+44 20 8123 2220
info@marketpublishers.com

IT & Telecom Cyber Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented by Deployment Modes (On-Premises, Cloud-Based) By Security Solution (Network Security, Endpoint Security, Cloud Security, Application Security), By End-User Industry (Telecom Service Providers, E-commerce, Enterprises, Utilities, Government and Defense, Others), By Region, By Competition, 2018-2028

https://marketpublishers.com/r/I4B054EE124BEN.html
Date: October 2023
Pages: 182
Price: US$ 4,900.00 (Single User License)
ID: I4B054EE124BEN

Abstracts

Global IT & Telecom Cyber Security Market has experienced tremendous growth in recent years and is poised to continue its strong expansion. The IT & Telecom Cyber Security Market reached a value of USD 198.38 billion in 2022 and is projected to maintain a compound annual growth rate of 8.74% through 2028.

In recent years, the Global IT & Telecom Cyber Security market has undergone remarkable growth, largely fueled by the widespread digital transformation initiatives undertaken by organizations worldwide. Businesses are increasingly embracing cutting-edge technologies such as AI, IoT, analytics, and wearables to optimize their operations, enhance customer engagement, and ensure stringent regulatory compliance.

One pivotal area experiencing a surge in the adoption of IT & Telecom Cyber Security solutions is talent management and workforce security. Innovative platforms harness the power of data analytics and AI, extracting valuable insights from employee devices to offer unprecedented visibility into workforce behaviors. These sophisticated tools

equipped with analytics capabilities continuously monitor employee activities in real-time, promptly flagging any non-compliant or risky actions. This proactive approach has proven instrumental in addressing challenges like fraud prevention, insider threats, and upholding regulatory standards. Notably, industries such as financial institutions and government bodies have been pioneers in the implementation of these solutions.

With the prevalence of remote and hybrid work models, the oversight of global operations through data and analytics has assumed greater significance. Leading companies are leveraging analytics from distributed endpoints and AI tools to streamline collaboration among their workforce while safeguarding sensitive data. This dual focus enables more productive engagement of remote employees while ensuring robust customer data security.

To further augment their offerings, data analytics vendors are making substantial investments in predictive modeling, integration capabilities, and user-friendly solutions. These investments are poised to unlock even greater value by enabling applications such as predictive threat detection, optimized access control, and the delivery of personalized digital services for customers, all while maintaining built-in privacy and security controls.

The confluence of workforce security and customer experience presents substantial growth opportunities for IT & Telecom Cyber Security providers. As these tools continue to evolve and integrate advanced functionalities, they are set to fuel the generation of personalized insights and the automation of critical processes. This, in turn, will empower businesses to address the ever-evolving compliance requirements in our increasingly digital world.

In conclusion, the outlook for the Global IT & Telecom Cyber Security industry remains decidedly positive. The industry's exponential growth trajectory is a testament to its indispensable role in safeguarding organizations' digital assets, promoting efficient operations, and enhancing the overall customer experience. As technology continues to advance, the IT & Telecom Cyber Security market will remain at the forefront of ensuring a secure and compliant digital landscape for businesses across the globe.

Key Market Drivers

Rise of Digitalization

With the rapid digital transformation across various industries, there has been a

+44 20 8123 2220
info@marketpublishers.com

massive rise in data generation and its exchange over networks. Organizations are increasingly moving their operations and services online which has expanded the attack surface for cybercriminals. Vast amounts of sensitive customer and organizational data is now stored in the cloud and transmitted over the internet. This has made data theft a lucrative business for hackers. To protect themselves against such online threats, companies are compelled to heavily invest in advanced cyber security solutions such as web filtering, firewalls, antivirus, identity and access management etc. The growing needs of securing digital infrastructure and the transition to Industry 4.0 is a major factor propelling the demand for cyber security in telecom and IT sectors.

Increase in Sophisticated Cyber Attacks

As digital networks become more complex with the integration of newer technologies, cyber attacks have also evolved in terms of complexity, frequency and impact. Threat actors are employing sophisticated techniques like ransomware, phishing scams, DDoS attacks and supply chain compromises to cause large scale disruptions. Moreover, state-sponsored hacking groups are specifically targeting critical infrastructure for cyber espionage and data theft. This has heightened security risks for businesses. The financial and reputational losses incurred due to cyber breaches have increased manifold. As a result, organizations are allocating more funds for proactive threat monitoring, detection and response capabilities. The growing need to mitigate financial and legal repercussions of security compromises is boosting investments in cyber security.

