+44 20 8123 2220
info@marketpublishers.com

Global Critical Infrastructure Protection Market by Component (Security Technologies (Network Security, Physical Security (Screening & Scanning, Video Surveillance, PSIM & PIAM, Access Control), Vehicle Identification Management, Building Management Systems, Secure Communications, Radars, SCADA Security, and CBRNE), Services (Risk Management Services, Designing, Integration, Consultation, Managed Services, Maintenance & Support), By Application (Energy & Power, Transportation, Sensitive Infrastructure & Enterprises, Others), By Region, Competition, 2018-2028

https://marketpublishers.com/r/GEFF38B8B79EN.html
Date: November 2023
Pages: 171
Price: US$ 4,900.00 (Single User License)
ID: GEFF38B8B79EN

Abstracts

The projected market size for the global critical infrastructure protection market is expected to reach USD 146.13 billion by the end of 2022, with a compound annual growth rate (CAGR) of 5.46% during the forecast period. The global critical infrastructure protection market is of paramount importance in today's interconnected world. This market revolves around safeguarding essential systems such as energy, transportation, communication, and healthcare against an array of threats, including cyberattacks, natural disasters, and terrorism. As these infrastructures become increasingly digitized, the market encompasses a wide range of solutions, from physical security measures to advanced cybersecurity technologies. Governments, enterprises, and organizations invest extensively in fortifying their critical assets to ensure uninterrupted operations, public safety, and national security. The market's evolution is

+44 20 8123 2220
info@marketpublishers.com

driven by the imperative to stay ahead of emerging threats, with the integration of technologies like AI, IoT, and data analytics enhancing its capabilities. As societies become more reliant on critical infrastructure, the protection market plays a pivotal role in maintaining stability and resilience.

Key Market Drivers

Escalating Cybersecurity Threats and Attacks

One of the primary drivers propelling the global critical infrastructure protection market is the escalating threat landscape posed by cyberattacks. As critical infrastructures become increasingly digitized and interconnected, they become vulnerable to sophisticated cyber threats from state-sponsored actors, hacktivists, criminal enterprises, and even insider threats. The potential impact of a successful cyberattack on critical systems, such as power grids, transportation networks, and healthcare facilities, is profound and can lead to disruption, financial losses, and compromised public safety. To counteract these threats, governments, organizations, and enterprises are investing significantly in advanced cybersecurity solutions. This includes deploying intrusion detection systems, firewalls, threat intelligence platforms, and security analytics tools. The need to stay ahead of evolving cyber threats is driving innovation in cybersecurity technologies, contributing to the growth of the critical infrastructure protection market.

Regulatory Mandates and Compliance

Stringent regulatory mandates and compliance requirements serve as another significant driver for the critical infrastructure protection market. Governments across the world are imposing regulations that mandate organizations to adopt specific security measures to safeguard critical assets. These regulations are designed to enhance the resilience of essential systems, prevent disruptions, and protect public safety. For instance, the NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards in the energy sector and regulations like NIS Directive in the European Union compel organizations to implement robust cybersecurity measures. Failure to comply with these regulations can result in severe penalties and reputational damage. Organizations are, therefore, investing in security solutions and best practices to ensure compliance and protect their critical infrastructure assets.

Growing Interconnectivity and IoT Adoption

+44 20 8123 2220
info@marketpublishers.com

The rapid growth of interconnected devices and the Internet of Things (IoT) is significantly driving the critical infrastructure protection market. While IoT promises enhanced efficiency and data-driven insights, it also introduces a broader attack surface and potential vulnerabilities. As critical infrastructure systems integrate IoT devices for improved operations and data collection, ensuring the security of these devices becomes imperative. Organizations are adopting solutions that provide comprehensive visibility and control over IoT devices within critical systems. These solutions include IoT security platforms, device authentication mechanisms, and anomaly detection systems. With the proliferation of IoT devices across industries such as energy, transportation, and manufacturing, the demand for robust security solutions is fueling the growth of the critical infrastructure protection market.

Increasing Investment in Smart Cities and Urbanization

The rapid growth of urbanization and the development of smart cities are contributing to the expansion of the critical infrastructure protection market. As cities become more interconnected and data-driven, their reliance on critical infrastructure systems intensifies. Smart city initiatives encompass a range of essential services, from smart transportation and energy grids to public safety and healthcare. To realize the potential benefits of smart cities while mitigating the associated risks, governments and urban planners are investing in advanced security solutions. These solutions help secure critical systems, prevent unauthorized access, and ensure the continuity of services in urban environments. The expansion of smart city projects worldwide is driving the demand for security technologies that can safeguard the intricate web of interconnected infrastructure components, fostering growth in the critical infrastructure protection market.

