Cloud Security In Banking - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Cloud Security In Banking Market Analysis

The cloud security in banking market stood at USD 36.17 billion in 2025 and is forecast to reach USD 80.66 billion by 2030, reflecting a 17.4% CAGR. This expansion mirrors banks' pivot toward cloud-native architectures that cut operating costs, improve agility, and satisfy regulators demanding proven operational resilience. Demand is also rising because ransomware incidents targeting financial workloads climbed to 78% in 2024, pushing chief information security officers to accelerate zero-trust adoption and deeper third-party risk oversight. Consolidation among security vendors is giving banks access to broad platforms that combine API protection, identity governance, and AI-powered fraud analytics. In parallel, public cloud providers are embedding pre-configured compliance tooling that simplifies audits under measures such as the EU's Digital Operational Resilience Act (DORA), which came into force in January 2025. Although North America retained a 37.2% share in 2024, Asia-Pacific is advancing the fastest on the back of national data-localization rules and mobile-first consumer banking, contributing a 17.8% regional CAGR to 2030.

Global Cloud Security In Banking Market Trends and Insights

Growing Volume and Sophistication of Cyber-Attacks on Banking Workloads

Financial institutions faced 78% ransomware hit rates in 2024, double the prior year. Attackers are now exploiting API abuse, container misconfigurations, and third-party software flaws-in 1 incident, a cloud misconfiguration exposed nearly 500,000

JPMorgan Chase customers, underlining the new perimeter-free threat surface. Average breach costs reach USD 10 million per incident, prompting urgent migration to behavior analytics-driven zero-trust controls that verify every session and asset. Major banks are embedding continuous compliance scanning and threat-hunting into DevSecOps pipelines to shrink exposure windows from days to hours. Global payments rail SWIFT is piloting federated-learning models with Google Cloud that flag anomalous transactions without moving sensitive data, showing how AI can detect fraud while protecting privacy. As organized crime monetizes access to stolen banking credentials on dark-net markets, proactive cloud segmentation and least-privilege IAM have become board-level priorities.

Real-Time Compliance Automation Requirements (Basel III, DORA, etc.)

The EU's DORA obliges 22,000 financial entities to report severe cyber incidents within 24 hours and test exit plans for critical cloud suppliers, pushing banks to deploy automated evidence-collection engines that feed regulators in near real time. U.S. regulators are moving in the same direction: the Treasury's 2025 cloud resilience report urges continuous control monitoring for systemic institutions. Cloud vendors now bundle mapping templates for Basel III, PCI DSS, and GDPR into dashboards, cutting manual audit workloads by 40%. Banks with global footprints are standardizing on unified compliance fabrics so a single policy set satisfies overlapping jurisdictions-particularly valuable when customer data flows span EU, U.S. and Asia. Early adopters report faster product launches because embedded governance eliminates lengthy security-review cycles, turning compliance from a blocker into a revenue enabler.

Data Residency Conflicts with Multi-Tenant Public Clouds

GDPR, China's CSL, and India's DPDP Act oblige banks to localize data, conflicting with global multi-tenant setups. Sovereign-cloud variants from hyperscalers promise metadata isolation and local key custody, yet still lack the granular placement controls some regulators demand. Smaller APAC markets often enforce data-center-in-country rules that erode economies of scale, nudging banks toward hybrid topologies where sensitive datasets stay on-prem or in local private regions. Resulting architectural complexity inflates cost and elevates configuration-error risk, adding drag to widespread cloud adoption plans. Policymakers are consulting with industry to refine residency stipulations so cyber resilience benefits outweigh jurisdictional concerns, but resolution is unlikely before the end of the decade.

Other drivers and restraints analyzed in the detailed report include:

Cost Avoidance Through Serverless and Container-Native Security Controls / Expansion of Open-Banking APIs Driving Zero-Trust Adoption / Shortage of Cloud-Security-Skilled Talent in Banks' SOC Teams /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Cloud Identity and Access Management accounted for 29.2% of the cloud security in the banking market share in 2024, reflecting banks' shift from perimeter controls to identity-centric guardrails that authenticate users, services, and APIs at a millisecond scale. As distributed work models persist, IAM consolidates single sign-on, privileged access management, and device posture checks, forming the backbone of zero-trust programs. Vendors are now embedding continuous risk scoring and passwordless flows that trim login friction-a critical user-experience factor in consumer banking.

