Big Data Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 100 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:

Big Data Security Market Analysis

The Big Data Security Market size is estimated at USD 27.63 billion in 2025, and is expected to reach USD 63.40 billion by 2030, at a CAGR of 1.54% during the forecast period (2025-2030).

Accelerated adoption stems from rising cyber-attack frequency, stricter data-protection laws, and the shift of petabyte-scale workloads to public clouds that demand zero-trust controls. Enterprises now treat data-centric security as a board-level priority as AI-enabled breaches, ransomware, and supply-chain intrusions elevate operational and financial risk. Healthcare, manufacturing, and financial services face the highest breach costs, which pushes capital toward encryption, tokenization, and AI-powered analytics. Meanwhile, platform vendors consolidate point tools to reduce complexity and offset the cybersecurity talent shortfall, while data-sovereignty rules in Asia Pacific spark record data-center investment.

Global Big Data Security Market Trends and Insights

AI-enabled breaches drive enterprise security budget reallocations

Ransomware groups now weaponize generative AI for rapid credential theft and social-engineering campaigns that bypass legacy defenses. Manufacturing downtime has surpassed USD 22,000 per minute during major incidents, prompting boards to lift security budgets well above prior allocations. Data-breach costs in industrial domains climbed to USD 5.56 million in 2024, eclipsing

general IT-spending growth and fueling demand for real-time analytics that detect lateral movement. Financial institutions concede that current allocations of only 13% of IT spend underfund defenses, with experts urging a shift toward 20% to keep pace with attacker automation. Across critical infrastructure, AI-powered security operations centers report 30% faster incident resolution once machine-learning correlation replaces manual triage. The result is sustained top-line expansion for the big data security market as enterprises reprioritize funding.

GDPR and national data laws mandate petabyte-scale compliance infrastructure

Europe's GDPR, California's CCPA, and similar statutes in Asia Pacific now obligate encryption, masking, and audit trails across ever-larger datasets. China's 2025 enhancements add real-time compliance audits for finance and insurance firms, tightening penalties for lax controls. European organizations have raised information-security budgets to 9% of total IT outlays under the NIS2 Directive, while average regional breach costs reached EUR 4.4 million in 2025. In the United States, the Department of Health and Human Services proposed USD 100 million for sector-wide cybersecurity coordination in its FY 2026 plan. As compliance moves from policy to technical enforcement, demand increases for scalable encryption, tokenization, and immutable logging key revenue streams within the big data security market.

Cybersecurity talent shortage constrains market growth

Thirty-two percent of EU organizations cannot fill essential cybersecurity roles, driving reliance on managed security service providers. Japan's operators collaborate with Cloudflare to supply turnkey zero-trust services that offset staffing gaps for SMEs. Microsoft's Secure Future Initiative applies 34,000 engineers to AI-driven automation, improving incident response by 30% and showcasing how hyperscalers compensate for scarce expertise. Although automation eases workloads, chronic shortages slow deployment and limit the near-term scale-up of the big data security market.

Other drivers and restraints analyzed in the detailed report include:

Cloud data lakes accelerate zero-trust architecture adoption / LLM training in data protection becomes a strategic imperative / Tool-orchestration complexity strains enterprise budgets /

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

Segment Analysis

Solutions held 63.0% of 2024 revenue, driven by robust demand for encryption, tokenization, and SIEM suites. At the same time, Services is set to grow at 19.08% CAGR as organizations outsource 24/7 monitoring and compliance integration. Talent scarcity and platform complexity push enterprises toward managed detection and response, consulting, and integration contracts. Vendors bundle these offerings with cloud subscriptions, enabling predictable OpEx and faster implementation cycles. As a result, the big data security market phrase continues to reflect service-led value creation throughout the forecast horizon.

Managed Security Services show the highest traction, while Advisory and Integration engagements surge as firms re-architect data lakes on cloud foundations. Data encryption and tokenization software remains the volume driver within Solutions, propelled by regulatory mandates. SIEM platforms evolve with AI inference that reduces alert fatigue, and IAM upgrades underpin zero-trust rollouts. The convergence of platform features signals ongoing consolidation in the big data security market as players chase end-to-end control points.

Large Enterprises dominated in 2024 with 69.5% revenue, reflecting multi-region operations and stringent compliance obligations. Yet SMEs are forecast to post a 20.04% CAGR, highlighting cloud subscription models that lower entry barriers. Hyperscalers now

embed enterprise-grade encryption, key management, and behavior analytics into baseline plans, letting resource-constrained firms access capabilities once exclusive to Fortune 500 peers. This shift broadens the customer base, sustaining double-digit expansion in the big data security market.

For large organizations, investments focus on advanced analytics, homomorphic encryption pilots, and AI-powered SOCs that mine petabyte-scale logs. Some institutions maintain teams exceeding 1,000 security specialists, underscoring the depth of in-house expertise. SMEs, by contrast, emphasize turnkey managed services that offload complexity. Vendors tailoring price points and automation to this segment stand to capture an outsized share as the big data security industry matures.

The Big Data Security Market Report is Segmented by Component (Solutions and Services), Organization Size (Small and Medium Enterprises and Large Enterprises), End-User Industry (Banking, Financial Services, and Insurance [BFSI], IT and Telecommunication, Manufacturing, Healthcare and Life Sciences, Aerospace and Defense, and More), Deployment Mode (On-Premise and Cloud), and Geography.

Geography Analysis

North America held 41.3% of 2024 revenue, benefiting from early zero-trust adoption, a dense vendor ecosystem, and mature breach-notification laws. Growth moderates as large enterprises complete initial cloud migrations, yet ongoing AI-security pilots maintain spending momentum. Europe follows, propelled by GDPR enforcement and the NIS2 Directive, with information-security allocations now 9% of total IT budgets. Regulatory certainty fuels demand even as economic headwinds weigh on discretionary IT projects.

Asia Pacific is forecast for a 20.61% CAGR through 2030, reflecting sovereign-cloud investments and domestic-technology mandates. AWS's pledge of 2.26 trillion yen (USD 15.3 billion) to expand Japanese regions by 2027 exemplifies its hyperscale commitment. Oracle separately plans USD 8 billion in local data centers to meet economic-security guidelines. China's information-security market could hit 37 trillion yuan by 2027 as state bodies prioritize indigenous tooling. Governments across the region encourage local data processing to spur security product adoption, enlarging the big data security market size in emerging economies.

The Middle East, Africa, and Latin America represent smaller bases but show rising adoption as cloud coverage widens and financial-sector modernization policies advance. Gulf Cooperation Council states issue new cyber regulations tied to Vision 2030 agendas, while Brazil's LGPD inspires neighbouring countries to legislate. Although infrastructure gaps temper growth, rising digital-banking penetration creates latent demand that the big data security market can tap as connectivity improves.

List of Companies Covered in this Report:

Amazon Web Services / Broadcom (Symantec) / Check Point Software Technologies / Cisco Systems / Cloudera / CrowdStrike / Dell Technologies / Elastic NV / Fortinet / Google Cloud (Alphabet) / Hewlett Packard Enterprise / IBM Corporation / Imperva / McAfee / Microsoft Corporation / Oracle Corporation / Palo Alto Networks / RSA Security / Snowflake Inc. / Splunk Inc. / Talend SA / Thales Group /

Additional Benefits:

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

Table of Contents:

Big Data Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 100 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	2026-02-28
		Signature