+357 96 030922
info@marketpublishers.com

Next-generation Cybersecurity Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Offering (Solutions, Services), By Security Type (Network Security, Endpoint Security, Cloud Security, Application Security, Data Security, Others), By End User (BFSI, Healthcare, Government & Defense, Retail & E-commerce, IT & Telecom, Energy & Utilities, Manufacturing, Others), By Region, By Competition 2020-2030F

https://marketpublishers.com/r/NA60120C355BEN.html
Date: September 2025
Pages: 185
Price: US$ 4,500.00 (Single User License)
ID: NA60120C355BEN

Abstracts

The Global Next-generation Cybersecurity Market was valued at USD 21.24 Billion in 2024 and is expected to reach USD 62.54 Billion by 2030 with a CAGR of 19.72% through 2030. The Global Next-generation Cybersecurity Market represents the advanced evolution of digital security solutions designed to protect enterprises, governments, and individuals against increasingly complex cyber threats. Unlike traditional security frameworks, next-generation cybersecurity leverages technologies such as artificial intelligence, machine learning, behavioral analytics, and zero-trust architectures to provide proactive defense mechanisms. These solutions focus on real-time threat detection, advanced malware prevention, identity management, and network resilience to secure cloud environments, data centers, and endpoint devices. With digital transformation accelerating worldwide, organizations require robust security strategies to safeguard sensitive information, intellectual property, and operational continuity from sophisticated cybercriminals.

+357 96 030922
info@marketpublishers.com

This market is expected to rise due to several critical drivers, primarily the exponential increase in cyberattacks and data breaches targeting enterprises and government systems. The expansion of the Internet of Things, 5G connectivity, and cloud computing has significantly widened the attack surface, making advanced security solutions indispensable. Additionally, regulatory frameworks such as the General Data Protection Regulation in Europe and the Cybersecurity Maturity Model Certification in the United States are compelling organizations to invest in stronger cybersecurity systems. Furthermore, the integration of artificial intelligence and automation is enhancing the effectiveness of cybersecurity platforms, enabling faster response times and predictive defense against evolving threats.

The growth of the Global Next-generation Cybersecurity Market will also be fueled by the adoption of remote and hybrid work models, which increase vulnerabilities across networks and endpoints. Businesses across industries such as banking, healthcare, retail, manufacturing, and government are prioritizing next-generation solutions like cloud security, endpoint protection, and zero-trust frameworks to secure operations. With the rise of generative artificial intelligence and advanced persistent threats, cybersecurity vendors are continuously innovating to stay ahead of adversaries. Moreover, emerging economies in Asia Pacific, Latin America, and the Middle East are investing heavily in cybersecurity infrastructure to strengthen national resilience against digital threats. As a result, the Global Next-generation Cybersecurity Market is set for substantial long-term expansion, playing a pivotal role in securing the digital economy.

Key Market Drivers

Rising Sophistication and Frequency of Cyber Threats

The Global Next-generation Cybersecurity Market is being fueled by the rising scale and sophistication of cyberattacks that challenge traditional defense systems. Modern attackers employ ransomware-as-a-service, zero-day exploits, and advanced persistent threats that can bypass conventional firewalls and antivirus tools. These threats are no longer random but often highly targeted, aiming to disrupt critical infrastructure, steal sensitive data, or compromise national security. Enterprises and governments face increased vulnerability due to hyper-connected ecosystems, including cloud platforms, remote endpoints, and Internet of Things devices. Next-generation cybersecurity leverages artificial intelligence, machine learning, and behavioral analytics to detect anomalies in real time, proactively respond to threats, and reduce the window of exploitation.

+357 96 030922
info@marketpublishers.com

Organizations today also realize that the reputational and financial impact of breaches is far greater than the cost of implementing strong cybersecurity. Industries like healthcare and finance, where sensitive data is at stake, are investing heavily in zero-trust frameworks, endpoint detection, and predictive security tools. Additionally, the digital acceleration driven by 5G networks and automation has created new entry points for attackers, making it essential for businesses to integrate next-generation cybersecurity into their operational models. This evolving threat landscape makes the sophistication of cybercrime one of the most pressing growth drivers for this market. The Federal Bureau of Investigation's Internet Crime Report 2023 highlighted that cybercrime losses in the United States crossed 12.5 billion USD, a 22 percent surge from 2022. This rising financial toll demonstrates how sophisticated and persistent attacks are escalating economic risks, forcing businesses and governments to adopt next-generation cybersecurity to minimize damage.