Remote Working Culture

The COVID-19 pandemic accelerated the shift to remote and hybrid work models across industries. While this provided greater flexibility, it has also increased the attack surface. With employees accessing corporate networks through personal devices outside the office premises, the risk of a breach has magnified. There is a lack of visibility and control over the home networks used by the remote workforce. Moreover, virtual private networks (VPNs) used by remote employees to access organizational resources have emerged as an important entry point for hackers. As the remote working trend is likely to stay, companies need endpoint protection, VPN security, identity management, email security, web filtering and malware prevention solutions to secure their remote workforce and applications. This expanding remote attack vector is driving the cyber security market growth.

Key Market Challenges

+44 20 8123 2220
info@marketpublishers.com

Shortage of Cyber Security Skills

While the demand for cyber security professionals has skyrocketed with growing threats, there is a significant talent crunch in the industry. According to estimates, there will be over 3.5 million unfilled cyber security jobs by 2021. Organizations struggle to find and retain skilled security analysts, engineers, threat hunters and security architects. This is mainly due to the very specialized nature of jobs and lack of trained workforce. Moreover, the job roles require constant upskilling as technologies and threats evolve rapidly. Training employees takes a lot of time and resources for companies. The dearth of cyber security experts impacts businesses' ability to deploy next-gen solutions, strengthen security controls, conduct risk assessments and respond to incidents in a timely manner. It also increases their reliance on external cyber security vendors and consultants which drives up costs. Unless the talent shortage is addressed, it can negatively impact the market's growth potential.

Budget Constraints

While the importance of cyber security spending is well-recognized, allocating appropriate budgets remains a challenge for many organizations. Security continues to be an expenditure center rather than an investment for most. Competing business priorities and lack of understanding of return on security investments at the board level leads to underfunding of security programs. Moreover, with the constant emergence of new threats, the necessary security solutions, services and tools keep changing rapidly, which requires flexible budgets. However, in reality cyber security budgets remain mostly static. The large number of small breaches also fail to communicate the true financial impact to senior management and stakeholders. As a result, security teams struggle to get adequate budgets for advanced technologies, managed services, regular audits and skilled talent. This budget crunch restricts organizations' ability to adopt cutting-edge solutions and implement robust security controls. It limits the market opportunity for vendors as well.

Key Market Trends

Adoption of Cloud-Based Security Solutions

With more applications and data moving to public and hybrid cloud environments, there is a rising trend where cyber security solutions themselves are being deployed over the cloud. Cloud-based security offerings provide advantages like scalability, lower upfront

+44 20 8123 2220
info@marketpublishers.com

costs, easy deployment and round-the-clock protection. They are driving increased spending on cloud-delivered services across endpoint protection, web security, firewalls, data loss prevention, identity access management etc. Vendors are innovating cloud-native security platforms that leverage technologies like AI/ML, analytics and automation to strengthen cloud security postures. They are also offering managed detection and response services. As cloud adoption grows exponentially, cloud security market size is projected to reach over USD20 billion by 2023. This clearly shows cloud is emerging as a disruptive delivery model for cyber security.

Adoption of AI and Machine Learning

Cybercriminals are using sophisticated AI/ML techniques to automate attacks at massive scale. To keep pace, security teams are increasingly leveraging cognitive technologies to gain real-time threat visibility, predictive analysis of anomalies and autonomous response. AI assists in monitoring vast volumes of security data, detecting even never-seen-before threats, prioritizing vulnerabilities, and streamlining incident response. It reduces the reliance on manual processes and security personnel shortages. The majority of organizations now consider AI/ML as important to their security programs. The AI cyber security market is estimated to grow at over 40% annually. Vendors are differentiating their offerings by incorporating behavioral analytics, deep learning, natural language processing and other cognitive capabilities.

Focus on Operational Technology Security

With the rise of IoT, automation and convergence of IT and OT networks, cyber risks have expanded to industrial control systems, manufacturing plants, oil & gas pipelines and critical national infrastructure as well. Even small glitches can disrupt operations and cause safety and environmental hazards. There is a growing need to secure these environments from threats like ransomware while ensuring safety, reliability and uptime of equipment. Vendors are developing OT/ICS-specific solutions around device authentication, anomaly detection, secure remote access and segmentation. Regulatory mandates are also driving spending on solutions for process monitoring, patch management, configuration control and security event management in OT. Governments are collaborating with industry to strengthen national cyber resilience. This presents a massive market potential for vendors catering to operational security needs.

