EINPRESSWIRE

Exploring the Growth Potential: Cyber Security Market to Reach USD 486.86 Billion by 2030 with 9.5% CAGR

The Cyber Security market is expected to grow from USD 218.00 billion in 2021 to USD 486.86 billion by 2030, at a CAGR of 9.5% during the forecast period.

NEW YORK CITY, NY, UNITED STATES, May 31, 2023 /EINPresswire.com/ -- The [Cyber Security market](#) is expected to grow from USD 218.00 billion in 2021 to USD 486.86 billion by 2030, at

Reports And Data

a CAGR of 9.5% during the forecast period. Focus of enterprises and government for secured sharing of information, rise in digitized workplaces & mobile workforce, increasing number of supply chain-based attacks damaging the software supply chain, strict government norms regarding security of data, increasing demand for cloud based solutions, increase in the Ecommerce penetration across industry verticals and emergence of AI, machine learning and block chain technologies for cyber defense are some of the driving factors of the market.

> "
> The major contributing factor for the growth of the market for Cyber Security can be the focus of enterprises and government for secured sharing of information."
>
> *Reports and Data*

Budget limitation of cyber security solutions, use of pirated and open source cyber security solutions, no such cyber security expertise for proactive strategic planning and no interoperability with the existing information systems may be the major restraining factors for the cyber security market.

Players will require increased investments to tackle these restraints and facilitate growth in the coming years. This report comprises drivers, restraints, opportunities, and challenges pertaining to the Cyber Security market; and extensive value chain analysis, patent analysis, analysis of the current manufacturing capability and technology status, commercialization potential in different devices, along with market size forecasts till 2030.

Get a Free Sample (PDF) Report @ https://www.reportsanddata.com/download-free-sample/931

Further key findings from the report suggest

The Cyber Security market is expected to grow from USD 218.00 billion in 2021 to USD 486.86 billion by 2030, at a CAGR of 9.5% during the forecast period.
The major contributing factors for the growth of the market for Cyber Security can be focus of enterprises and government for secured sharing of information, rise in digitized workplaces & mobile workforce, increasing number of supply chain-based attacks damaging the software supply chain, strict government norms regarding security of data, increasing demand for cloud based solutions, increase in the Ecommerce penetration across industry verticals and leveraging AI, machine learning and block chain technologies for cyber defense.

The Cyber Security market is segmented by deployment type into cloud and on-premises. The cloud deployment type is expected to witness highest growth, at a CAGR of 9.1% during the forecast period, due to its high demand by organizations, since it provides many benefits like affordable, scalability, reliability, flexibility, and remote location access.

The Cyber Security market is segmented by security type into network security, endpoint security, application security, cloud security, others (content security, industrial control system (ICS) security, database security, and web security). The network security type is expected to witness highest growth, at a CAGR of 8.8% during the forecast period, due to rise in the number of security breaches targeting networks where hackers try to gain access to sensitive data.

The Cyber Security Market is segmented by component into solutions and services. Solutions segment is expected to grow with the highest CAGR of approximately 10.1% during the forecast period, due to growth of encryption solutions since they offer consistent protection to sensitive data across all critical points in the entire lifecycle which enables enterprises to hide their critical data from unauthorized bad actors.

The Cyber Security market is segmented by organization size into large and small & medium-sized enterprises. Large and medium-sized mostly adapt the cyber security solutions, small-sized enterprises may find the cyber security solutions a little unaffordable, thus lowering the market of cyber security in the small-sized enterprise segment.

The Cyber Security Market is segmented by industry vertical into aerospace and defence, government, banking, financial services, and insurance (BFSI), IT and telecom, healthcare, retail, manufacturing, energy and utilities and others (education, media and entertainment, and transportation and logistics). Healthcare segment is expected to witness the highest growth, at a CAGR of 9.3% during the forecast period, since the segment is prone to security breaches. Other segments which are expected to witness growth are the banking, financial services and insurance, and IT and telecom industries.

