

Telecommunications Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2025 - 2030)  
Industry: Cybersecurity  
URL: <https://www.mordorintelligence.com/industry-reports/telecommunications-cybersecurity-market>

Telecommunications Cybersecurity Market Size and ShareMarket OverviewStudy Period | 2019 - 2030 |  
Market Size (2025) | USD 45.23 Billion |  
Market Size (2030) | USD 78.42 Billion |  
Growth Rate (2025 - 2030) | 11.63 % |  
Fastest Growing Market | Asia Pacific |  
Largest Market | North America |  
Market Concentration | Medium |  
Major Players\*Disclaimer: Major Players sorted in no particular order

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Telecommunications Cybersecurity Market Analysis by Mordor IntelligenceThe telecommunications cybersecurity market size stood at USD 45.23 billion in 2025 and is set to advance to USD 78.42 billion by 2030, translating into an 11.63% CAGR over the forecast period. Rising 5G roll-outs, expanding cloud adoption, and stricter global data-protection mandates are combining to reposition network security from a cost center to a board-level priority. Tier-1 carriers are allocating a growing share of their annual network budgets to zero-trust controls, while smaller mobile virtual network operators (MVNOs) are embracing consumption-based service models that lower capital intensity. Demand is further lifted by intensified state-sponsored intrusions and highly automated fraud campaigns that exploit signalling weaknesses, prompting operators to consolidate point tools into integrated security platforms. 0-RAN security certification schemes are also accelerating platform convergence, as carriers aim to simplify vendor management and gain uniform policy visibility across physical, virtual, and cloud domains. As a result, the telecommunications cybersecurity market is expected to remain one of the fastest-compounding segments in the wider enterprise security landscape.

Key Report Takeaways\* By Managed Security Services captured 34.81% of telecommunications cybersecurity market share in 2024, whereas Security Analytics/SIEM logged the highest projected growth at 13.74% CAGR through 2030.

\* By Cloud deployment models commanded 44.31% share of the telecommunications cybersecurity market size in 2024, but hybrid approaches are forecast to scale at 19.02% CAGR to 2030 thanks to data-sovereignty and latency requirements.

\* Tier-1 communication service providers (CSPs) held 64.72% of global demand in 2024; regional and MVNO operators are expected to expand at 14.08% CAGR and influence purchasing toward SaaS-based delivery.

\* By Control-Plane Security accounted for 19.81% share of the telecommunications cybersecurity market in 2024, while Signalling Security is on track for an 18.54% CAGR through 2030 as 5G network slicing multiplies signalling domains.

\* By North America led with 32.85% regional share in 2024; Asia-Pacific is forecast to outpace all regions with a 14.73% CAGR, propelled by large-scale 5G investments and new cyber-safety laws.

Note: Market size and forecast figures in this report are generated using Mordor Intelligence's proprietary estimation framework, updated with the latest available data and insights as of January 2026.

Market Trends and InsightsDrivers Impact Analysis of Telecommunications Cybersec

urity Market\*Driver | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |

Surge in 5G roll-outs expanding attack surface | +2.8% | Global, with concentration in North America, Europe, and APAC | Medium term (2-4 years) |

Heightened global and national data-protection mandates | +2.1% | Global, with strongest impact in EU and North America | Short term ( $\leq 2$  years) |

Escalating telecom fraud (SIM-swap, DDoS) incidents | +1.9% | Global, with particular severity in North America and Europe | Short term ( $\leq 2$  years) |

Cloud-native and NFV adoption requiring zero-trust controls | +1.7% | Global, led by developed markets | Medium term (2-4 years) |

Satellite backhaul vulnerabilities driving new spend | +1.2% | Global, with focus on remote and underserved regions | Long term ( $\geq 4$  years) |

Open RAN security-certification programs accelerating tools uptake | +0.9% | North America, Europe, and select APAC markets | Medium term (2-4 years) |

Source: Mordor Intelligence |

Surge in 5G roll-outs expanding attack surfaceCommercial 5G networks are deployed with service-based architectures that decouple control and user planes, multiplying potential entry points compared with legacy 4G designs.[1]Heidi Adams, "Securing 5G with AI," Nokia, nokia.com Network slicing creates logically isolated sub-networks that each require bespoke policy enforcement, thereby lifting demand for Security Analytics/SIEM able to correlate anomalies across thousands of virtual instances. Distributed edge nodes push critical functions closer to users, forcing carriers to secure far-flung micro-data-centers and radio units. Operators now dedicate 15-20% of new-build budgets to security versus 8-12% under 4G, which is directly fueling the telecommunications cybersecurity market. Vendors able to automate policy orchestration across slices and regions are therefore gaining competitive traction.

