# Global Cyber Security Market to Reach Valuation of US$ 882.1 Bn by 2034; at a CAGR of 13.2% During 2024 – 2034;says TNR

*Rapid Adoption of Digital Technologies and Stringent Data Protection Regulations are Driving the Global Cyber Security Market*

WILMINGTON, DELAWARE, UNITED STATES, June 12, 2024 /EINPresswire.com/ -- Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, cyberattacks, and malicious activities. It encompasses a range of strategies, technologies, and processes designed to safeguard digital assets, ensure confidentiality, integrity, and availability of information, and mitigate the risks posed by cyber threats. Key aspects of cybersecurity include threat detection, prevention, incident response, and recovery. By implementing robust security measures such as firewalls, encryption, antivirus software, and access controls, organizations aim to protect against a variety of cyber threats, including malware, phishing, ransomware, and data breaches. Effective cybersecurity practices are essential in safeguarding sensitive information, maintaining operational resilience, and preserving trust in the digital environment amidst the evolving landscape of cyber threats and vulnerabilities.

Get Sample Copy of the Report

The demand for cybersecurity is primarily driven by the increasing frequency and sophistication of cyber threats, coupled with the growing reliance on digital technologies across various sectors. As organizations digitize their operations and data, they become more susceptible to cyberattacks such as ransomware, phishing, and data breaches. Heightened awareness of the financial, reputational, and regulatory risks associated with cyber incidents compels businesses to invest in robust cybersecurity measures to protect their digital assets and maintain operational continuity. Additionally, regulatory compliance requirements, such as GDPR, CCPA, and industry-specific standards, mandate stringent data protection practices, further driving the demand for cybersecurity solutions. However, one significant restraint in the cybersecurity landscape is the shortage of skilled cybersecurity professionals. The cybersecurity skills gap

limits the availability of qualified personnel needed to effectively manage and respond to cyber threats, hindering organizations' ability to implement comprehensive security strategies and leaving them vulnerable to potential breaches and attacks. Addressing this skills shortage remains a critical challenge for the cybersecurity industry.

Global Cyber Security Market: Key Inclusions

Hardware segment of the cyber security market to gain momentum over the forecast period. The demand for hardware-based cybersecurity solutions stems from the critical need to protect physical devices and infrastructure from cyber threats. With the proliferation of connected devices in the Internet of Things (IoT) and Industrial Internet of Things (IIoT) ecosystems, ensuring the security of hardware components becomes paramount. Hardware-based security solutions, such as secure microcontrollers, hardware encryption modules, and Trusted Platform Modules (TPMs), offer robust protection against various cyber threats, including unauthorized access, tampering, and data breaches. As cyberattacks targeting hardware vulnerabilities become more prevalent and sophisticated, organizations across industries, including automotive, healthcare, and manufacturing, are increasingly investing in hardware-based security solutions to safeguard their devices and infrastructure. Moreover, regulatory requirements and industry standards, such as ISO 27001 and NIST Cybersecurity Framework, drive the adoption of hardware-based cybersecurity measures, ensuring compliance and mitigating risks associated with cyber threats targeting hardware components.



Application security segment of the cyber security market to witness highest CAGR (2024 – 2034). The demand for application security within the realm of cybersecurity is propelled by the increasing sophistication of cyber threats targeting software vulnerabilities. As organizations rely more heavily on digital applications for critical business functions, the risk of exploitation by malicious actors grows. Application security ensures that software systems are protected against various threats such as unauthorized access, data breaches, and manipulation of code. With the rising prevalence of cyberattacks exploiting application vulnerabilities, there is a heightened emphasis on secure software development practices, including regular code reviews, vulnerability assessments, and penetration testing. Additionally, regulatory requirements and industry standards such as PCI DSS and HIPAA mandate robust application security measures, further driving demand. Furthermore, the shift towards DevSecOps methodologies, integrating security into the software development lifecycle, underscores the importance of application security in safeguarding digital assets and maintaining trust in the increasingly digitalized world.

