+357 96 030922
info@marketpublishers.com

Cybersecurity in Financial Services Market Forecasts to 2032 – Global Analysis By Security Type (Network Security, Endpoint Security, Application Security, Cloud Security, Data Security & Privacy, and Other Security Types), Deployment (Cloud and On-Premises), Solution, End User and By Geography

https://marketpublishers.com/r/CC337FBD5F18EN.html
Date: September 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: CC337FBD5F18EN

Abstracts

According to Stratistics MRC, the Global Cybersecurity in Financial Services Market is accounted for $273.5 billion in 2025 and is expected to reach $623.8 billion by 2032 growing at a CAGR of 12.5% during the forecast period. Cybersecurity solutions for financial services protect banks, fintechs, and enterprises from cyber threats, data breaches, and fraud. The market includes threat detection, identity management, encryption, and compliance tools. Rising digitalization, fintech adoption, and increasing cyberattacks drive market growth. Providers focus on advanced analytics, AI-driven defense, and regulatory compliance. The market targets financial institutions, insurers, and fintech companies seeking to safeguard sensitive data, ensure operational continuity, and maintain customer trust in an increasingly digital and interconnected financial ecosystem.

According to CERT-In's Digital Threat Report 2024, the BFSI sector faces systemic cyber risks, and coordinated defense strategies are now essential to protect $3.1 trillion in digital transactions projected by 2028.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Rising frequency, sophistication, and severity of cyber attacks

Financial institutions face an accelerating onslaught of cyber attacks both in number and complexity driven by organised crime, state-sponsored actors, and monetisation techniques such as ransomware and credential theft. This escalation forces banks, insurers, and payment providers to invest heavily in detection, incident response, and zero-trust architectures to protect customer data and maintain trust. Furthermore, regulators are tightening oversight after high-profile incidents, increasing compliance demands and disclosure requirements which in turn create sustained demand for advanced security solutions and specialist vendors. Investment cycles support vendor innovation, M&A activity, and professional services growth globally.

Restraint:

Rapidly evolving threat vectors

Generative AI, deepfakes, automated attack kits, and polymorphic malware lower the barrier to sophisticated intrusion, while cloud APIs, third-party integrations, and IoT endpoints broaden the attack surface. These shifts force continuous retooling of detection, expanded telemetry, and frequent security policy changes. It increases costs and talent gaps and strain governance, compliance, and vendor management. As a result, financial firms confront higher residual risk and operational strain when trying to keep pace with adversaries.

Opportunity:

Growth in managed security services (MSS)

The rising complexity of threats and shortage of in-house security talent create a significant opportunity for managed security services (MSS). Financial institutions increasingly outsource monitoring, threat hunting, and incident response to specialised providers offering 24/7 SOC capabilities, compliance expertise, and scalable analytics. MSS providers also bundle advisory services, vulnerability management, and managed detection and response to reduce time-to-remediation, deliver predictable operating costs, and accelerate regulatory alignment. Additionally, MSS adoption allows banks and fintechs to focus on core products while leveraging economies of scale in tooling, telemetry, and threat intelligence offered by third-party specialists

Threat:

+357 96 030922
info@marketpublishers.com

Persistent cyber-attack risks and data breaches

Persistent cyber-attack risks and data breaches pose an existential threat to financial services, jeopardising customer trust, regulatory standing, and capital adequacy. Successful intrusions can trigger regulatory fines, class-action lawsuits, and prolonged remediation costs while exposing institutions to reputational damage that suppresses business growth. Additionally, secondary impacts such as payment system disruptions and fraud losses can cascade through third-party ecosystems. Boards demand stronger oversight and insurers raise premiums significantly. Consequently, organisations must sustain elevated investment in resilience, insurance, and contingency planning to protect core financial operations.

Covid-19 Impact:

The COVID-19 pandemic accelerated digital adoption across banking and payments, expanding remote access and cloud dependencies while simultaneously increasing exposure to cyber threats. Rapid migrations and stretched IT teams created misconfigurations and gaps exploited by attackers, prompting urgent investments in endpoint security, secure remote access, and cloud controls. Moreover, pandemic-driven regulatory guidance and industry collaboration boosted information sharing and crisis response. It exposed supply-chain weaknesses and elevated third-party risk management urgency.