Heightened global and national data-protection mandatesThe European Union's NIS2 Directive obliges telecom entities to report incidents within 24 hours and introduces fines up to EUR 10 million (USD 11 million) for non-compliance, driving urgent upgrades in monitoring and identity management.[2]ENISA, "Supporting NIS2 Implementation Through Actionable Guidance," enisa.europa.eu India's Digital Personal Data Protection Act imposes breach reporting within six hours and penalties of up to 4% of global turnover, extending regulatory pressure into Asia. In the United States, the Federal Communications Commission activated stricter SIM-swap controls in July 2024, making multi-factor authentication mandatory for number-porting processes.[3]Federal Communications Commission, "FCC Announces Effective Compliance Date for SIM Swapping Item," fcc.gov Collectively, these statutes force operators to prove granular access control and real-time visibility, sustaining double-digit growth in IAM and analytics tools within the telecommunications cybersecurity market.

Escalating telecom fraud (SIM-swap, DDoS) incidentsSIM-swap cases rose 40% over 2023-2024, enabling criminals to intercept SMS-based one-time passwords and gain account takeovers that ripple into banking and cryptocurrency platforms. The high-profile hack of the U.S. SEC's X account revealed how telecom weaknesses can disrupt capital markets and inflate digital-asset prices within minutes. State-sponsored actors, such as China-linked Salt Typhoon, have infiltrated major U.S. carriers to harvest subscriber data. These incidents elevate board-level risk perception, accelerate AI-driven anomaly detection roll-outs, and solidify the telecommunications cybersecurity market as a top spending priority.

Cloud-native and NFV adoption requiring zero-trust controlsAs network-function virtualization spreads, 96% of operators cite elevated cloud-security concerns, particularly around service-based APIs that broker inter-function communications. 3GPP standards mandate mutual TLS across 5G core functions, expanding the scope of certificate lifecycle management. Yet enforcing 256-bit ciphers can add latency unless offset by hardware acceleration, encouraging adoption of inline crypto appliances and software-defined security orchestrators able to balance throughput and trust. This transition places zero-trust architectures at the heart of the telecommunications cybersecurity market.

Restraints Impact Analysis of Telecommunications Cybersecurity Market\*  
Restraint | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |  
Legacy-network budget constraints | -1.8% | Global, with particular impact in emerging markets and smaller operators | Medium term (2-4 years) |  
Shortage of telecom-focused cyber-talent | -1.4% | Global, with acute shortages in developed markets | Long term ( $\geq 4$  years) |  
Multi-vendor integration complexity | -0.8% | Global, with highest impact in North America and Europe | Medium term (2-4 years) |  
Encryption export-control limits in emerging markets | -0.6% | Emerging markets, particularly in Asia-Pacific, Middle East, and Africa | Short term ( $\leq 2$  years) |

Source: Mordor Intelligence |

Legacy-network budget constraints Operators must sustain PSTN and 3G footprints even as they fund 5G core upgrades, creating allocation trade-offs that slow security refresh cycles. Legacy switches often lack modern logging capability, complicating end-to-end threat visibility and forcing carriers to accept higher residual risk or accelerate decommissioning. Capital rationing is most acute in emerging markets where ARPU remains flat, restraining nearer-term growth in the telecommunications cybersecurity market.

Shortage of telecom-focused cyber-talent Eighty-nine percent of carriers anticipate staffing shortfalls in 2025, especially in protocol-aware security operations and 5G core engineering. Candidates with combined telecom and cyber skills command premium salaries, inflating operational cost structures. The scarcity fuels outsourcing to managed security service providers (MSSPs), but also delays complex on-premise deployments, softening top-line growth potential.

\*Our forecasts treat driver/restraint impacts as directional, not additive. The impact forecasts reflect baseline growth, mix effects, and variable interactions.

-----  
Telecommunications Cybersecurity Market Segment Analysis  
By Solution Type: Managed Services Lead Platform Consolidation  
Managed Security Services held a 34.81% telecommunications cybersecurity market share in 2024 as operators sought 24 x 7 monitoring without expanding internal headcount. Security Analytics/SIEM is projected to accelerate at 13.74% CAGR through 2030, spurred by compulsory log retention and real-time threat-hunting tied to national incident-reporting deadlines.