In the Asia-Pacific region, the demand for cybersecurity is fueled by rapid digitalization, increasing cyber threats, and regulatory requirements, thus making it witness exponential CAGR during 2024 – 2034. As countries in the region undergo significant digital transformation across various sectors, including finance, healthcare, and manufacturing, the volume of sensitive data

being generated and transmitted online continues to grow. This surge in digital activity presents lucrative targets for cybercriminals, driving the need for robust cybersecurity measures to protect against threats such as malware, ransomware, and data breaches. Additionally, regulatory frameworks such as the Personal Data Protection Act (PDPA) in Singapore and the Privacy Act in Australia mandate organizations to implement stringent data protection practices, further driving the demand for cybersecurity solutions. Moreover, the proliferation of IoT devices, cloud computing, and remote work arrangements amplifies the complexity of cybersecurity challenges, necessitating comprehensive security strategies to safeguard digital assets and ensure business continuity in the Asia-Pacific region.

Browse Related Category Reports

Global Cyber Security Market Key Players:
- Atos SE
- Broadcom
- Cisco Systems, Inc.
- CyberSapiens
- Dark Matter LLC
- Digital Security Company | DIGISEC
- EMTECH
- Fortinet, Inc.
- IBM
- Imperva
- Looptech Co.
- Microsoft
- Open Text Corporation
- Palo Alto Networks
- Thales
- Trend Micro Incorporated
- Other Market Participants

Global Cyber Security Market

Global Cyber Security Market Offering Outlook (Revenue, USD Million, 2016 - 2034)
- Hardware
- Software
- Services
  - Professional Services
  - Managed Services

Global Cyber Security Market Deployment Outlook (Revenue, USD Million, 2016 - 2034)
- Cloud
- On Premise

Global Cyber Security Market Organization Size Outlook (Revenue, USD Million, 2016 - 2034)
- Small and Medium Enterprises
- Large Enterprises

Global Cyber Security Market End User Outlook (Revenue, USD Million, 2016 - 2034)
- Information Technology and Telecommunication
- Healthcare
- Education
  - K-12
  - Higher Education
- Energy and Utilities
- Banking, Financial Services and Insurance (BFSI)
- Government
- Transportation & Logistics
- Manufacturing
- Military and Defense
- Electrical and Electronics
- Hospitality
- Oil & Gas
- Retail
- Media & Entertainment
- Others

Global Cyber Security Market Security Type/Function Outlook (Revenue, USD Million, 2016 - 2034)
- Data Protection
- Governance, risk and compliance
- Email security and awareness
- Cloud Security
- End-Point Security
- Identity and access management
- Security Consulting
- Network Security
- Application Security
- Others

Global Cyber Security Market Threat Type Outlook (Revenue, USD Million, 2016 - 2034)
- Distributed Denial of Service (DDoS)
- Malware
- Phishing
- Spoofing
- Ransomware

- Others

Global Cyber Security Market Regional Outlook (Revenue, USD Million, 2016 - 2034)
- North America (U.S., Canada, Mexico, Rest of North America)
- Europe (France, The UK, Spain, Germany, Italy, Nordic Countries (Denmark, Finland, Iceland, Sweden, Norway), Benelux Union (Belgium, The Netherlands, Luxembourg), Rest of Europe)
- Asia Pacific (China, Japan, India, New Zealand, Australia, South Korea, Southeast Asia (Indonesia, Thailand, Malaysia, Singapore, Rest of Southeast Asia), Rest of Asia Pacific)
- Middle East & Africa (Saudi Arabia, UAE, Egypt, Kuwait, South Africa, Rest of Middle East & Africa)
- Latin America (Brazil, Argentina, Rest of Latin America)

Jay Reynolds
The Niche Research
+1 302-232-5106
email us here

---