+357 96 030922
info@marketpublishers.com

Cybersecurity for Telecom & IT Market Forecasts to 2032 – Global Analysis By Component (Hardware, Software and Services), Security Type, Deployment Mode, Organization Size, Security Layer, End User and By Geography

https://marketpublishers.com/r/C74E80728923EN.html
Date: November 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: C74E80728923EN

Abstracts

According to Stratistics MRC, the Global Cybersecurity for Telecom & IT Market is accounted for $40.44 billion in 2025 and is expected to reach $108.90 billion by 2032 growing at a CAGR of 15.2% during the forecast period. Cybersecurity within Telecom & IT is increasingly essential as networks broaden, cloud systems evolve, and digital ecosystems become deeply interconnected. Telecom environments process highly valuable data, exposing them to frequent threats like ransomware, DDoS attacks, and sophisticated intrusions. To defend operations, companies now deploy advanced encryption tools, zero-trust security models, AI-based monitoring, and automated response workflows. Securing 5G networks, edge platforms, and software-defined network elements has also become a major strategic focus. Compliance-driven protocols, real-time analytics, and strict access-control mechanisms further strengthen overall protection. Collectively, these initiatives help maintain operational stability, safeguard user information, and uphold the security of vital digital communication infrastructures.

According to Sysdig's Global Cloud Threat Report, the telecommunications industry was the most targeted sector by cyberattackers in 2023, accounting for 38% of all tracked attacks. This highlights how telecom networks, due to their complexity and reliance on cloud services, have become prime targets for cybercriminals.

Market Dynamics:

+357 96 030922
info@marketpublishers.com

Driver:

Rising frequency & sophistication of cyber attacks

A major force behind the Cyber security for Telecom & IT Market is the accelerating surge in complex cyber attacks aimed at digital communication systems. With telecom networks handling enormous volumes of sensitive and real-time data, adversaries increasingly deploy ransom ware campaigns, large-scale DDoS strikes, and stealthy persistent intrusions. The evolution toward cloud-native systems, virtualized networks, and IP-centric architectures widens exposure points and strengthens the need for smarter protection. Consequently, enterprises focus on AI-enabled analytics, proactive surveillance, and zero-trust environments to safeguard operations. This intensifying threat landscape directly fuels demand for comprehensive cyber security platforms, driving operators to adopt advanced countermeasures to protect infrastructure integrity and service continuity.

Restraint:

High cost of advanced cybersecurity solutions

A significant limitation for the Cybersecurity for Telecom & IT Market is the considerable expense associated with advanced protection technologies. Deploying sophisticated threat intelligence tools, AI-powered monitoring systems, and robust 5G security frameworks demands high capital investment. Many mid-sized and small telecom providers struggle to fund qualified cybersecurity teams, ongoing maintenance, and consistent technology upgrades. Compliance with global and regional regulations also raises financial requirements. Moreover, integrating modern security architectures within outdated telecom networks increases implementation costs. These financial challenges hinder the adoption of cutting-edge cybersecurity solutions, especially across developing regions, slowing market penetration despite the rising urgency for strong cyber defense.

Opportunity:

Rising demand for cloud security & virtualized network protection

The growing move toward cloud-native networks and virtualized telecom infrastructures presents strong market opportunities for cybersecurity providers. As operators embrace multi-cloud, hybrid systems, and software-defined technologies, safeguarding cloud

+357 96 030922
info@marketpublishers.com

cores, containerized applications, APIs, and orchestration layers becomes increasingly critical. This shift fuels demand for cloud security services, identity management platforms, DevSecOps automation, and continuous compliance monitoring. Additionally, NFV and SDN technologies create avenues for virtualized firewalls, AI-based detection tools, and cloud-delivered security layers. These needs support the development of scalable, flexible, subscription-based cybersecurity offerings. As telecom networks evolve into cloud-centric ecosystems, the market for advanced, adaptive security solutions expands substantially.

Threat:

Escalating sophistication of cyberattacks

Rising cyberattack sophistication poses a major threat to the Cybersecurity for Telecom & IT Market. Attackers increasingly deploy AI-powered malware, automated exploitation tools, and coordinated multi-layer breaches targeting telecom infrastructures. As networks evolve toward cloud-native, API-driven, and IoT-rich environments, security gaps appear across virtualized cores and edge systems. These complex attacks often evade traditional defenses, resulting in large-scale data leaks, operational downtimes, and compromised services. The rapid advancement of criminal and state-backed cyber groups further escalates risks, forcing telecom and IT operators to continually upgrade their defenses. This ongoing escalation threatens overall network trust and heightens long-term vulnerability across digital ecosystems.

Covid-19 Impact:

The Covid-19 pandemic reshaped the Cybersecurity for Telecom & IT Market by dramatically expanding remote operations and increasing reliance on digital communication networks. As organizations adopted cloud services, video conferencing, and remote access tools at unprecedented speed, new security gaps emerged across devices, applications, and distributed networks. Cybercriminals exploited this environment through sophisticated phishing campaigns, targeted ransomware, and attacks on home-based connectivity. These disruptions pushed telecom and IT providers to enhance identity management, secure remote access, and deploy intelligent threat-detection platforms. Although the crisis created operational strain, it accelerated long-term cybersecurity adoption, boosting demand for robust, flexible, and automated protection frameworks.