Cloud Encryption is the fastest segment, posting an 18.2% CAGR through 2030. Quantum-threat awareness and stricter data-protection statutes are pushing banks to deploy hardware security modules and centralized key orchestration. The cloud security in the banking market size for encryption-focused products is forecast to rise alongside pilots of quantum-safe algorithms

across payment rails, positioning cryptography as both a compliance must-have and a competitive differentiator. Multi-party computation and format-preserving encryption are gaining traction, letting institutions analyze data without decrypting it, a breakthrough for cross-border fraud analytics and AI model training.

Public-cloud implementations captured 62.4% of the cloud security in the banking market size in 2024, underscoring confidence in hyperscaler defenses, dedicated financial-services regions, and shared-responsibility blueprints. Providers such as AWS and Microsoft report double-digit growth in bank workloads, aided by artifacts like PCI DSS on-demand audit packs that slice assessment times. However, sovereign-cloud and regional-cloud variants illustrate that one model will not fit every jurisdiction, and exit-strategy testing demanded by U.K. supervisors underscores residual concentration risk.

Hybrid-cloud installations are expanding at a 20.1% CAGR because they let banks meet data residency mandates while still bursting to public fabric for analytics surges. Containers and service meshes deliver workload portability, enabling stress-exit drills that shift traffic off a compromised provider within hours. As regulators scrutinize single-vendor dependencies, multi-cloud toolchains are becoming broad metrics for operational resilience, accelerating procurement of abstraction layers that secure and orchestrate across providers.

Cloud Security in Banking Market is Segmented by Software Type (Cloud Identity and Access Management, Cloud Email Security, and More), Deployment Model (Public Cloud, Private Cloud, and Hybrid Cloud), Security Service (Data Security, Application Security, and More), Banking Type (Retail/Consumer Banking, Corporate and Investment Banking, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America dominated the cloud security in the banking market with a 37.2% share in 2024. Long-standing regulator-vendor dialog, mature private-public threat-sharing, and USD 17 billion in annual tech spending at JPMorgan Chase underline the depth of local demand. The U.S. Treasury's 2025 cloud-resilience study formally encourages critical institutions to adopt multi-cloud while implementing real-time monitoring pipelines, accelerating orders for unified security stacks that can span providers. Canadian regulators now reference zero-trust and secure-API norms explicitly in open-banking guidance, signaling further investment momentum.

Asia-Pacific delivers the fastest CAGR at 17.8% to 2030 as regulators balance data-localization with innovation. Japan's consortium of regional banks adopted a shared hybrid platform running on IBM and Kyndryl infrastructure, illustrating collaborative approaches to cost-effective yet compliant security. Singapore's national digital ID roll-out and Malaysia's RMiT standard also drive the adoption of IAM and real-time monitoring, respectively. China's multi-level protection scheme (MLPS 2.0) compels encryption, continuous monitoring, and onshore key custody, prompting providers to launch local-only regions with hardware attestation.

Europe is accelerating due to DORA and PSD2/PSD3. Italian bank Credem Banca migrated to a specialist security cloud that embeds encryption and real-time incident notification, achieving 20% faster regulatory reporting. The Thales 2024 study notes that 65% of European firms rank cloud security as their second-largest cyber priority, evidencing board-level focus. Multi-cloud resilience drills and sovereign-cloud pilots are now contractual requirements, spurring demand for orchestration layers that enforce policies across Amazon, Microsoft, and Google environments without manual rule duplication.

List of Companies Covered in this Report:

AWS (Amazon.com, Inc.) / Google Cloud Platform (Alphabet Inc.) / Microsoft Azure (Microsoft Corporation) / IBM Cloud Security (IBM Corporation) / Oracle Cloud (Oracle Corporation) / Salesforce, Inc. / Palo Alto Networks, Inc. / Fortinet Inc. / Check Point Software Technologies Ltd. / Trend Micro Inc. / CrowdStrike Holdings, Inc. / Zscaler, Inc. / Proofpoint Inc. / Okta, Inc. / Ping

Identity Corporation / SailPoint Technologies Holdings Inc. / Netskope, Inc. / Imperva, Inc. / Qualys, Inc. / Rapid7, Inc. / Sophos Ltd. / Illumio Inc. / Akamai Technologies Inc. / Thales Group (Vormetric) / Temenos AG / nCino, Inc. /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

Cloud Security In Banking - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-18
		Signature