Key Market Challenges

Evolving and Sophisticated Cyber Threats

One of the foremost challenges confronting the global critical infrastructure protection market is the relentless evolution of cyber threats. Cyber adversaries are continuously adapting their tactics, techniques, and procedures to exploit vulnerabilities within critical infrastructure systems. These threats range from nation-state actors seeking to disrupt essential services to criminal organizations aiming for financial gain and hacktivists motivated by ideological reasons. The increasing sophistication and innovation of cyber threats present a significant hurdle for organizations tasked with protecting critical

+44 20 8123 2220
info@marketpublishers.com

assets. Cyber threats encompass a wide range of attack vectors, including malware, ransomware, phishing, denial-of-service attacks, and zero-day exploits. These threats are designed to infiltrate systems, compromise data, and disrupt services, often with far-reaching consequences for public safety, economies, and national security. Furthermore, the rise of advanced persistent threats (APTs) underscores the deliberate and persistent nature of attacks, challenging organizations to detect and mitigate threats that may remain hidden for extended periods.

Complexity of Interconnected Systems

The increasing complexity of interconnected critical infrastructure systems presents a significant challenge for the global critical infrastructure protection market. The drive toward digitization and the Internet of Things (IoT) has led to the integration of a myriad of devices, sensors, and components into critical infrastructure networks. While this connectivity offers numerous benefits, it also introduces complexities that can hinder effective security and protection.

Interconnected systems create an expanded attack surface, as each connected device potentially becomes a point of entry for cyberattacks. Moreover, the diversity of devices and communication protocols complicates security management and monitoring. A vulnerability in one part of the system can potentially cascade into a widespread disruption affecting multiple interconnected components. Additionally, legacy systems that were not initially designed with security in mind pose a challenge. Many critical infrastructure components were deployed before the current cybersecurity landscape emerged, making them more susceptible to exploitation. Retrofitting these systems with modern security measures can be intricate and costly, requiring a delicate balance between security enhancements and system functionality. Addressing the challenge of interconnected complexity demands comprehensive risk assessment, network segmentation, and the implementation of security controls that can adapt to dynamic environments. Organizations must adopt strategies that strike a balance between connectivity and security, incorporating technologies such as network segmentation, micro-segmentation, and zero-trust architecture. Collaboration between different sectors and industries is also crucial to ensure a unified approach to safeguarding interconnected systems against evolving threats.

Key Market Trends

Convergence of Physical and Cybersecurity

+44 20 8123 2220
info@marketpublishers.com

A prominent trend shaping the global critical infrastructure protection market is the convergence of physical and cybersecurity. Traditionally, physical security and cybersecurity operated as separate domains, but the increasing digitalization of critical infrastructure has blurred these boundaries. As a result, organizations are adopting integrated solutions that address both physical threats, such as unauthorized access, and cyber threats, like malware and hacking. This convergence involves the deployment of sophisticated security information and event management (SIEM) systems that provide a holistic view of security incidents across both digital and physical environments. Integrated access control systems, video surveillance solutions, and cybersecurity platforms enable real-time monitoring and response. This trend reflects the recognition that comprehensive protection requires a unified approach, where insights from both domains inform effective decision-making. The convergence trend is likely to accelerate as threats continue to evolve and interconnected systems become more complex.

Adoption of Artificial Intelligence and Machine Learning

The integration of artificial intelligence (AI) and machine learning (ML) technologies is emerging as a transformative trend in the global critical infrastructure protection market. The massive volume of data generated by critical systems is challenging to analyze and interpret using traditional methods. AI and ML offer the capability to process and analyze this data rapidly, identifying patterns, anomalies, and potential threats in real time. AI-driven threat detection systems can identify and respond to deviations from normal behavior across various systems, such as energy grids or transportation networks. Predictive analytics powered by ML algorithms can anticipate potential vulnerabilities and prescribe proactive measures. Additionally, AI-enabled cybersecurity solutions can autonomously detect and neutralize cyber threats, reducing response times and minimizing potential damages. As organizations seek ways to enhance their threat detection capabilities and response times, the adoption of AI and ML in critical infrastructure protection is poised to increase, revolutionizing how security operations are conducted.

Emphasis on Resilience and Rapid Recovery

The trend toward emphasizing resilience and rapid recovery strategies is gaining prominence in the global critical infrastructure protection market. Recognizing that complete prevention of disruptions is challenging, organizations are focusing on building resilience by establishing robust backup systems, redundancy mechanisms, and contingency plans. This approach aims to minimize the impact of potential disruptions

+44 20 8123 2220
info@marketpublishers.com

and accelerate recovery when incidents occur.

