risk. Limited visibility across hybrid digital-analog systems further complicates threat detection. These integration challenges slow modernization efforts and delay full-scale implementation of advanced cyber-physical security frameworks.

Opportunity:

AI-driven grid security platforms

AI-driven grid security platforms present substantial growth opportunities as utilities seek proactive threat detection and response capabilities. Machine learning models enable real-time anomaly detection, predictive risk assessment, and automated incident response. Increasing volumes of grid data improve AI accuracy and adaptability. Adoption of cloud-based analytics and digital twins further enhances situational awareness. These technologies allow energy operators to transition from reactive to predictive security postures, strengthening market growth potential.

Threat:

Sophisticated nation-state cyberattacks

Sophisticated nation-state cyberattacks pose a critical threat to the energy system cyber-physical security market. Advanced persistent threats targeting power grids can cause large-scale outages and physical damage. Such attacks evolve rapidly, outpacing traditional security defenses. Escalating geopolitical tensions increase frequency and complexity of state-sponsored intrusions. Failure to counter these threats effectively can undermine confidence in digital grid initiatives and delay investment in interconnected

+357 96 030922
info@marketpublishers.com

energy infrastructure.

Covid-19 Impact:

The COVID-19 pandemic increased reliance on remote grid operations and digital control systems, amplifying cybersecurity exposure. Utilities accelerated digitalization to maintain operational continuity amid workforce restrictions. This shift highlighted vulnerabilities in existing security frameworks. As a result, investment in cyber-physical security solutions gained momentum during and after the pandemic. Enhanced focus on resilient and remotely manageable grid security has strengthened long-term demand across energy systems.

The network security segment is expected to be the largest during the forecast period

The network security segment is expected to account for the largest market share during the forecast period, resulting from its foundational role in protecting communication channels across energy systems. Securing data flows between substations, control centers, and distributed assets is critical for grid stability. Increasing use of IP-based networks and remote monitoring intensifies demand for robust network security solutions. These systems form the first line of defense against cyber intrusions, supporting segment dominance.

The malware & ransomware attacks segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the malware & ransomware attacks segment is predicted to witness the highest growth rate, propelled by the rising frequency and sophistication of targeted cyberattacks on energy infrastructure. Threat actors increasingly exploit software vulnerabilities, remote access points, and operational technology networks to disrupt grid operations or demand ransom payments. Expanding digitalization of energy systems heightens exposure to such attacks. In response, utilities are investing in advanced detection, response, and recovery solutions, accelerating segment growth.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by early adoption of advanced grid digitalization and critical infrastructure protection initiatives. Fueled by rising cyberattack incidences on energy utilities, the region continues to invest heavily in real-time monitoring, intrusion

+357 96 030922
info@marketpublishers.com

detection, and resilience frameworks. Moreover, stringent regulatory mandates and strong presence of leading cybersecurity solution providers further reinforce market penetration. Consequently, large-scale deployment across power generation, transmission, and distribution networks sustains regional dominance.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, spurred by rapid expansion of smart grids and renewable energy integration. Driven by accelerating industrialization and urbanization, countries such as China, India, and Japan are increasingly prioritizing energy infrastructure security. In addition, rising government investments in grid modernization and digital energy management platforms are strengthening demand. As a result, the convergence of energy digitization and cybersecurity awareness is propelling robust regional growth.

Key players in the market

Some of the key players in Energy System Cyber-Physical Security Market include Palo Alto Networks, Fortinet, Inc., Cisco Systems, Inc., Siemens AG, Schneider Electric, ABB Ltd., Honeywell International Inc., Dragos, Inc., Nozomi Networks, Claroty, IBM Corporation, Microsoft Corporation, Darktrace, Tenable, Inc., Check Point Software, FireEye (Trellix), Thales Group, and BAE Systems.

Key Developments:

In December 2025, Fortinet, Inc. introduced next-generation energy sector firewalls and OT/IT convergence security solutions, improving resilience against cyberattacks on smart grids and distributed energy assets.

In November 2025, Cisco Systems, Inc. expanded its industrial cybersecurity portfolio with adaptive intrusion prevention and real-time monitoring for electric utilities and smart energy networks.

In September 2025, Schneider Electric enhanced its EcoStruxure cybersecurity suite with real-time threat detection and anomaly response for industrial and utility-scale energy operations.

Security Layers Covered:

+357 96 030922
info@marketpublishers.com

- Network Security
- Device & Endpoint Security
- Application Security
- Data Integrity Protection
- Control System Security
- Physical Asset Protection

Threat Types Covered:

- Malware & Ransomware Attacks
- Insider Threats
- Supply Chain Attacks
- Advanced Persistent Threats
- Physical Intrusion Risks

Energy Infrastructures Covered:

- Power Generation Facilities
- Transmission Networks
- Distribution Grids
- Renewable Energy Installations
- Energy Storage Systems

+357 96 030922
info@marketpublishers.com

Applications Covered:

- Grid Monitoring & Control
- SCADA Protection
- Incident Detection & Response
- Compliance & Risk Management
- Operational Resilience Enhancement

End Users Covered:

- Utilities & Grid Operators
- Renewable Energy Operators
- Independent Power Producers
- Government & Defense Agencies
- Energy Infrastructure Operators

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany

+357 96 030922
info@marketpublishers.com

- UK
- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

+357 96 030922
info@marketpublishers.com

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & 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 2024, 2025, 2026, 2028, and 2032
- 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)

+357 96 030922
info@marketpublishers.com

Competitive Benchmarking

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

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Energy System Cyber-Physical Security Market Forecasts to 2032 – Global Analysis By Security Layer (Network Security, Device & Endpoint Security, Application Security, Data Integrity Protection, Control System Security and Physical Asset Protection), Threat Type, Energy Infrastructure, Application, End User and By Geography

Product link: https://marketpublishers.com/r/E30F4C44321CEN.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/E30F4C44321CEN.html