Cybersecurity in Critical Infrastructure Market Size Is Likely To Reach a Valuation of Around $31.8 Billion by 2032

Cybersecurity in critical infrastructure market is expanding rapidly due to rising threats, regulatory demands, and the need for resilient protection systems.

WILMINGTON, DE, UNITED STATES, January 28, 2025 /EINPresswire.com/ -- According to the report, the [cybersecurity in critical infrastructure market](#) was valued at $21.8 billion in 2023, and is estimated to reach $31.8 billion by 2032, growing at a CAGR of 3.9% from 2024 to 2032.

Increasing cyber threats and rise in regulatory compliance are the factors expected to propel the growth of the global cybersecurity in critical infrastructure market. However, advancements in technology and growing digital transformation are anticipated to hamper the growth of global market. On the contrary, complexity of legacy systems and shortage of skilled cybersecurity professionals are further likely to create lucrative opportunities for the growth of the global market.

Allied Market Research - Logo

Download Sample Report (Get Full Insights in PDF - 231 Pages) at:
https://www.alliedmarketresearch.com/request-sample/A324118

The cybersecurity in critical infrastructure market focuses on safeguarding essential systems and networks that support vital societal functions, such as energy, transportation, water supply, and healthcare. It encompasses strategies, technologies, and services aimed at defending against cyber threats that could disrupt operations, compromise sensitive data, or cause physical harm. Key objectives include protecting infrastructure assets from malicious cyber activities, enhancing resilience against evolving threats, ensuring compliance with regulatory standards, and promoting collaboration among stakeholders to maintain operational continuity and ensure

public safety.

By type, the network access control (NAC) and firewalls segment accounted for the largest share in 2023 due to its essential role in safeguarding network perimeters and controlling access to sensitive systems and data. NAC solutions enforce security policies by authenticating and authorizing devices and users before granting access to network resources. Firewalls, on the other hand, monitor and filter incoming and outgoing network traffic based on predefined security rules, thereby preventing unauthorized access and defending against cyber threats such as malware and intrusions, which is further expected to propel the overall market growth.

However, the encryption segment is expected to attain the highest CAGR from 2024 to 2032 and is projected to maintain its lead position during the forecast period, owing to escalating concerns over data privacy and the proliferation of stringent regulatory mandates worldwide. Encryption technologies encode sensitive data into unreadable ciphertext, ensuring confidentiality and integrity during transmission and storage. As organizations increasingly digitize their operations and adopt cloud services and IoT devices, the volume of data requiring protection grows exponentially and driving the growth of this segment in the global cybersecurity in critical infrastructure market.

Buy Now & Get Exclusive Discount on this Report:
https://www.alliedmarketresearch.com/cybersecurity-in-critical-infrastructure-market/purchase-options

By application, the government & defense segment accounted for the largest share in 2023, owing to the strategic importance of securing national defense networks, government operations, and essential public services. Government agencies and defense organizations manage critical infrastructure assets vital to national security, including communication systems, defense networks, and public utilities, which is further expected to propel the overall market growth.

However, the energy and power segment is expected to attain the largest CAGR from 2024 to 2032 and is projected to maintain its lead position during the forecast period, owing the increasing digitalization and interconnectivity of energy grids, power generation facilities, and utilities. As the energy sector adopts smart grid technologies, IoT devices, and renewable energy solutions, it becomes more vulnerable to cyber threats such as ransomware attacks, data breaches, and operational disruptions. Thereby, driving the growth of this segment in the global Cybersecurity in critical infrastructure market.

By region, the North America segment held the highest market share in terms of revenue in 2023, as the region has a highly developed critical infrastructure sector, including energy, transportation, and healthcare, which are prime targets for cyber threats. Moreover, stringent regulatory frameworks such as the NERC CIP standards in the U.S mandate robust cybersecurity measures, driving significant investments in advanced technologies and services, anticipated to

propel the growth of the market in this region.

If you have any special requirements, Request customization: https://www.alliedmarketresearch.com/request-for-customization/A324118

However, Asia-Pacific is projected to attain the highest CAGR from 2024 to 2032, owing to rapid economic development, extensive infrastructure investments, and increasing digitalization across sectors such as energy, telecommunications, and manufacturing. As countries in the region modernize their infrastructure and adopt IoT and cloud technologies, they face heightened cybersecurity risks and vulnerabilities. Governments and organizations are thus prioritizing cybersecurity investments to fortify defences against cyber threats and ensure the resilience of critical services, further expected to contribute to the growth of the market in this region.

Leading Market Players:

· Huawei

· Cisco Systems, Inc.

· NortonLifeLock

· Palo Alto Networks, Inc.

· Check Point Software Technologies Ltd.

· Fortinet, Inc.

· RSA Security LLC

· FireEye, Inc.

· Trend Micro, Inc.

The report provides a detailed analysis of these key players in the cybersecurity in critical infrastructure market. These players have adopted different strategies such as new product launches, collaborations, expansion, joint ventures, agreements, and others to increase their market share and maintain dominant shares in different countries. The report is valuable in highlighting business performance, operating segments, product portfolio, and strategic moves of market players to highlight the competitive scenario.

Inquiry Before Buying: https://www.alliedmarketresearch.com/purchase-enquiry/A324118

About Us:

Allied Market Research (AMR) is a full-service market research and business-consulting wing of Allied Analytics LLP, based in Portland, Oregon. AMR provides global enterprises as well as medium and small businesses with unmatched quality of "Market Research Reports" and "Business Intelligence Solutions." AMR has a targeted view to provide business insights and consulting to assist its clients in making strategic business decisions and achieving sustainable growth in their respective market domains.

AMR launched its user-based online library of reports and company profiles, Avenue. An e-access library is accessible from any device, anywhere, and at any time for entrepreneurs, stakeholders, researchers, and students at universities. With reports on more than 60,000 niche markets with data comprising 600,000 pages along with company profiles on more than 12,000 firms, Avenue offers access to the entire repository of information through subscriptions. A hassle-free solution to clients' requirements is complemented with analyst support and customization requests.

Contact:
David Correa
1209 Orange Street,
Corporation Trust Center,
Wilmington, New Castle,
Delaware 19801 USA.
Int'l: +1-503-894-6022
Toll Free: + 1-800-792-5285
UK: +44-845-528-1300
India (Pune): +91-20-66346060
Fax: +1-800-792-5285
help@alliedmarketresearch.com

David Correa
Allied Market Research
+ + +1 800-792-5285
email us here
Visit us on social media:
Facebook
X
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/780974876

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.