+357 96 030922
info@marketpublishers.com

Cybersecurity Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Deployment (Cloud, On-Premises, and Hybrid), Security Type, Organization Size, End User, and By Geography

https://marketpublishers.com/r/CE4936ED86F6EN.html
Date: July 2026
Pages: 0
Price: US$ 4,150.00 (Single User License)
ID: CE4936ED86F6EN

Abstracts

According to Stratistics MRC, the Global Cybersecurity Market is accounted for $265.4 billion in 2026 and is expected to reach $652.5 billion by 2034 growing at a CAGR of 11.9% during the forecast period. Cybersecurity encompasses technologies, processes, and practices designed to protect networks, devices, applications, and data from unauthorized access, cyberattacks, and damage. The market includes network security, endpoint security, cloud security, application security, data security, identity and access management, email security, IoT security, and operational technology (OT) security solutions deployed across cloud, on-premises, and hybrid environments. The rapid digitization of businesses, increasing sophistication of cyber threats, stringent regulatory requirements, and growing adoption of remote work models are key drivers of market expansion across all industry verticals.

Market Dynamics:

Driver:

Increasing frequency and sophistication of cyberattacks

The rising frequency, scale, and sophistication of cyberattacks worldwide is a primary driver for the cybersecurity market. Organizations across all sectors are facing growing threats including ransomware, phishing, advanced persistent threats, and zero-day exploits targeting sensitive data and critical infrastructure. The financial impact of data breaches continues increasing, with costs rising for incident response, regulatory fines, and reputational damage. High-profile attacks on government agencies, healthcare institutions, financial services, and major corporations have elevated cybersecurity to board-level priority. As cybercriminals adopt advanced techniques including AI-powered attacks, organizations are compelled to invest in comprehensive security solutions to protect their digital assets.

Restraint:

Shortage of skilled cybersecurity professionals

The significant global shortage of qualified cybersecurity professionals represents a major restraint for market growth. Organizations struggle to recruit and retain skilled personnel including security analysts, penetration testers, security architects, and incident responders. The skills gap limits organizations' ability to effectively deploy and manage security solutions, reducing the value of technology investments. Competition for talent drives up salaries, increasing operational costs. The shortage is particularly acute in developing regions where security education and training infrastructure is limited. This talent gap may lead organizations to delay security initiatives or adopt managed security services to compensate.

Opportunity:

Growing adoption of AI and automation in cybersecurity

The integration of artificial intelligence and automation into cybersecurity solutions presents significant opportunities for market expansion. AI-powered security enables real-time threat detection, automated incident response, and predictive analytics that identify vulnerabilities before exploitation. Machine learning algorithms analyze vast amounts of security data to detect anomalies and emerging threats faster than human analysts. Automated security orchestration reduces response times and frees security teams for higher-value activities. As AI capabilities advance and become more accessible, organizations increasingly adopt intelligent security solutions, creating substantial growth opportunities for vendors.

Threat:

Complexity of managing hybrid and multi-cloud environments

The increasing complexity of securing hybrid and multi-cloud environments poses significant threats to cybersecurity effectiveness and market growth. Organizations operate applications and data across on-premises infrastructure, multiple public cloud providers, and edge environments, each with distinct security requirements and tools. Consistent security policy enforcement across diverse environments requires sophisticated orchestration and integration. The proliferation of security tools creates management complexity and potential gaps in coverage. Compliance requirements vary across jurisdictions and cloud platforms, adding operational burden. These complexities may lead organizations to simplify architectures or delay cloud adoption, affecting security solution demand.

Covid-19 Impact:

The COVID-19 pandemic significantly accelerated cybersecurity market growth as organizations rapidly shifted to remote work models and digital services. The expansion of attack surfaces, with employees accessing corporate resources from home networks and personal devices, created new security challenges. Cybercriminals exploited pandemic-related themes in phishing and ransomware attacks. Organizations accelerated security investments to protect distributed workforces. Digital transformation initiatives were prioritized, driving cloud security and identity management adoption. Post-pandemic, hybrid work models have sustained elevated security requirements, with the crisis permanently raising cybersecurity awareness and investment levels across all sectors.

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

The Cloud segment is expected to account for the largest market share during the forecast period, driven by the accelerating migration of applications, data, and infrastructure to cloud environments. Cloud-based security solutions offer advantages including scalability, automatic updates, and reduced infrastructure management burden. Organizations are adopting cloud security platforms for comprehensive protection across public, private, and hybrid cloud environments. The shift toward security-as-a-service models and zero-trust architectures supports cloud security adoption. As organizations continue their cloud migration journeys and cloud-native security capabilities advance, the cloud deployment segment maintains the largest market share throughout the forecast period.