Segmental Insights

+44 20 8123 2220
info@marketpublishers.com

Deployment Modes Insights

The on-premises deployment mode dominated the global IT & telecom cyber security market in 2022 and is expected to continue its dominance during the forecast period. The on-premises security solutions are preferred by many large enterprises and government organizations due to factors such as high-level customization needs, complete control over infrastructure, data residency compliance and avoidance of recurring costs associated with cloud solutions. However, the cloud-based security segment is anticipated to witness the highest growth rate during the projected timeframe. This shift can be attributed to advantages of cloud like scalability, pay-as-you-go pricing, easy deployment and maintenance, centralized management and round-the-clock protection. As more security functions are virtualized and workloads migrate to public/hybrid clouds, the demand for cloud-delivered security services including web security, firewall, endpoint protection, IAM and DLP is growing rapidly. The cloud security market is further accelerated by the COVID-19 pandemic induced remote working culture which necessitates cloud-based access to security tools for distributed workforce. Various industry experts also predict that cloud adoption will outpace on-premises in the coming years, which will boost spending on cloud security subscriptions and managed security services.

Security Solution Insights

The network security segment dominated the global IT & telecom cyber security market in 2022 and is expected to maintain its dominance during the forecast period. Network security solutions help organizations secure their wide and complex networks from constantly evolving cyber threats such as malware, phishing attacks, ransomware and zero-day exploits. The growing network traffic volumes, increasing number of connected devices, and transition to remote working have expanded the attack surface significantly. Consequently, there is high demand for advanced network security controls including firewalls, secure web gateways, intrusion prevention systems, and unified threat management. Moreover, with more applications moving to public clouds, the need to protect cloud workloads and cloud-to-ground traffic is driving spending on cloud-delivered network security services. The network security segment is anticipated to continue leading over the forecast period owing to the criticality of networks for business operations and growing sophistication of network attacks. However, the endpoint security and application security segments are expected to witness lucrative growth rates. This can be attributed to the rise in BYOD and mobility trends increasing vulnerabilities at endpoints and growing investments in application security testing and runtime protection solutions.

+44 20 8123 2220
info@marketpublishers.com

Regional Insights

The North American region dominated the global IT & telecom cyber security market in 2022 and is expected to maintain its dominance during the forecast period. This can be attributed to early adoption of advanced cyber security technologies and solutions across various industries in the US and Canada. Presence of many innovative solution providers and cyber security vendors in the region has accelerated product development. Moreover, stringent data protection regulations such as GDPR and CCPA have compelled organizations to heavily invest in security upgrades. High defense, IT and telecom spending by governments in the region provides further impetus. During the pandemic, remote working surge increased the need for effective cyber security controls. Growing concerns around critical infrastructure protection and ransomware also augment market revenues. Asia Pacific is anticipated to witness the fastest growth rate owing to rapid digitalization of economies, increasing cyber threats, and supportive government initiatives for cyber security preparedness in major countries like India, China, Japan and Australia. Europe will exhibit steady demand fueled by initiatives like the NIS Directive and Cyber Security Act focusing on national cyber resilience.

Key Market Players

Cisco Systems

IBM CORPORATION.

Symantec

Trend Micro

FireEye

Check Point Software Technologies

Juniper Networks

Sophos

Rapid7

+44 20 8123 2220
info@marketpublishers.com

Micro Focus International

Report Scope:

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

IT & Telecom Cyber Security Market, By Deployment Modes:

On-Premises

Cloud-Based

IT & Telecom Cyber Security Market, By Security Solution:

Network Security

Endpoint Security

Cloud Security

Application Security

IT & Telecom Cyber Security Market, By End-User Industry:

Telecom Service Providers

E-commerce

Enterprises

Utilities

Government and Defense

IT & Telecom Cyber Security Market, By Region:

North America

+44 20 8123 2220
info@marketpublishers.com

- United States
- Canada
- Mexico

Europe

- France
- United Kingdom
- Italy
- Germany
- Spain

Asia-Pacific

- China
- India
- Japan
- Australia
- South Korea

South America

- Brazil
- Argentina
- Colombia

+44 20 8123 2220
info@marketpublishers.com

- Middle East & Africa
  - South Africa
  - Saudi Arabia
  - UAE
  - Kuwait
  - Turkey
  - Egypt

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global IT & Telecom Cyber Security Market.

Available Customizations:

Global IT & Telecom Cyber Security 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

7. NORTH AMERICA IT & TELECOM CYBER SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

8. EUROPE IT & TELECOM CYBER SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

9. ASIA-PACIFIC IT & TELECOM CYBER SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA IT & TELECOM CYBER SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST AND AFRICA IT & TELECOM CYBER SECURITY 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: IT & Telecom Cyber Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented by Deployment Modes (On-Premises, Cloud-Based) By Security Solution (Network Security, Endpoint Security, Cloud Security, Application Security), By End-User Industry (Telecom Service Providers, E-commerce, Enterprises, Utilities, Government and Defense, Others), By Region, By Competition, 2018-2028

Product link: https://marketpublishers.com/r/I4B054EE124BEN.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/I4B054EE124BEN.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 _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

+44 20 8123 2220
info@marketpublishers.com

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