The shift toward software-defined networks increases the attack surface at both container and microservice layers, elevating demand for specialized application, cloud, and data-encryption controls. Vendors integrating firewall, DDoS, IAM, and lawful-interception features onto single dashboards are best positioned, as carriers move to simplify tool sprawl and shrink mean time to detect across their telecommunications cybersecurity market deployments.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.  
By Deployment Mode: Hybrid Models Balance Control and Scalability  
Cloud-delivered offerings secured 44.31% share of the telecommunications cybersecurity market size in 2024, riding operator enthusiasm for elastic compute and automated updates. Yet hybrid architectures are expected to post a 19.02% CAGR by 2030 because latency-sensitive traffic and sovereign-data mandates keep certain control-plane workloads on-premise.

Carriers such as BT and Deutsche Telekom segment workloads across private cores and public IaaS, orchestrating policy via centralized security-as-code templates. This design reduces over-provisioning while retaining local packet inspection at edge sites, demonstrating a pragmatic path for broad-scale adoption throughout the telecommunications cybersecurity market.

By Organization Size: Tier-1 Dominance Drives Innovation Investment Tier-1 CSPs represented 64.72% of 2024 spending, often deploying bespoke architectures financed through multi-year transformation budgets. In contrast, regional and MVNO players are forecast to increase outlays at 14.08% CAGR by adopting standardized SECaaS bundles that scale with subscriber growth and reduce initial capex.

The divergence creates a two-speed purchasing environment: global majors pioneer AI-driven threat-intel fusion, while challengers favor turnkey ISO-mapped controls. Both cohorts, however, prioritize rapid compliance with the same statutory frameworks, keeping the overall telecommunications cybersecurity market on a consistent growth arc.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By Security Layer: Control-Plane Dominance Faces Signalling Challenges Control-Plane Security contributed 19.81% of 2024 revenue, safeguarding session management and route selection that underpin service continuity [3gpp.org]. Signalling-layer tools are on track for an 18.54% CAGR as slice-specific signalling in 5G-SA demands granular inspection and anomaly detection.

Layer integration is becoming non-optional; packet analyzers must correlate physical-layer eavesdropping, transport-layer injection, and application-layer API abuse under unified analytics. Vendors demonstrating low-latency encryption inline with carrier-grade throughput are attracting premium valuations within the telecommunications cybersecurity market.

-----

Geography Analysis North America Telecommunications Cybersecurity Market North America accounted for 32.85% of global revenue in 2024 as the FCC tightened SIM-swap regulations and large operators-Verizon among them-publicly linked brand trust to cyber-resilience investments. Mature adoption of IAM and analytics suites, coupled with early open-RAN pilots, ensures steady but more incremental growth relative to emerging regions.

Europe Telecommunications Cybersecurity Market Europe's cohesive NIS2 legislation harmonizes expectations across 27 member states, compelling both incumbent and challenger carriers to level-set risk management protocols. Delays in national transpositions have added compliance uncertainty, yet also intensify urgency to deploy market-ready controls once final rules crystallize. Hybrid deployment preference is pronounced, reflecting GDPR-driven data-residency policies that shape purchasing across the telecommunications cybersecurity market.

APAC Telecommunications Cybersecurity Market Asia-Pacific delivers the highest trajectory at 14.73% CAGR through 2030, propelled by India's USD 250 million federal cyber-budget and Japan's domestic supply-chain imperatives that channel spend into local ecosystem partners. Massive 5G base-station roll-outs in China, India, and Indonesia translate into fresh attach opportunities for cloud-native security services, positioning the region as the primary engine of incremental revenue for the telecommunications cybersecurity market.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

-----

### Competitive Landscape

The market remains moderately fragmented: network-equipment titans such as Cisco, Nokia, and Ericsson leverage embedded footprints to upsell security modules, while pure-play cyber firms-including Palo Alto Networks and Fortinet-compete on behavioral analytics and machine-learning efficacy. Consolidation is gathering pace; 2024-2025 witnessed deals like CyberArk's USD 1.54 billion Venafi acquisition that fold machine-identity management into privileged-access portfolios, sign

aling a drive toward integrated stacks.