Key Market Challenges

High Implementation and Operational Costs

One of the most significant challenges restraining the Global Next-generation Cybersecurity Market is the high cost of implementation and ongoing operations. Advanced cybersecurity tools such as zero-trust architecture, threat intelligence platforms, and artificial intelligence-powered detection systems require substantial upfront investments in infrastructure, skilled workforce, and integration. Small and medium-sized enterprises, which represent a majority of global businesses, often struggle to afford such sophisticated systems, leaving them exposed to attacks. Beyond initial costs, maintenance, upgrades, and the need for continuous monitoring further increase the financial burden. This creates a cost imbalance where larger enterprises are better positioned to invest in resilience, while smaller players remain vulnerable.

The economic challenge also extends to the scarcity of skilled cybersecurity professionals who can manage next-generation technologies effectively. Hiring or training such experts requires additional expenditure, and the global shortage of cybersecurity talent intensifies the problem. As a result, many businesses delay or limit adoption despite acknowledging the risks of cyber threats. For governments and regulators, this widening cybersecurity divide is alarming, as vulnerabilities in smaller enterprises can cascade into supply chain risks for larger corporations. While the demand for next-generation cybersecurity remains strong, cost-related hurdles significantly slow adoption, particularly in emerging markets and cost-sensitive industries.

+357 96 030922
info@marketpublishers.com

Key Market Trends

Rise of Zero-Trust Architecture Adoption

Zero-trust architecture is rapidly emerging as a dominant trend in the Global Next-generation Cybersecurity Market. Unlike traditional perimeter-based security models, zero-trust operates on the principle of “never trust, always verify,” ensuring that every access request is authenticated and authorized regardless of location or user. With the surge in cloud adoption, remote work, and mobile devices, the traditional corporate perimeter has dissolved, exposing organizations to higher risks of unauthorized access and insider threats. Zero-trust frameworks address these vulnerabilities by enforcing strict identity verification, least privilege access, and micro-segmentation across networks. This shift is increasingly viewed as an essential component of digital resilience strategies.

Organizations are also motivated to adopt zero-trust by increasing regulatory pressure and industry mandates for stronger identity and access management. Governments worldwide are issuing guidelines for zero-trust adoption in critical infrastructure, including defense, healthcare, and finance. Enterprises that once considered zero-trust as optional are now prioritizing it to minimize breaches and align with compliance requirements. With the support of vendors integrating artificial intelligence and behavioral analytics into zero-trust frameworks, adoption is expected to accelerate rapidly.

Key Market Players

Palo Alto Networks, Inc.

CrowdStrike Holdings, Inc.

Fortinet, Inc.

Check Point Software Technologies Ltd.

Zscaler, Inc.

SentinelOne, Inc.

+357 96 030922
info@marketpublishers.com

IBM Corporation

Cisco Systems, Inc.

Okta, Inc.

Darktrace Ltd.

Report Scope:

In this report, the Global Next-generation Cybersecurity Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Next-generation Cybersecurity Market, By Offering:

Solutions

Services

Next-generation Cybersecurity Market, By Security Type:

Network Security

Endpoint Security

Cloud Security

Application Security

Data Security

Others

Next-generation Cybersecurity Market, By End User:

BFSI

+357 96 030922
info@marketpublishers.com

- Healthcare
- Government & Defense
- Retail & E-commerce
- IT & Telecom
- Energy & Utilities
- Manufacturing
- Others

Next-generation Cybersecurity Market, By Region:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - Germany
  - France
  - United Kingdom
  - Italy
  - Spain
- Asia Pacific
  - China

+357 96 030922
info@marketpublishers.com

India

Japan

South Korea

Australia

Middle East & Africa

Saudi Arabia

UAE

South Africa

South America

Brazil

Colombia

Argentina

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Next-generation Cybersecurity Market.

Available Customizations:

Global Next-generation Cybersecurity Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

+357 96 030922
info@marketpublishers.com

Detailed analysis and profiling of additional market players (up to five).

+357 96 030922
info@marketpublishers.com

Contents

1. SOLUTION OVERVIEW

1.1. Market Definition
1.2. Scope of the Market
  1.2.1. Markets Covered
  1.2.2. Years Considered for Study
  1.2.3. Key Market Segmentations

2. RESEARCH METHODOLOGY

2.1. Objective of the Study
2.2. Baseline Methodology
2.3. Key Industry Partners
2.4. Major Association and Secondary Sources
2.5. Forecasting Methodology
2.6. Data Triangulation & Validation
2.7. Assumptions and Limitations

3. EXECUTIVE SUMMARY

3.1. Overview of the Market
3.2. Overview of Key Market Segmentations
3.3. Overview of Key Market Players
3.4. Overview of Key Regions/Countries
3.5. Overview of Market Drivers, Challenges, and Trends

4. VOICE OF CUSTOMER

5. GLOBAL NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

5.1. Market Size & Forecast
  5.1.1. By Value
5.2. Market Share & Forecast
  5.2.1. By Offering (Solutions, Services)
  5.2.2. By Security Type (Network Security, Endpoint Security, Cloud Security, Application Security, Data Security, Others)
  5.2.3. By End User (BFSI, Healthcare, Government & Defense, Retail & E-commerce,