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, fueled by the explosive growth of connected devices across industrial, consumer, and enterprise environments. IoT devices present unique security challenges including limited computing resources, diverse protocols, and long device lifecycles. The expansion of smart manufacturing, connected healthcare devices, smart cities, and consumer IoT creates substantial demand for specialized security solutions. Regulatory requirements for IoT security are emerging, driving compliance-driven adoption. As device proliferation continues and attacks on IoT infrastructure increase, IoT security delivers the fastest segment growth.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by the high concentration of cyber threats, strong regulatory frameworks, and significant cybersecurity investment. The region's advanced digital economy and technology sector create substantial demand for security solutions. Stringent regulatory requirements including HIPAA, CCPA, and sector-specific standards drive compliance-related adoption. Strong presence of major cybersecurity vendors and continuous innovation support market growth. High cybersecurity awareness and board-level priority ensure sustained investment. With established adoption and ongoing threat landscape evolution, North America maintains its dominant market position throughout the forecast period.

Region with highest CAGR:

Over the forecast period, the Asia-Pacific region is anticipated to exhibit the highest CAGR, driven by rapid digital transformation, expanding internet and mobile penetration, and increasing cyber threats across developing economies. Countries including China, India, Japan, and Southeast Asia are experiencing growing cybersecurity investment as digital services expand. Government cybersecurity initiatives and regulations are driving adoption across public and private sectors. Rising awareness of cyber risks and the financial impact of breaches is increasing investment priorities. As the region's digital economy continues expanding and threat awareness increases, Asia Pacific delivers the fastest cybersecurity market growth globally.

Key players in the market

Some of the key players in Cybersecurity Market include Palo Alto Networks, Inc., Cisco

+357 96 030922
info@marketpublishers.com

Systems, Inc., Fortinet, Inc., Check Point Software Technologies Ltd., CrowdStrike Holdings, Inc., Trend Micro Incorporated, Broadcom Inc., IBM Corporation, Microsoft Corporation, McAfee Corp., Sophos Ltd., SentinelOne, Inc., Rapid7, Inc., Tenable Holdings, Inc., Qualys, Inc., F5, Inc., and Proofpoint, Inc.

Key Developments:

In July 2026, Check Point Software officially announced its partnership with the newly established AWS European Sovereign Cloud. Through this collaboration, Check Point's native Cloud Firewall offering became immediately available on the independent European infrastructure to deliver prevention-first security across network and application layers.

In June 2026, Palo Alto Networks finalized its structural integration of CyberArk and Chronosphere assets into its core security stack. The additions added $1.6 billion in Next-Generation Security (NGS) Annual Recurring Revenue (ARR) to its unified platform.

In June 2026, the UK's National Cyber Security Centre (NCSC) issued a critical advisory alongside global researchers regarding 'FortiBleed'—a massive brute-force and credential-stuffing campaign targeting internet-facing FortiGate firewalls and VPN gateways that resulted in leaked enterprise credential databases.

Components Covered:

- Solutions
- Services

Deployments Covered:

- Cloud
- On-Premises
- Hybrid

Security Types Covered:

- Network Security
- Endpoint Security
- Cloud Security
- Application Security
- Data Security
- Identity and Access Management
- Email Security
- IoT Security
- Operational Technology (OT) Security

Organization Sizes Covered:

- Large Enterprises
- Small and Medium Enterprises (SMEs)

End Users Covered:

- BFSI
- Government & Defense
- Healthcare
- Manufacturing
- IT & Telecommunications

+357 96 030922
info@marketpublishers.com

Retail

Energy & Utilities

Transportation & Logistics

Education

Other End Users

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

+357 96 030922
info@marketpublishers.com

- Switzerland
- Poland
- Rest of Europe

Asia Pacific

- China
- Japan
- India
- South Korea
- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore
- Vietnam
- Rest of Asia Pacific

South America

- Brazil
- Argentina
- Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of 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, 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)

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

13.4 Check Point Software Technologies Ltd.
13.5 CrowdStrike Holdings, Inc.
13.6 Trend Micro Incorporated
13.7 Broadcom Inc.
13.8 IBM Corporation
13.9 Microsoft Corporation
13.10 McAfee Corp.
13.11 Sophos Ltd.
13.12 SentinelOne, Inc.
13.13 Rapid7, Inc.
13.14 Tenable Holdings, Inc.
13.15 Qualys, Inc.
13.16 F5, Inc.
13.17 Proofpoint, Inc.

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

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

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cybersecurity Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Deployment (Cloud, On-Premises, and Hybrid), Security Type, Organization Size, End User, and By Geography

Product link: https://marketpublishers.com/r/CE4936ED86F6EN.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/CE4936ED86F6EN.html