+357 96 030922
info@marketpublishers.com

Telecom Network Security Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Network Type, Application, End User and By Geography

https://marketpublishers.com/r/T74A8BB2F110EN.html
Date: May 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: T74A8BB2F110EN

Abstracts

According to Stratistics MRC, the Global Telecom Network Security Market is accounted for $5.9 billion in 2026 and is expected to reach $28.4 billion by 2034 growing at a CAGR of 21.7% during the forecast period. Telecom network security refers to comprehensive cybersecurity solutions and managed services encompassing threat detection platforms, network perimeter protection systems, signaling security gateways, fraud management solutions, and security operations center capabilities deployed across telecommunications infrastructure including core networks, radio access networks, internet peering points, and customer-facing service platforms to protect operator network assets, subscriber data, and service continuity from evolving cyber threats targeting telecommunications infrastructure and the enterprise customers dependent on operator network connectivity.

Market Dynamics:

Driver:

5G Network Attack Surface Expansion

Fifth-generation network deployment substantially expanding telecommunications attack surface through cloud-native core network functions, network slicing architecture, massive IoT device connectivity, and distributed mobile edge computing infrastructure creates compelling operator investment drivers for comprehensive network security platforms addressing new threat vectors absent in legacy network generations. 5G

+357 96 030922
info@marketpublishers.com

service-based architecture exposing network functions through open APIs and containerized microservices introducing software vulnerability exploitation risks that traditional telecommunications security approaches designed for hardware-centric network architectures cannot adequately address.

Restraint:

Security Operations Talent Scarcity

Telecommunications industry facing persistent shortage of qualified cybersecurity professionals with specialized expertise in telecom network protocols, signaling security, and carrier-grade security platform operations creates workforce constraint limiting operator ability to effectively deploy and manage advanced network security solutions. Security talent competition from financial services, technology, and defense sectors offering premium compensation packages reduces telecommunications operator capacity to maintain expert security operations teams required for proactive threat hunting, incident response, and continuous security posture management.

Opportunity:

Enterprise Security-as-a-Service Revenue

Telecommunications operators leveraging network visibility and security infrastructure investments to deliver managed security services including threat intelligence, DDoS mitigation, secure connectivity, and security operations center capabilities to enterprise customers represent high-margin revenue opportunity beyond traditional connectivity services. Operator network positioning enabling unique security service capabilities including network-level threat blocking, subscriber traffic analysis, and edge security enforcement that cloud-delivered security services cannot replicate creating differentiated managed security service offerings commanding premium enterprise contract values.

Threat:

Sophisticated State-Sponsored Attack Campaigns

Nation-state threat actors targeting telecommunications infrastructure for intelligence collection, critical infrastructure disruption, and supply chain compromise through advanced persistent threat campaigns employing zero-day vulnerabilities, supply chain

+357 96 030922
info@marketpublishers.com

implants, and long-duration network infiltration techniques that exceed conventional security solution detection capabilities create escalating security investment requirements for operators managing national communications infrastructure serving government, military, and critical industry customers requiring enhanced threat protection.

Covid-19 Impact:

COVID-19 pandemic accelerating remote workforce deployment substantially increased enterprise VPN traffic, remote access infrastructure exposure, and attack surface across telecommunications networks serving enterprise customers transitioning to distributed work models. Post-pandemic enterprise hybrid work permanence maintaining elevated network security investment requirements and operator managed security service demand as enterprise organizations seek comprehensive network protection for geographically dispersed workforces dependent on telecommunications connectivity for business operations.

The 5G Network Security segment is expected to be the largest during the forecast period

The 5G Network Security segment is expected to account for the largest market share during the forecast period, due to the accelerating commercial 5G deployment globally requiring comprehensive security architecture addressing cloud-native core network protection, network slicing isolation, open RAN interface security, and mobile edge computing application security that telecommunications operators must implement to protect 5G service revenue, enterprise customer data, and national critical communications infrastructure from escalating cyber threat activity.

The IoT Security segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the IoT Security segment is predicted to witness the highest growth rate, driven by explosive growth in IoT device connectivity across consumer, industrial, and smart city applications creating billions of network endpoints with diverse security postures requiring telecommunications operator network-level security enforcement, device authentication, and anomalous behavior detection capabilities that protect network infrastructure integrity and enterprise customer environments from IoT-originated attack campaigns.

+357 96 030922
info@marketpublishers.com

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to stringent regulatory requirements for telecommunications security including FCC cybersecurity mandates, advanced threat environment from nation-state and criminal actors targeting US communications infrastructure, significant enterprise security spending driving managed security service demand, and leading security technology vendors including Palo Alto Networks, CrowdStrike, and Fortinet generating substantial North American telecommunications security revenue.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, due to rapid 5G network deployment across China, Japan, South Korea, and India expanding telecommunications security investment requirements, growing regulatory mandates for telecommunications cybersecurity across Asian markets, increasing sophisticated cyber attack activity targeting regional telecommunications infrastructure, and strong government digital security investment programs creating favorable policy environments for telecom network security solution deployment.

Key players in the market

Some of the key players in Telecom Network Security Market include Cisco Systems, Palo Alto Networks, Fortinet, Check Point Software, Ericsson, Nokia, Huawei Technologies, ZTE Corporation, IBM Security, Tata Communications, Syniverse Technologies, TELARIX, Subex Limited, Mobileum, and Anam Technologies.

Key Developments:

In April 2026, Palo Alto Networks launched a specialized telecommunications network security platform combining 5G core network protection, signaling security monitoring, and AI-driven threat detection capabilities specifically designed for cloud-native telecommunications operator security operations center deployment.

In February 2026, Ericsson introduced an enhanced network security management solution for 5G operators incorporating real-time threat intelligence feeds, automated security policy enforcement, and cross-domain security analytics spanning radio access, transport, and core network infrastructure.

+357 96 030922
info@marketpublishers.com

Components Covered:

- Solutions
- Services

Security Types Covered:

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

Deployment Modes Covered:

- On-Premises
- Cloud-Based
- Hybrid Deployment

Network Types Covered:

- Legacy Telecom Networks
- IP-Based Networks
- Software-Defined Networking (SDN) Security

+357 96 030922
info@marketpublishers.com

Network Functions Virtualization (NFV) Security

5G Network Security

Applications Covered:

Mobile Network Security

Fixed Network Security

IoT Security

5G Network Security

Core Network Security

Edge Network Security

End Users Covered:

Telecom Operators

Internet Service Providers (ISPs)

Enterprises

Managed Security Service Providers (MSSPs)

Government & Regulatory Bodies

Regions Covered:

North America

US

+357 96 030922
info@marketpublishers.com

- Canada
- Mexico

Europe

- Germany
- UK
- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil

+357 96 030922
info@marketpublishers.com

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

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 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2032 and 2034
- 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)

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

13 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

14 COMPANY PROFILES

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Telecom Network Security Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Network Type, Application, End User and By Geography

Product link: https://marketpublishers.com/r/T74A8BB2F110EN.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/T74A8BB2F110EN.html