+357 96 030922
info@marketpublishers.com

IT & Telecom, Energy & Utilities, Manufacturing, Others)
5.2.4. By Region (North America, Europe, South America, Middle East & Africa, Asia Pacific)
5.3. By Company (2024)
5.4. Market Map

6. NORTH AMERICA NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

6.1. Market Size & Forecast
6.1.1. By Value
6.2. Market Share & Forecast
6.2.1. By Offering
6.2.2. By Security Type
6.2.3. By End User
6.2.4. By Country
6.3. North America: Country Analysis
6.3.1. United States Next-generation Cybersecurity Market Outlook
6.3.1.1. Market Size & Forecast
6.3.1.1.1. By Value
6.3.1.2. Market Share & Forecast
6.3.1.2.1. By Offering
6.3.1.2.2. By Security Type
6.3.1.2.3. By End User
6.3.2. Canada Next-generation Cybersecurity Market Outlook
6.3.2.1. Market Size & Forecast
6.3.2.1.1. By Value
6.3.2.2. Market Share & Forecast
6.3.2.2.1. By Offering
6.3.2.2.2. By Security Type
6.3.2.2.3. By End User
6.3.3. Mexico Next-generation Cybersecurity Market Outlook
6.3.3.1. Market Size & Forecast
6.3.3.1.1. By Value
6.3.3.2. Market Share & Forecast
6.3.3.2.1. By Offering
6.3.3.2.2. By Security Type
6.3.3.2.3. By End User

7. EUROPE NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

7.1. Market Size & Forecast
7.1.1. By Value
7.2. Market Share & Forecast
7.2.1. By Offering
7.2.2. By Security Type
7.2.3. By End User
7.2.4. By Country
7.3. Europe: Country Analysis
7.3.1. Germany Next-generation Cybersecurity Market Outlook
7.3.1.1. Market Size & Forecast
7.3.1.1.1. By Value
7.3.1.2. Market Share & Forecast
7.3.1.2.1. By Offering
7.3.1.2.2. By Security Type
7.3.1.2.3. By End User
7.3.2. France Next-generation Cybersecurity Market Outlook
7.3.2.1. Market Size & Forecast
7.3.2.1.1. By Value
7.3.2.2. Market Share & Forecast
7.3.2.2.1. By Offering
7.3.2.2.2. By Security Type
7.3.2.2.3. By End User
7.3.3. United Kingdom Next-generation Cybersecurity Market Outlook
7.3.3.1. Market Size & Forecast
7.3.3.1.1. By Value
7.3.3.2. Market Share & Forecast
7.3.3.2.1. By Offering
7.3.3.2.2. By Security Type
7.3.3.2.3. By End User
7.3.4. Italy Next-generation Cybersecurity Market Outlook
7.3.4.1. Market Size & Forecast
7.3.4.1.1. By Value
7.3.4.2. Market Share & Forecast
7.3.4.2.1. By Offering
7.3.4.2.2. By Security Type
7.3.4.2.3. By End User
7.3.5. Spain Next-generation Cybersecurity Market Outlook
7.3.5.1. Market Size & Forecast

+357 96 030922
info@marketpublishers.com

7.3.5.1.1. By Value
7.3.5.2. Market Share & Forecast
7.3.5.2.1. By Offering
7.3.5.2.2. By Security Type
7.3.5.2.3. By End User

8. ASIA PACIFIC NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

8.1. Market Size & Forecast
8.1.1. By Value
8.2. Market Share & Forecast
8.2.1. By Offering
8.2.2. By Security Type
8.2.3. By End User
8.2.4. By Country
8.3. Asia Pacific: Country Analysis
8.3.1. China Next-generation Cybersecurity Market Outlook
8.3.1.1. Market Size & Forecast
8.3.1.1.1. By Value
8.3.1.2. Market Share & Forecast
8.3.1.2.1. By Offering
8.3.1.2.2. By Security Type
8.3.1.2.3. By End User
8.3.2. India Next-generation Cybersecurity Market Outlook
8.3.2.1. Market Size & Forecast
8.3.2.1.1. By Value
8.3.2.2. Market Share & Forecast
8.3.2.2.1. By Offering
8.3.2.2.2. By Security Type
8.3.2.2.3. By End User
8.3.3. Japan Next-generation Cybersecurity Market Outlook
8.3.3.1. Market Size & Forecast
8.3.3.1.1. By Value
8.3.3.2. Market Share & Forecast
8.3.3.2.1. By Offering
8.3.3.2.2. By Security Type
8.3.3.2.3. By End User
8.3.4. South Korea Next-generation Cybersecurity Market Outlook
8.3.4.1. Market Size & Forecast