The services segment is expected to be the largest during the forecast period

+357 96 030922
info@marketpublishers.com

The services segment is expected to account for the largest market share during the forecast period due to the growing need for expert-led protection across increasingly complex telecom networks. As threats intensify and infrastructures expand to cloud, IoT, and 5G environments, organizations depend heavily on managed security services, continuous monitoring, rapid incident handling, and risk-based advisory support. These services help telecom providers overcome workforce shortages, streamline security integration, and ensure consistent regulatory compliance. Additionally, service teams enable deployment of advanced analytics, automated defense tools, and multi-layered security models across diverse architectures. This sustained reliance on specialized security expertise makes services the most dominant segment in the market.

The cloud security segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud security segment is predicted to witness the highest growth rate due to the sector's expanding reliance on cloud-enabled environments and virtual network layers. As operators migrate operations to hybrid and multi-cloud systems, safeguarding containers, APIs, cloud cores, and orchestrated services becomes increasingly critical. The integration of cloud technologies into 5G, IoT, and software-defined frameworks creates new security requirements that demand advanced, flexible solutions. Cloud Security platforms offer automated compliance, strong encryption, identity-centric controls, and AI-driven monitoring tailored for dynamic cloud settings. With telecom infrastructures continually evolving toward cloud-first models, the need for advanced cloud defense grows rapidly.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, owing to its robust telecom infrastructure, pioneering adoption of 5G, and a large concentration of top cyber security firms. Frequent cyber threats in the region, combined with strict regulatory mandates, drive telecom and IT companies to allocate substantial resources toward protection technologies. A significant part of this demand comes from managed security services, continuous threat monitoring, and zero-trust strategies, bolstered by strong cooperation between the private sector and governments. These combined dynamics cement North America's role as the leading regional power in telecom-security investments.

Region with highest CAGR:

+357 96 030922
info@marketpublishers.com

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, owing to its rapid digitization, widespread 5G rollout, and booming mobile and internet usage in major economies like India and China. These developments compel telecom and IT providers to invest heavily in next-generation security tools — for instance, cloud-focused defenses, identity control systems, and real-time threat analysis. In addition, supportive government policies for digitalization and cyber regulation strongly boost the demand for telecom-specific cyber security solutions throughout the region.

Key players in the market

Some of the key players in Cybersecurity for Telecom & IT Market include Palo Alto Networks, CrowdStrike, IBM Corporation, Cisco Systems, Broadcom, Rapid7, McAfee, Fortinet, Microsoft, Sophos, Kaspersky Lab, Verizon Communications, AT&T, Trend Micro and Velox Solutions.

Key Developments:

In October 2025, IBM announced that it has signed a definitive agreement to acquire Cognitus, a leading SAP S/4HANA services provider, with industry-specific, AI-powered solutions. Cognitus will bring mission-critical SAP skills, including in RISE and GROW with SAP, as well as an extensive portfolio of software assets.

In September 2025, CrowdStrike and Redington announce new distribution agreement to accelerate cybersecurity transformation across India. This partnership strengthens Redington’s channel reach, expands CrowdStrike’s regional channel ecosystem, and enables Redington’s partner base of leading resellers to drive vendor consolidation and stop breaches with cybersecurity’s leading platform for the AI era.

In July 2025, Palo Alto Networks® announced that they have entered into a definitive agreement under which Palo Alto Networks will acquire CyberArk. Under the terms of the agreement, CyberArk shareholders will receive $45.00 in cash and 2.2005 shares of Palo Alto Networks common stock for each CyberArk share. This represents an equity value of approximately $25 billion for CyberArk and a 26% premium to the unaffected 10-day average of the daily VWAPs of CyberArk.

Components Covered:

+357 96 030922
info@marketpublishers.com

- Hardware
- Software
- Services

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Identity & Access Security

Deployment Modes Covered:

- On-Premise
- Cloud

Organization Sizes Covered:

- Small & Medium Enterprises (SMEs)
- Large Enterprises

Security Layers Covered:

- Physical Layer
- Network Layer

+357 96 030922
info@marketpublishers.com

- Application Layer

End Users Covered:

- Telecom Service Providers
- IT Enterprises
- E-commerce & Digital Platforms
- Utilities
- Government & Defense

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain

+357 96 030922
info@marketpublishers.com

- Rest of Europe
- Asia Pacific
  - Japan
  - China
  - India
  - Australia
  - New Zealand
  - South Korea
  - Rest of Asia Pacific
- South America
  - Argentina
  - Brazil
  - Chile
  - Rest of South America
- Middle East & Africa
  - Saudi Arabia
  - UAE
  - Qatar
  - South Africa
  - Rest of Middle East & Africa

+357 96 030922
info@marketpublishers.com

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 GLOBAL CYBERSECURITY FOR TELECOM & IT MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cybersecurity for Telecom & IT Market Forecasts to 2032 – Global Analysis By Component (Hardware, Software and Services), Security Type, Deployment Mode, Organization Size, Security Layer, End User and By Geography

Product link: https://marketpublishers.com/r/C74E80728923EN.html

Price: US$ 4,150.00 (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/C74E80728923EN.html