Open-RAN standardization unsettles traditional procurement by lowering switching costs between radio vendors. New entrants capitalizing on open interfaces can differentiate on security, not legacy hardware lock-in, injecting competitive pressure that ultimately widens solution choice for carriers. Meanwhile, innovation races around quantum-safe encryption and AI-generated attack simulations are giving rise to specialist firms that, while niche today, could reshape value pools within the telecommunications cybersecurity market if their technologies mature into carrier-grade form factors.

Vendor success increasingly hinges on providing demonstrable return on risk-mitigation spend-quantified in faster incident resolution, lower fraud losses, and verified compliance adherence. Those able to evidence such metrics through unified dashboards and outcome-based SLAs are earning premium share of wallet across buyer segments, reinforcing the strategic evolution of the telecommunications cybersecurity industry.

Telecommunications Cybersecurity Industry Leaders\* Cisco Systems, Inc.

\* Huawei Technologies Co., Ltd.

\* Nokia Corporation

\* Telefonaktiebolaget LM Ericsson

\* Juniper Networks, Inc.

\* \*Disclaimer: Major Players sorted in no particular order

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. Telecommunications Cybersecurity Market Companies Covered in this Report\* Cisco Systems, Inc.

\* Huawei Technologies Co., Ltd.

\* Nokia Corporation

\* Telefonaktiebolaget LM Ericsson

\* Juniper Networks, Inc.

\* Palo Alto Networks, Inc.

\* Fortinet, Inc.

\* Check Point Software Technologies Ltd.

\* AdaptiveMobile Security Ltd.

\* Allot Ltd.

\* Sandvine Corporation

\* Radware Ltd.

\* ZTE Corporation

\* A10 Networks, Inc.

\* BAE Systems plc

\* Spirent Communications plc

\* NETSCOUT Systems, Inc.

\* F-Secure Corporation

\* Dell Technologies Inc.

\* Oracle Corporation

\* IBM Corporation

-----  
Recent Industry Developments in Telecommunications Cybersecurity Market\* May 2025: KDDI and NEC formed a strategic cybersecurity alliance to localize supply-chain assurance and co-develop 5G security appliances, reinforcing Japan's push for self-reliant critical-infrastructure protection while opening cross-selling routes for NEC's AI analytics stack.

\* March 2025: NTT Communications disclosed unauthorized access affecting 18,000 enterprise clients; the breach is prompting regional carriers to harden third-party

ty governance frameworks and creating near-term demand for continuous-monitoring services that verify partner access paths.

- \* January 2025: The Global Coalition on Telecommunications issued open-RAN certification principles, giving operators a blueprint for security validation that could compress time-to-deploy for multivendor RAN environments and stimulate investment in automated compliance-testing tools.
- \* December 2024: The European Commission launched infringement actions against 23 member states for late NIS2 adoption; uncertainty is pushing operators to accelerate interim controls and engage professional-service partners to interpret evolving legal obligations.

