Cloud Encryption Software - 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 Encryption Software Market Analysis

The cloud encryption software market size stands at USD 7.43 billion in 2025 and is on course to reach USD 26.15 billion by 2030, registering a 28.6% CAGR. The surge blends three powerful forces: unrelenting cyber-attacks, mounting regulatory pressure, and the operational shift toward multi-cloud computing. Post-quantum cryptography standards finalized by the National Institute of Standards and Technology (NIST) in August 2024 accelerated enterprise migration road maps as boards realized that harvest-now-decrypt-later risks have already materialized. At the same time, 98% of financial-services firms now operate workloads in public cloud, creating an urgent need for unified key management across heterogeneous platforms. North America leads adoption, propelled by FedRAMP and Department of Defense mandates for quantum-safe algorithms, while sovereign-cloud policies push Asia-Pacific to the fastest regional CAGR. The encryption ecosystem is also shaped by performance-optimized symmetric tools, breakthrough fully homomorphic encryption, and hardware-assisted confidential-computing technologies that seal data during use.

Global Cloud Encryption Software Market Trends and Insights

Tightening Data-Protection Regulations

Worldwide statutes are raising the security baseline. PCI DSS 4.0, effective March 2025, forces annual cryptographic reviews and multi-factor authentication across all card-holder environments. Europe's Digital Operational Resilience Act and NIS 2 directive

require quantum-resistant encryption by 2030 for banking and critical infrastructure. In the United States, the Quantum Computing Cybersecurity Preparedness Act compels federal agencies to pivot to NIST-approved post-quantum algorithms, setting a template the private sector is following. FedRAMP has already mandated FIPS 140-2 validated modules for all federal cloud services, turning compliance into a de facto market entry ticket. Even universities are hardening controls because the 2002 FERPA framework never anticipated cloud-stored student data, prompting encryption measures that exceed legal minima.

Surge in Sophisticated Cyber-Attacks on Cloud

Cloud workloads absorbed 31% of recorded cyber incidents in 2024, with ransomware costs in financial services averaging USD 5.37 million. Advanced persistent-threat actors now harvest encrypted troves, betting on future quantum decryption. Real-time encryption monitoring and hybrid classical-plus-post-quantum key exchange are therefore gaining traction. Misconfigurations cause 44% of public-cloud breaches, so automated policy engines that wrap encryption around every object-independent of administrator skill-are becoming mandatory. Attackers increasingly target control-plane identities rather than endpoints, reinforcing the need for data-centric protection that stays effective even when perimeter controls fail.

Performance Overhead and Latency

Encrypting data adds compute cycles and I/O waits. Classical encryption-at-rest slows SQL queries by several hundred milliseconds in high-volume databases. Fully homomorphic encryption, while revolutionary for privacy, can inflate processing time by 1 000□ unless hardware acceleration is employed. GPU-assisted frameworks cut that overhead by roughly 12% according to recent benchmark studies published in Computers, Materials and Continua. Edge-computing scenarios feel the penalty most because encryption delay compounds existing network latency, forcing architects to weigh real-time responsiveness against confidentiality. Post-quantum algorithms also raise computational tax because of larger key sizes, challenging performance budgeting in low-power devices.

Other drivers and restraints analyzed in the detailed report include:

Enterprise Multi-Cloud Adoption / Confidential-Computing Demand / Key-Management Complexity /

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

Segment Analysis

Symmetric methods dominate the cloud encryption software market with 35.6% share in 2024, favored for their speed and low CPU overhead. Fully homomorphic encryption, despite its infancy, is the fastest-rising technique, forecast to grow at 29.0% CAGR as confidential-computing use cases blossom. The August 2024 release of FIPS 203, FIPS 204, and FIPS 205 set the baseline for post-quantum key encapsulation, digital signatures, and stateless hash-based signatures, prompting vendors to embed these algorithms into product road maps.

Enterprises are deploying hybrid cryptography that blends classical elliptic-curve methods with post-quantum lattices, hedging against algorithmic failure. Format-preserving encryption is also expanding because it lets legacy applications store protected data without schema redesign. With NIST's March 2025 selection of HQC as a fifth algorithm for additional diversity, crypto-agile tooling has become a board-level priority. As a result, the cloud encryption software market size for symmetric workloads is projected to climb steadily, while quantum-safe options capture a larger slice of new deployments.

Data-at-rest still tops the application stack with 36.8% share of the cloud encryption software market in 2024, reflecting mature backup and storage practices. Yet it is data-in-use encryption that makes headlines, surging at a 29.7% CAGR as TEEs remove the

longstanding barrier of processing on plaintext. The cloud encryption software market size for confidential-computing workloads will therefore expand faster than any other segment.

Transport-layer protection remains indispensable for inter-cloud links, but performance tuning has shifted toward post-quantum handshake algorithms. SaaS collaboration tools are seeing wider client-side encryption rollouts so organizations retain control over cryptographic keys. Searchable symmetric encryption now appears in big-data environments, where latency overhead can be tolerated for high-value queries. Together these shifts advance the vision of persistent, state-agnostic protection across the entire data life cycle.

The Cloud Encryption Software Market Report is Segmented by Encryption Type (Symmetric, Asymmetric / PKI, and More), Application (Data-At-Rest, Data-In-Transit, and More), Organization Size (Large Enterprises and Small and Medium Enterprises (SMEs)), Industry Vertical (BFSI, Healthcare and Life Sciences, Education, Retail and E-Commerce, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America held 38.9% of the cloud encryption software market in 2024, underpinned by FedRAMP mandates, Department of Defense directives and aggressive enterprise migration to post-quantum controls. Multi-cloud penetration is high, and vendors secure revenue through managed key services and crypto-agile orchestration. Large healthcare and finance clients also test confidential-computing frameworks at scale, accelerating innovation cycles.

Asia-Pacific is the fastest-growing region with a 29.5% CAGR through 2030. Sovereign-cloud blueprints in Australia, Japan, South Korea and India demand that encryption keys remain on domestic soil, spurring sales of external key-management gateways and hardware security modules that support national algorithms where required. The Asian Development Bank estimates improved cloud policy could lift regional GDP by up to 0.7% during 2024-2028, and encryption is cited as a pivotal enabler. Chinese and Southeast Asian hyperscalers are forming in-country alliances with chipmakers to deliver quantum-safe network encryption, keeping pace with Western rivals.

Europe maintains steady expansion driven by GDPR enforcement and the Digital Operational Resilience Act. Financial institutions must file resilience plans outlining migration to quantum-resistant algorithms, a move that is turning Europe into a laboratory for cross-border key-escrow interoperability. Privacy-preserving analytics-especially in health and mobility-stimulate demand for fully homomorphic encryption. Smaller markets in South America and the Middle East and Africa trail but present greenfield opportunities, particularly where 5G rollouts introduce edge-cloud architectures that require lightweight, low-latency encryption.

List of Companies Covered in this Report:

Trend Micro / CipherCloud / Lookout CASB / Broadcom (Symantec) / Hewlett Packard Enterprise / Google LLC / Sophos / Micro Focus (Voltage) / CyberArk / Thales (SafeNet) / Hitachi Vantara / Boxcryptor / Microsoft Corporation / Amazon Web Services / IBM Corporation / Check Point Software / Palo Alto Networks / Netskope / Fortanix / Zscaler / Akeyless Security /

Additional Benefits:

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

Table of Contents:

Cloud Encryption Software - 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	2026-03-01
		Signature