SCOTTS INTERNATIONAL

Data Loss Prevention (DLP) - 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:

Data Loss Prevention (DLP) Market Analysis

The data loss prevention market is valued at USD 35.38 billion in 2025 and is forecast to reach USD 94.09 billion by 2030, translating into a vigorous 21.61% CAGR over the period. Rapid expansion is rooted in mounting regulatory penalties, the dispersal of sensitive data across hybrid workplaces, and the embedding of DLP controls inside zero-trust and Secure Access Service Edge platforms. Artificial-intelligence policy tuning is further accelerating adoption by trimming false-positive rates and reducing analyst fatigue, while cloud-delivered deployment models deliver the elasticity enterprises need to secure distributed users. Vendor consolidation driven by acquisitions that fold DLP into broader data-security posture offerings underscores a strategic pivot toward unified platforms capable of discovery, classification, and protection across endpoints, networks, and multicloud estates.

Global Data Loss Prevention (DLP) Market Trends and Insights

Escalating Cyber-Breach Fines Under GDPR 2.0 and CCPA Amendments

Maximum penalties are reshaping spending priorities: TikTok's EUR 530 million (USD 624.18 million) fine in 2025 spotlighted regulators' readiness to levy record sanctions for lax data-transfer controls. In parallel, the UK Data (Use and Access) Bill tightens data-handling rules, and the EU AI Act introduces mandatory transparency audits, both driving proactive DLP investment. California's latest CCPA amendments widen the definition of sensitive personal information and strengthen consumer rights, expanding compliance exposure for enterprises operating nationwide. Across jurisdictions, executives now view robust DLP capability as a demonstrable risk-mitigation measure rather than a discretionary cybersecurity layer, propelling the data loss prevention market toward accelerated growth.

Hybrid-Work Data Sprawl Raising Endpoint and Cloud Risk

IBM's 2023 breach report revealed that 82% of incidents involved cloud-resident data, underscoring the erosion of perimeter defenses IBM. Employees increasingly use personal devices and unsanctioned SaaS tools, creating blind spots that traditional controls cannot monitor. In sectors such as manufacturing where operational technology merges with IT systems the attack surface widens as production gear becomes network-connected. Organizations therefore adopt endpoint DLP for device-level controls while extending cloud DLP rules across multiple providers, fuelling demand in the data loss prevention market.

Complexity and Skills Gap in Multi-Cloud Roll-Outs

Firms commonly operate three to five cloud platforms, each with unique access controls and encryption schemes. Security teams struggle to harmonize policies without dedicated expertise, lengthening deployment cycles and inflating operating costs. The shortage of cloud-security talent therefore restrains the pace at which the data loss prevention market can transition toward fully orchestrated multicloud protection.

Other drivers and restraints analyzed in the detailed report include:

Convergence of DLP with CASB and DSPM Platforms / AI-Assisted Policy Tuning Slashing False-Positive Rates / High TCO for Legacy On-Prem Policies /

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

Segment Analysis

Cloud-based deployment models secured 67.3% market share in 2024, and this segment is projected to sustain a 22.1% CAGR through 2030. The data loss prevention market size for cloud services will therefore scale in parallel with enterprise SASE adoption. Cloud delivery enables single console management and elastic policy enforcement across remote users, mitigating the burdens of patching and hardware refresh cycles. On-prem solutions persist in heavily regulated sectors such as defense or critical infrastructure where data must remain within physically controlled locations. Yet their relative growth is subdued because hybrid-work realities demand anywhere-access inspection that pure on-site deployments cannot deliver efficiently.

Cloudflare's SASE framework illustrates how integrated DLP detects and blocks policy violations within secure web gateway and CASB streams, demonstrating the architectural preference shift toward converged services. Organizations scaling rapidly or dealing with seasonal data spikes benefit from metered consumption models that align cost with usage, thereby reinforcing the demand trajectory of the data loss prevention market.

Endpoint controls accounted for 46.7% of revenue in 2024 and remain the fastest advancing solution at 22.4% CAGR, reflecting the surge in device-centric data handling. The rising prevalence of generative-AI coding assistants introduces novel exfiltration vectors that endpoint agents are uniquely positioned to intercept. Researchers demonstrated a "rules file backdoor" that smuggles secrets via benign-looking configuration files, bypassing conventional reviews. Vendors now embed behavioral AI to monitor clipboard use, screen capture, and code-generation patterns, increasing protection precision and powering growth in the data loss prevention market.

Network DLP preserves relevance for in-flight data scrutiny, especially in complex campus networks. Meanwhile, storage-centric tools protect high-volume file shares inside data centers. Nonetheless, enterprises gravitate toward endpoint-first strategies because employees engage with sensitive data directly on laptops, mobiles, and virtual desktops. Microsoft's Purview suite extends endpoint policies into browser traffic and SaaS sessions, signalling how platform vendors fuse data governance with endpoint telemetry.

Data Loss Prevention Market is Segmented by Deployment (On-Premises, Cloud-Based), Solution (Network DLP, Endpoint DLP, and More), End-User Industry (BFSI, IT and Telecom, Manufacturing, and More), Application (Cloud Storage Security, Email and Collaboration Protection, and More), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America commanded 24.2% of global revenue in 2024, anchored by stringent federal and state regulations plus a well-capitalized private sector that budgets for zero-trust programs. United States agencies embrace DLP inside SASE blueprints published by the Cybersecurity and Infrastructure Security Agency, while Canada's privacy regime and Mexico's expanding fintech ecosystem add regional momentum. High breach costs and mature cyber-insurance markets sustain a premium on advanced controls, consolidating North America's role as a technology proving ground for the data loss prevention market.

Asia-Pacific is forecast to accelerate at 21.1% CAGR, catalyzed by rapid digitization and sovereign-cloud laws that mandate resident data storage. China's Cybersecurity Law and India's Digital Personal Data Protection Act compel localized policy orchestration, driving regional demand for cloud-delivered yet jurisdiction-aware solutions. Japan and South Korea deploy endpoint DLP to safeguard manufacturing know-how, while ASEAN economies leapfrog to cloud-native stacks that bundle DLP with secure web gateways. This regulatory and threat-exposure cocktail positions APAC as the most dynamic arena within the data loss prevention market.

Europe's growth rests on GDPR enforcement and complementary statutes such as the Digital Operational Resilience Act, which raise minimum control baselines for financial entities. Germany and the United Kingdom anchor spending through robust banking and industrial sectors, whereas France advances sovereign-cloud projects that favor locally hosted DLP services. Southern European economies adopt DLP at a steadier pace, yet pan-EU privacy-by-design mandates universally influence vendor offerings. Data localization clauses inside cloud-outsourcing guidelines spur interest in platforms capable of maintaining policy fidelity across borders, sustaining incremental gains for the data loss prevention market.

List of Companies Covered in this Report:

Broadcom (Symantec) / Microsoft / Forcepoint / Proofpoint / Zscaler / Trend Micro / Check Point / Cisco / Palo Alto Networks / CrowdStrike / Netskope / Trellix / Digital Guardian (Fortra) / CoSoSys / GTB Technologies / Spirion / Safetica / Code42 / Nightfall AI / Cyera / Fortinet /

Additional Benefits:

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

Table of Contents:

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

Data Loss Prevention (DLP) - 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	2026-02-26
		Signature	