One facet of this trend is the adoption of disaster recovery and business continuity solutions that facilitate swift restoration of critical services after an incident. Additionally, organizations are investing in cyber resilience strategies that ensure continuous operations even in the face of cyberattacks. This involves training personnel, conducting regular drills, and simulating attack scenarios to test response capabilities. The shift towards resilience and rapid recovery is driven by the understanding that disruptions can have cascading effects on public safety, economies, and national security. As critical infrastructure becomes more complex and interconnected, the focus on resilience becomes crucial to maintaining the integrity and functionality of essential systems. Consequently, solutions and strategies that enhance resilience and recovery capabilities are expected to gain traction across sectors and industries in the critical infrastructure protection market.

Segmental Insights

Application Insights

Based on service, the consultation segment emerges as the predominant segment, exhibiting unwavering dominance projected throughout the forecast period. Consultation services are instrumental in guiding organizations through the intricate landscape of critical infrastructure protection. Expert consultants offer insights, tailored strategies, and recommendations that align with an organization's unique needs and vulnerabilities. This segment's dominance reflects the market's recognition of the value that specialized consultation brings to the table in terms of comprehensive threat assessment, risk mitigation, and proactive defense strategies. As threats evolve and security needs become increasingly sophisticated, the consultation segment's enduring influence underscores the vital role of expert guidance in ensuring the resilience, continuity, and security of critical infrastructure systems.

End User Insights

Based on application, the energy & power segment emerges as a formidable frontrunner, exerting its dominance and shaping the market's trajectory throughout the forecast period. This dominance underscores the paramount importance of securing energy production, distribution, and transmission systems, which are essential for the functioning of modern societies and economies. As the energy & power sector becomes more digitized and interconnected, the potential consequences of disruptions due to

+44 20 8123 2220
info@marketpublishers.com

cyberattacks, physical breaches, or other threats are profound. Therefore, the market's focus on providing robust security solutions tailored to the unique challenges of the energy & power sector is crucial in ensuring uninterrupted operations, safeguarding critical assets, and contributing to the overall stability of national infrastructures.

Regional Insights

North America stands resolutely as a dominant force within the global critical infrastructure protection market, solidifying its preeminent position and underscoring its pivotal role in steering the industry's trajectory. With its technologically advanced economies and extensive critical infrastructure networks, North America's commitment to fortifying essential systems against diverse threats underscores its pivotal role. The region's robust adoption of cutting-edge security technologies, regulatory frameworks, and proactive defense strategies further cements its influence in shaping the market's evolution. As the complexity of threats continues to rise, North America's resolute stance in prioritizing the security and resilience of critical assets sets a benchmark for global best practices and positions it as a driving force in the critical infrastructure protection landscape.

Key Market Players

McAfee Corporation

Bae Systems PLC

Lockheed Martin Corporation

Honeywell International Inc.

Airbus SE

Northrop Grumman Corporation

Hexagon AB (Intergraph Corporation)

General Dynamics Corporation

General Electric Company

+44 20 8123 2220
info@marketpublishers.com

Waterfall Security Solutions Ltd.

Report Scope:

In this report, the global critical infrastructure protection market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Global Critical Infrastructure Protection Market, By Component:

Security Technologies

Network Security

Physical Security

Screening & Scanning

Video Surveillance

PSIM & PIAM

Access Control

Vehicle Identification Management

Building Management Systems

Secure Communications

Radars

SCADA Security

CBRNE

Services

+44 20 8123 2220
info@marketpublishers.com

Risk Management Services

Designing

Integration

Consultation

Managed Services

Maintenance & Support

Global Critical Infrastructure Protection Market, By Application:

Energy & Power

Transportation

Sensitive Infrastructure & Enterprises

Others

Global Critical Infrastructure Protection Market, By Region:

North America

Europe

South America

Middle East & Africa

Asia Pacific

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Critical Infrastructure Protection Market.

+44 20 8123 2220
info@marketpublishers.com

Available Customizations:

Global Critical Infrastructure Protection 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

8. NORTH AMERICA CRITICAL INFRASTRUCTURE PROTECTION MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

9. EUROPE CRITICAL INFRASTRUCTURE PROTECTION MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA CRITICAL INFRASTRUCTURE PROTECTION MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST & AFRICA CRITICAL INFRASTRUCTURE PROTECTION MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

12. ASIA PACIFIC CRITICAL INFRASTRUCTURE PROTECTION 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: Global Critical Infrastructure Protection Market by Component (Security Technologies (Network Security, Physical Security (Screening & Scanning, Video Surveillance, PSIM & PIAM, Access Control), Vehicle Identification Management, Building Management Systems, Secure Communications, Radars, SCADA Security, and CBRNE), Services (Risk Management Services, Designing, Integration, Consultation, Managed Services, Maintenance & Support), By Application (Energy & Power, Transportation, Sensitive Infrastructure & Enterprises, Others), By Region, Competition, 2018-2028

Product link: https://marketpublishers.com/r/GEFF38B8B79EN.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/GEFF38B8B79EN.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