+357 96 030922
info@marketpublishers.com

Smart Grid Security Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented, By Deployment Mode (On-Premises, and Cloud), By Security Type (Endpoint, Network, Application, and Database), By Application (Consumption, Generation, and Distribution & Control), By Region & Competition, 2021-2031F

https://marketpublishers.com/r/SA023FBF4D75EN.html
Date: January 2026
Pages: 188
Price: US$ 4,500.00 (Single User License)
ID: SA023FBF4D75EN

Abstracts

The Global Smart Grid Security Market is projected to expand from USD 67.92 Billion in 2025 to USD 171.21 Billion by 2031, registering a CAGR of 16.66%. This sector encompasses digital protective architectures, encryption protocols, and identity management systems aimed at safeguarding modernized electrical power networks from cyber espionage, data breaches, and physical sabotage. Market growth is largely driven by strict government mandates regarding critical infrastructure protection and the operational need to secure distributed energy resources against hostile threats. Furthermore, the rapid digitization of utility frameworks to support renewable energy has necessitated significant investment in defensive mechanisms. According to the International Energy Agency, global investment in electricity grids was expected to reach USD 400 billion in 2024, signaling a massive push for infrastructure modernization that directly fuels the demand for embedded security measures.

Despite these drivers, the market faces a significant hurdle regarding the interoperability between legacy analog systems and modern digital protocols. Utilities often encounter difficulties when attempting to overlay advanced cybersecurity controls onto aging infrastructure that was not originally engineered for connectivity, resulting in potential vulnerabilities and higher implementation costs. This complexity creates integration friction that can delay comprehensive security deployments and hinder compliance with

+357 96 030922
info@marketpublishers.com

evolving industry standards, ultimately slowing the overall pace of market expansion.

Market Driver

The increasing frequency and sophistication of cyberattacks on critical energy infrastructure act as a primary catalyst for the Global Smart Grid Security Market. As utilities merge Information Technology (IT) with Operational Technology (OT), the attack surface widens, creating vulnerabilities that malicious actors exploit for digital extortion and geopolitical disruption. This evolving threat landscape necessitates advanced threat intelligence and intrusion detection systems to neutralize ransomware campaigns before they compromise grid reliability. According to Zscaler?s 'ThreatLabz 2024 Ransomware Report' from July 2024, the energy sector saw a year-over-year rise of approximately 527% in ransomware attacks, highlighting the critical need for fortified defensive architectures in modern utility environments.

Additionally, the rapid modernization and digitization of aging power grid infrastructure drive the adoption of specialized security solutions. Governments are heavily investing in grid resilience programs that add digital communication layers to legacy hardware to support distributed energy resources and electric vehicle integration, requiring concurrent investments in cybersecurity. For instance, the U.S. Department of Energy announced in an August 2024 press release regarding the 'Grid Resilience and Innovation Partnerships (GRIP) Program' a federal investment of USD 2.2 billion to strengthen the grid against extreme weather and cyber threats. The operational risks of this connectivity are significant; Thales?s '2024 Data Threat Report' from March 2024 noted that 42% of critical infrastructure organizations experienced a data breach in the past year, underscoring the need for robust security governance.

Market Challenge

A major obstacle hindering the Global Smart Grid Security Market is the integration complexity caused by interoperability issues between legacy analog systems and modern digital protocols. Utilities frequently face technical difficulties when attempting to apply digital security controls to aging infrastructure that was built without connectivity or external access features. This incompatibility forces organizations to undertake extensive and costly customization instead of deploying standardized security solutions, raising the financial and operational barriers to market entry. Consequently, these technical challenges delay project timelines and cause hesitation among utility operators, who fear that introducing new security layers might disrupt the stability of

+357 96 030922
info@marketpublishers.com

essential, older grid components.

The prevalence of antiquated assets fundamentally limits the speed at which security mechanisms can be adopted across the sector. According to Eurelectric, in 2024, 30% of the existing electricity grid was reported to be over 40 years old. This significant volume of aging infrastructure requires that substantial capital be directed toward basic asset replacement before advanced cybersecurity measures can be effectively integrated. As a result, the addressable market for security vendors is artificially constrained, as the prerequisite modernization of physical assets slows down the procurement cycle for digital defense systems.

Market Trends

The emergence of Digital Twins for Cyber Risk Simulation and Resilience Testing enables utilities to generate virtual replicas of their physical grid assets to model attack scenarios without risking operational stability. These high-fidelity simulations allow operators to stress-test security protocols against hypothetical ransomware or DDoS events, identifying vulnerabilities in a safe, isolated environment prior to deployment. The sophistication of these systems is increasing; according to a November 2024 review in the journal Applied Sciences titled 'The Applications and Challenges of Digital Twin Technology in Smart Grids', 67% of successful digital twin implementations analyzed between 2022 and 2024 incorporated artificial intelligence and machine learning technologies to improve predictive capabilities.

Simultaneously, the implementation of Zero Trust Architecture across utility networks is shifting the industry from perimeter-based defense to a model that requires continuous verification of every user and device. This approach reduces the risk of lateral movement by hostile actors who breach the outer network boundary, ensuring that compromised assets cannot automatically access sensitive control systems. This architectural shift is receiving significant institutional support; according to an Iowa State University article from October 2024, 'Engineers build zero-trust, real-time cybersecurity tools to protect renewables on the grid', the U.S. Department of Energy allocated USD 45 million to a cybersecurity initiative specifically focused on developing and validating zero-trust solutions for energy infrastructure.

Key Market Players

Broadcom, Inc.

+357 96 030922
info@marketpublishers.com

Eaton Corporation plc

McAfee, LLC

Entergy Corporation

Alert Enterprise, Inc,

IOActive, Inc.

IBM Corporation

Black & Veatch Holdings

Cisco Systems, Inc.

BAE Systems plc

Report Scope

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

Smart Grid Security Market, By Deployment Mode

On-Premises

Cloud

Smart Grid Security Market, By Security Type

Endpoint

Network

Application

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Australia

South Korea

South America

Brazil

Argentina

Colombia

Middle East & Africa

South Africa

Saudi Arabia

UAE

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Smart Grid Security Market.

Available Customizations:

Global Smart Grid Security Market report with the given market data, TechSci 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).

+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

8. ASIA PACIFIC SMART GRID SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

9. MIDDLE EAST & AFRICA SMART GRID SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

10. SOUTH AMERICA SMART GRID SECURITY MARKET OUTLOOK

11. MARKET DYNAMICS

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Smart Grid Security Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented, By Deployment Mode (On-Premises, and Cloud), By Security Type (Endpoint, Network, Application, and Database), By Application (Consumption, Generation, and Distribution & Control), By Region & Competition, 2021-2031F

Product link: https://marketpublishers.com/r/SA023FBF4D75EN.html

Price: US$ 4,500.00 (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/SA023FBF4D75EN.html