The network security segment is expected to be the largest during the forecast period

The network security segment is expected to account for the largest market share during the forecast period because financial firms prioritise protecting high-value transaction channels, payment rails, and data centres. Traditional network controls firewalls, intrusion prevention, and DDoS mitigation and their modern counterparts in SASE and micro segmentation provide foundational protection for latency-sensitive systems and large-scale traffic flows. Moreover, regulatory focus on secure interbank messaging and payment integrity sustains demand for robust network controls. This core role in securing transaction integrity stays essential to operational continuity and risk management, while vendors integrate analytics and automation into solutions.

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

Over the forecast period, the cloud segment is predicted to witness the highest growth

+357 96 030922
info@marketpublishers.com

rate as financial institutions accelerate migration of applications and data to cloud platforms for scalability and operational agility. Cloud-native security tools CASB, CWPP, cloud workload protection and identity-centric controls address data protection and configuration drift while enabling pay-as-you-grow consumption models. Additionally, the rise of fintechs and cloud-first digital banks favours cloud-delivered security services, increasing demand for continuous monitoring and rapid policy orchestration.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share owing to a mature financial ecosystem, high regulatory scrutiny, and significant cybersecurity spend by banks and fintechs. Large-scale adoption of advanced security architectures, extensive cloud usage, and a dense vendor ecosystem contribute to market depth. Additionally, frequent disclosure requirements and active incident reporting increase visibility into threats and justify continued investment. The combination of capital availability, professional services capacity, and enterprise demand means vendors find a substantial addressable market in the region.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR as rapid digitalisation, expanding fintech adoption, and increasing cross-border payments drive security investments. Developing economies are upgrading legacy infrastructure and embracing cloud and mobile-first strategies, creating new requirements for regionalised security solutions. Furthermore, growing regulatory initiatives, heightened awareness after high-profile breaches, and rising venture activity in cybersecurity startups accelerate market growth and adoption across banking, payments, and insurance verticals that prioritise local data protection, identity frameworks, and security adoption by mid-sized institutions.

Key players in the market

Some of the key players in Cybersecurity in Financial Services Market include Palo Alto Networks Inc., IBM Corporation, Cisco Systems Inc., Check Point Software Technologies Ltd., Fortinet Inc., CrowdStrike Holdings Inc., Netskope Inc., Darktrace plc, Splunk Inc., Sift Inc., Stripe Inc., and Plaid Inc.

Key Developments:

+357 96 030922
info@marketpublishers.com

In September 2025, Check Point® Software Technologies Ltd., a pioneer and global leader of cyber security solutions, today announced it has entered into an agreement to acquire Lakera, one of the world's leading AI-native security platforms for Agentic AI applications. With this acquisition, Check Point sets a new standard in cyber security, becoming able to deliver a full end-to-end AI security stack designed to protect enterprises as they accelerate their AI journey.

In September 2025, Darktrace opened a new deployment center, advancing its self-learning AI capabilities for financial sector email and messaging security.

In July 2025, Acquisition of CyberArk – Palo Alto agreed to acquire CyberArk for about US$25 billion in a cash-and-stock deal, to strengthen its identity security / privileged access management capabilities.

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Data Security & Privacy
- Other Security Types

Deployments Covered:

- Cloud
- On-Premises

Solutions Covered:

+357 96 030922
info@marketpublishers.com

- Identity & Access Management (IAM)
- Risk & Compliance Management
- Encryption
- Firewall
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Other Solutions

End Users Covered:

- Banks
- Insurance Companies
- FinTech Firms
- Other Financial Institutions

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK

+357 96 030922
info@marketpublishers.com

- Italy
- France
- Spain
- 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

+357 96 030922
info@marketpublishers.com

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 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

+357 96 030922
info@marketpublishers.com

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

10 KEY DEVELOPMENTS

+357 96 030922
info@marketpublishers.com

11 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

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 in Financial Services Market Forecasts to 2032 – Global Analysis By Security Type (Network Security, Endpoint Security, Application Security, Cloud Security, Data Security & Privacy, and Other Security Types), Deployment (Cloud and On-Premises), Solution, End User and By Geography

Product link: https://marketpublishers.com/r/CC337FBD5F18EN.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/CC337FBD5F18EN.html