The Cyber Security Market is segmented by Geography into North, America, Europe, Asia Pacific and Rest of the World. North America, being a developed region, dominates the market, with a market share of around USD 45.9 Billion in the base year, since it focuses on utmost security and is readily adopting new and advanced technologies.

Key players within Cyber Security market are:

Sophos (UK), Cisco (US), F5 Networks (US), CyberArk (Israel), FireEye (US), Forcepoint (US), Check Point (US), Fortinet (US), Amazon Web Services (US), Oracle (US), Imperva (US), Qualys (US), Palo Alto Networks (US), RSA Security (US), McAfee (US), F-Secure (Finland), Micro Focus (UK), Microsoft (US), Proofpoint (US), Symantec (US), IBM (US), Rapid7 (US), Splunk (US), Trend Micro (Japan), and Juniper Networks (US).

Segments Covered in the Reports:

This report focuses on the market segmentation of the security industry based on various factors such as deployment type, component, security type, organization size, industry vertical, and regional analysis.

In terms of deployment type, the market can be categorized into two main segments: cloud and on-premises. The cloud segment refers to security solutions that are delivered and managed through a cloud-based platform. On the other hand, the on-premises segment involves security solutions that are installed and managed locally within an organization's infrastructure.

The security type segment encompasses various categories that include network security, endpoint security, application security, cloud security, and others. The "others" category includes content security, industrial control system (ICS) security, database security, and web security.

When considering the components of security solutions, the market can be further divided into two main categories: solutions and services. The solutions category comprises identity and access management (IAM), risk and compliance management, encryption, data loss prevention (DLP), unified threat management (UTM), firewall, antivirus/antimalware, intrusion detection system (IDS)/intrusion prevention system (IPS), security and vulnerability management, disaster recovery, distributed denial of service (DDoS) mitigation, web filtering, and others. The services category consists of professional services, such as design and implementation, risk and threat assessment, consulting, training and education, support and maintenance, as well as managed services.

Organization size is another important factor in market segmentation. It includes large enterprises and small and medium-sized enterprises (SMEs). Large enterprises refer to established companies with significant operations and revenue, while SMEs encompass smaller organizations with relatively limited resources.

The industry vertical segment looks at different sectors that require security solutions. Some of the major industry verticals include aerospace and defense, government, banking, financial services, and insurance (BFSI), IT and telecom, healthcare, retail, manufacturing, energy and utilities, and others. The "others" category includes education, media and entertainment, transportation and logistics, and other miscellaneous sectors.

Finally, the market is analyzed from a regional perspective. The regions considered in this report are North America (including the US, Canada, and Mexico), Europe (including Germany, France, the UK, and the rest of Europe), Asia Pacific (including China, Japan, South Korea, and the rest of APAC), and the rest of the world (RoW), which comprises the Middle East and Africa, as well as South America.

By examining these various segments, this report provides a comprehensive analysis of the security market, allowing businesses and organizations to understand the opportunities and challenges within each segment and make informed decisions regarding their security strategies.

Request a customized copy of the report @ https://www.reportsanddata.com/request-customization-form/931

Thank you for reading our report. We also offer customized report as per client requirement. Kindly connect with us to know more about customization plan and our team will offer you the altered report.

Browse More Reports:

Power Rental Systems Market @ https://www.reportsanddata.com/report-detail/power-rental-systems-market

Product Lifecycle Management (PLM) Market @ https://www.reportsanddata.com/report-detail/product-lifecycle-management-plm-market

Quality Management Software (QMS) Market @ https://www.reportsanddata.com/report-detail/quality-management-software-qms-market

Railway Telematics Market @ https://www.reportsanddata.com/report-detail/railway-telematics-market

Artificial Intelligence (AI) Diagnostics Market @ https://www.reportsanddata.com/report-detail/artificial-intelligence-ai-diagnostics-market

Nikhil Morankar

Reports and Data
+ + 12127101370
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/636816054