-----

## Table of Contents for Telecommunications Cybersecurity Industry Report1. INTRODUCTION

- \* 1.1 Study Assumptions and Market Definition

- \* 1.2 Scope of the Study

### 2. RESEARCH METHODOLOGY

### 3. EXECUTIVE SUMMARY

### 4. MARKET LANDSCAPE

- \* 4.1 Market Overview

- \* 4.2 Market Drivers\* 4.2.1 Surge in 5G roll-outs expanding attack surface

- \* 4.2.2 Heightened global and national data-protection mandates

- \* 4.2.3 Escalating telecom fraud (SIM-swap, DDoS) incidents

- \* 4.2.4 Cloud-native and NFV adoption requiring zero-trust controls

- \* 4.2.5 Satellite backhaul vulnerabilities driving new spend

- \* 4.2.6 Open RAN security-certification programs accelerating tools uptake

- \* 4.3 Market Restraints\* 4.3.1 Legacy-network budget constraints

- \* 4.3.2 Shortage of telecom-focused cyber-talent

- \* 4.3.3 Multi-vendor integration complexity

- \* 4.3.4 Encryption export-control limits in emerging markets

- \* 4.4 Value Chain Analysis

- \* 4.5 Regulatory Landscape

- \* 4.6 Technological Outlook

- \* 4.7 Porter's Five Forces Analysis\* 4.7.1 Competitive Rivalry

- \* 4.7.2 Threat of New Entrants

- \* 4.7.3 Bargaining Power of Suppliers

- \* 4.7.4 Bargaining Power of Buyers

- \* 4.7.5 Threat of Substitutes

### 5. MARKET SIZE AND GROWTH FORECASTS (VALUES)

- \* 5.1 By Solution Type\* 5.1.1 Network Security

- \* 5.1.2 Application Security

- \* 5.1.3 Cloud and Virtualization Security

- \* 5.1.4 Data and Encryption Security

- \* 5.1.5 Identity and Access Management

- \* 5.1.6 Security Analytics/SIEM

- \* 5.1.7 Managed Security Services

- \* 5.1.8 Lawful Interception Solutions

- \* 5.2 By Deployment Mode\* 5.2.1 On-Premise

- \* 5.2.2 Cloud

- \* 5.2.3 Hybrid

- \* 5.3 By Organization Size\* 5.3.1 Tier-1 CSPs / Large Telecom Groups

- \* 5.3.2 Regional and MVNO / SME Operators
- \* 5.4 By Security Layer\* 5.4.1 Physical Layer Security
- \* 5.4.2 Transport Layer
- \* 5.4.3 Signalling Security
- \* 5.4.4 Application Layer Security
- \* 5.4.5 Control-Plane Security

## \* 5.5 By Geography\* 5.5.1 North America

- \* 5.5.1.1 United States
- \* 5.5.1.2 Canada
- \* 5.5.1.3 Mexico
- \* 5.5.2 Europe
- \* 5.5.2.1 United Kingdom
- \* 5.5.2.2 Germany
- \* 5.5.2.3 France
- \* 5.5.2.4 Italy
- \* 5.5.2.5 Spain
- \* 5.5.2.6 Russia
- \* 5.5.2.7 Rest of Europe
- \* 5.5.3 Asia-Pacific
- \* 5.5.3.1 China
- \* 5.5.3.2 Japan
- \* 5.5.3.3 South Korea
- \* 5.5.3.4 India
- \* 5.5.3.5 Australia
- \* 5.5.3.6 Indonesia
- \* 5.5.3.7 Rest of Asia-Pacific
- \* 5.5.4 South America
- \* 5.5.4.1 Brazil
- \* 5.5.4.2 Argentina
- \* 5.5.4.3 Chile
- \* 5.5.4.4 Rest of South America
- \* 5.5.5 Middle East and Africa
- \* 5.5.5.1 Middle East
- \* 5.5.5.1.1 United Arab Emirates
- \* 5.5.5.1.2 Turkey
- \* 5.5.5.1.3 Saudi Arabia
- \* 5.5.5.1.4 Israel
- \* 5.5.5.1.5 Qatar
- \* 5.5.5.1.6 Rest of Middle East
- \* 5.5.5.2 Africa
- \* 5.5.5.2.1 South Africa
- \* 5.5.5.2.2 Nigeria
- \* 5.5.5.2.3 Kenya
- \* 5.5.5.2.4 Egypt
- \* 5.5.5.2.5 Rest of Africa

## 6. COMPETITIVE LANDSCAPE

- \* 6.1 Market Concentration
- \* 6.2 Strategic Moves
- \* 6.3 Market Share Analysis
- \* 6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share, Products and Services, Recent Developments)\* 6.4.1 Cisco Systems, Inc.
- \* 6.4.2 Huawei Technologies Co., Ltd.
- \* 6.4.3 Nokia Corporation
- \* 6.4.4 Telefonaktiebolaget LM Ericsson
- \* 6.4.5 Juniper Networks, Inc.
- \* 6.4.6 Palo Alto Networks, Inc.
- \* 6.4.7 Fortinet, Inc.

- \* 6.4.8 Check Point Software Technologies Ltd.
- \* 6.4.9 AdaptiveMobile Security Ltd.
- \* 6.4.10 Allot Ltd.
- \* 6.4.11 Sandvine Corporation
- \* 6.4.12 Radware Ltd.
- \* 6.4.13 ZTE Corporation
- \* 6.4.14 A10 Networks, Inc.
- \* 6.4.15 BAE Systems plc
- \* 6.4.16 Spirent Communications plc
- \* 6.4.17 NETSCOUT Systems, Inc.
- \* 6.4.18 F-Secure Corporation
- \* 6.4.19 Dell Technologies Inc.
- \* 6.4.20 Oracle Corporation
- \* 6.4.21 IBM Corporation