+357 96 030922
info@marketpublishers.com

8.3.4.1.1. By Value
8.3.4.2. Market Share & Forecast
8.3.4.2.1. By Offering
8.3.4.2.2. By Security Type
8.3.4.2.3. By End User
8.3.5. Australia Next-generation Cybersecurity Market Outlook
8.3.5.1. Market Size & Forecast
8.3.5.1.1. By Value
8.3.5.2. Market Share & Forecast
8.3.5.2.1. By Offering
8.3.5.2.2. By Security Type
8.3.5.2.3. By End User

9. MIDDLE EAST & AFRICA NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

9.1. Market Size & Forecast
9.1.1. By Value
9.2. Market Share & Forecast
9.2.1. By Offering
9.2.2. By Security Type
9.2.3. By End User
9.2.4. By Country
9.3. Middle East & Africa: Country Analysis
9.3.1. Saudi Arabia Next-generation Cybersecurity Market Outlook
9.3.1.1. Market Size & Forecast
9.3.1.1.1. By Value
9.3.1.2. Market Share & Forecast
9.3.1.2.1. By Offering
9.3.1.2.2. By Security Type
9.3.1.2.3. By End User
9.3.2. UAE Next-generation Cybersecurity Market Outlook
9.3.2.1. Market Size & Forecast
9.3.2.1.1. By Value
9.3.2.2. Market Share & Forecast
9.3.2.2.1. By Offering
9.3.2.2.2. By Security Type
9.3.2.2.3. By End User
9.3.3. South Africa Next-generation Cybersecurity Market Outlook

+357 96 030922
info@marketpublishers.com

9.3.3.1. Market Size & Forecast
9.3.3.1.1. By Value
9.3.3.2. Market Share & Forecast
9.3.3.2.1. By Offering
9.3.3.2.2. By Security Type
9.3.3.2.3. By End User

10. SOUTH AMERICA NEXT-GENERATION CYBERSECURITY MARKET OUTLOOK

10.1. Market Size & Forecast
10.1.1. By Value
10.2. Market Share & Forecast
10.2.1. By Offering
10.2.2. By Security Type
10.2.3. By End User
10.2.4. By Country
10.3. South America: Country Analysis
10.3.1. Brazil Next-generation Cybersecurity Market Outlook
10.3.1.1. Market Size & Forecast
10.3.1.1.1. By Value
10.3.1.2. Market Share & Forecast
10.3.1.2.1. By Offering
10.3.1.2.2. By Security Type
10.3.1.2.3. By End User
10.3.2. Colombia Next-generation Cybersecurity Market Outlook
10.3.2.1. Market Size & Forecast
10.3.2.1.1. By Value
10.3.2.2. Market Share & Forecast
10.3.2.2.1. By Offering
10.3.2.2.2. By Security Type
10.3.2.2.3. By End User
10.3.3. Argentina Next-generation Cybersecurity Market Outlook
10.3.3.1. Market Size & Forecast
10.3.3.1.1. By Value
10.3.3.2. Market Share & Forecast
10.3.3.2.1. By Offering
10.3.3.2.2. By Security Type
10.3.3.2.3. By End User

+357 96 030922
info@marketpublishers.com

11. MARKET DYNAMICS

11.1. Drivers
11.2. Challenges

12. MARKET TRENDS AND DEVELOPMENTS

12.1. Merger & Acquisition (If Any)
12.2. Product Launches (If Any)
12.3. Recent Developments

13. COMPANY PROFILES

13.1. Palo Alto Networks, Inc.
  13.1.1. Business Overview
  13.1.2. Key Revenue and Financials
  13.1.3. Recent Developments
  13.1.4. Key Personnel
  13.1.5. Key Product/Services Offered
13.2. CrowdStrike Holdings, Inc.
13.3. Fortinet, Inc.
13.4. Check Point Software Technologies Ltd.
13.5. Zscaler, Inc.
13.6. SentinelOne, Inc.
13.7. IBM Corporation
13.8. Cisco Systems, Inc.
13.9. Okta, Inc.
13.10. Darktrace Ltd.

14. STRATEGIC RECOMMENDATIONS

15. ABOUT US & DISCLAIMER

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Next-generation Cybersecurity Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Offering (Solutions, Services), By Security Type (Network Security, Endpoint Security, Cloud Security, Application Security, Data Security, Others), By End User (BFSI, Healthcare, Government & Defense, Retail & E-commerce, IT & Telecom, Energy & Utilities, Manufacturing, Others), By Region, By Competition 2020-2030F

Product link: https://marketpublishers.com/r/NA60120C355BEN.html

Price: US$ 4,500.00 (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/NA60120C355BEN.html