## 7. MARKET OPPORTUNITIES AND FUTURE OUTLOOK

### \* 7.1 White-space and Unmet-Need Assessment

-----

Global Telecommunications Cybersecurity Market Report ScopeBy Solution TypeNetwork Security |  
 Application Security |  
 Cloud and Virtualization Security |  
 Data and Encryption Security |  
 Identity and Access Management |  
 Security Analytics/SIEM |  
 Managed Security Services |  
 Lawful Interception Solutions |  
 By Deployment ModeOn-Premise |  
 Cloud |  
 Hybrid |  
 By Organization SizeTier-1 CSPs / Large Telecom Groups |  
 Regional and MVNO / SME Operators |  
 By Security LayerPhysical Layer Security |  
 Transport Layer |  
 Signalling Security |  
 Application Layer Security |  
 Control-Plane Security |  
 By GeographyNorth America | United States |  
 | Canada |  
 | Mexico |  
 Europe | United Kingdom |  
 | Germany |  
 | France |  
 | Italy |  
 | Spain |  
 | Russia |  
 | Rest of Europe |  
 Asia-Pacific | China |  
 | Japan |  
 | South Korea |  
 | India |  
 | Australia |  
 | Indonesia |  
 | Rest of Asia-Pacific |  
 South America | Brazil |  
 | Argentina |  
 | Chile |  
 | Rest of South America |  
 |

Middle East and Africa | Middle East | United Arab Emirates |

| Turkey |  
| Saudi Arabia |  
| Israel |  
| Qatar |  
| Rest of Middle East |

Africa | South Africa |

| Nigeria |  
| Kenya |  
| Egypt |  
| Rest of Africa |

By Solution Type | Network Security |

| Application Security |  
| Cloud and Virtualization Security |  
| Data and Encryption Security |  
| Identity and Access Management |  
| Security Analytics/SIEM |  
| Managed Security Services |  
| Lawful Interception Solutions |

By Deployment Mode | On-Premise |

| Cloud |  
| Hybrid |

By Organization Size | Tier-1 CSPs / Large Telecom Groups |

| Regional and MVNO / SME Operators |

By Security Layer | Physical Layer Security |

| Transport Layer |  
| Signalling Security |  
| Application Layer Security |  
| Control-Plane Security |

By Geography | North America | United States |

| Canada |  
| Mexico |

Europe | United Kingdom |

| Germany |  
| France |  
| Italy |  
| Spain |  
| Russia |  
| Rest of Europe |

Asia-Pacific | China |

| Japan |  
| South Korea |  
| India |  
| Australia |  
| Indonesia |  
| Rest of Asia-Pacific |

South America | Brazil |

| Argentina |  
| Chile |  
| Rest of South America |

Middle East and Africa | Middle East | United Arab Emirates |

| Turkey |  
| Saudi Arabia |  
| Israel |  
| Qatar |  
| Rest of Middle East |

|  |  |                |              |
|--|--|----------------|--------------|
|  |  |                |              |
|  |  | Africa         | South Africa |
|  |  | Nigeria        |              |
|  |  | Kenya          |              |
|  |  | Egypt          |              |
|  |  | Rest of Africa |              |

-----

Key Questions Answered in the ReportWhat is the current value of the telecommunications cybersecurity market? It was USD 45.23 billion in 2025 and is forecast to reach USD 78.42 billion by 2030, expanding at an 11.63% CAGR.

Which solution type leads operator spending? Managed Security Services commanded 34.81% of 2024 revenue due to 24 x 7 monitoring needs and talent shortages.

Why is hybrid deployment gaining traction? Hybrid models grow at 19.02% CAGR because they pair cloud scalability with on-premise data-sovereignty and latency benefits.

Which region is growing fastest? Asia-Pacific is projected to advance at a 14.73% CAGR through 2030, driven by large-scale 5G build-outs and new cyber mandates.

How are open-RAN standards influencing security budgets? Certification schemes are pushing carriers to integrate continuous vulnerability scanning and encrypted fronthaul, expanding spend on analytics and key-management platforms.

What is the biggest restraint on market growth? Legacy-network budget constraints subtract an estimated 1.8 percentage points from CAGR because operators must balance 5G upgrades with aging infrastructure upkeep.

-----

Related Reports Explore More Reports Find Latest Data onCybersecurity MarketUS Cybersecurity Market ForecastsGrowth Forecasts for Cybersecurity Software MarketUnited States Telecom Services MarketGovernment And Public Sector Cybersecurity MarketMEA Cybersecurity Market GrowthMarket Report on Network SecuritySouth Africa Cybersecurity Market ReportCybersecurity Insurance Market GrowthEurope Cybersecurity Market GrowthPolicy Management In Telecom Market Size