

# **Data Security Posture Management (DSPM) Market Forecasts to 2034 – Global Analysis By Data Environment (Public Cloud, Private Cloud, Hybrid Cloud, SaaS Applications, and Data Lakes and Data Warehouses), Component, Organization Size, Data Sensitivity Level, Application, End User and By Geography**

<https://marketpublishers.com/r/D7405078C6BCEN.html>

Date: April 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: D7405078C6BCEN

## **Abstracts**

According to Statistics MRC, the Global Data Security Posture Management (DSPM) Market is accounted for \$1.3 billion in 2026 and is expected to reach \$13.9 billion by 2034, growing at a CAGR of 34.4% during the forecast period. Data Security Posture Management (DSPM) is a set of technologies and practices designed to continuously discover, classify, and monitor sensitive data across an organization's data environments, including cloud platforms, databases, and storage systems. DSPM solutions help organizations understand where their data resides, who has access to it, and how it is being used. By providing visibility into data risks, misconfigurations, and potential exposures, DSPM enables organizations to strengthen data protection strategies, maintain regulatory compliance, and minimize the risk of data breaches.

Market Dynamics:

Driver:

Explosive growth in cloud and multi-cloud adoption

Organizations are rapidly migrating workloads to public, private, and hybrid clouds, creating fragmented data landscapes. Each cloud platform has unique security controls,

leading to inconsistent policies and visibility gaps. DSPM solutions automatically discover and classify sensitive data across these distributed environments, addressing blind spots. The need to enforce uniform security postures across AWS, Azure, and Google Cloud is accelerating adoption. Additionally, remote work and SaaS applications have further dispersed corporate data, making manual oversight impossible. Enterprises now prioritize DSPM to continuously monitor data exposure, misconfigurations, and unauthorized access, directly driving market expansion.

#### Restraint:

##### Integration complexity with existing security stacks

Adding DSPM requires seamless integration to avoid alert fatigue and overlapping functionalities. APIs between cloud platforms and DSPM solutions are not always fully mature, leading to data synchronization delays. Legacy on-premises systems often lack native compatibility with modern DSPM architectures. Customizing workflows for different data types and sensitivity levels demands significant engineering effort. Smaller teams struggle with resource constraints to maintain real-time posture visibility. Without standardized interoperability frameworks, integration challenges slow down large-scale DSPM deployments across complex IT environments.

#### Opportunity:

##### Rising demand for AI-driven data security automation

Artificial intelligence and machine learning are transforming DSPM by enabling predictive risk analytics and automated remediation. AI algorithms can identify anomalous data access patterns, classify unstructured data at scale, and prioritize critical exposures in real time. Organizations are seeking solutions that reduce manual intervention in compliance reporting and threat hunting. Generative AI adoption in enterprises also creates new data leakage vectors, increasing the need for AI-aware DSPM. Vendors that embed large language model security and automated policy enforcement will capture significant market share. This trend opens opportunities for innovation in behavioral analytics and self-healing data security.

#### Threat:

##### Shortage of skilled cybersecurity professionals

The DSPM market relies on security analysts who understand cloud architectures, data classification frameworks, and regulatory landscapes. A global shortage of qualified personnel limits the effective deployment and management of DSPM tools. Many organizations purchase solutions but fail to configure them optimally, leading to false positives or missed exposures. Small and mid-sized enterprises particularly struggle to hire experts who can operationalize posture management. This skills gap also slows incident response times when DSPM flags critical risks. Without enough trained professionals, the full value of DSPM investments remains unrealized, potentially reducing long-term market growth.

### Covid-19 Impact

The pandemic triggered mass remote work and accelerated cloud migration, dramatically expanding attack surfaces. Many organizations lost visibility over data spread across home networks, personal devices, and unsanctioned SaaS tools. Budgets for security automation increased as manual audits became impossible. DSPM vendors saw rising demand for cloud-native solutions that could quickly discover shadow data. However, supply chain delays for hardware appliances and initial economic uncertainty slowed some enterprise contracts. Post-pandemic, hybrid work models are permanent, and regulatory scrutiny on data privacy has intensified. DSPM is now embedded into zero-trust and compliance frameworks globally.

The data discovery and classification engine segment is expected to be the largest during the forecast period

The data discovery and classification engine segment is expected to account for the largest market share during the forecast period. This component forms the foundation of any DSPM solution by automatically identifying structured and unstructured data across clouds, data lakes, and SaaS applications. It labels information based on sensitivity levels such as personally identifiable information, financial records, or intellectual property. Accurate classification enables risk prioritization, access governance, and compliance reporting. As data volumes grow exponentially, manual tagging becomes impossible, driving demand for AI-powered classification.

The highly sensitive data segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the highly sensitive data segment is predicted to witness the highest growth rate. This includes personal health information, payment card data, trade

secrets, and government classified materials. Breaches involving highly sensitive data carry severe financial penalties, reputational damage, and legal liabilities. Regulations such as GDPR, HIPAA, and CCPA mandate strict controls over such data, compelling enterprises to prioritize its protection. DSPM solutions offer granular visibility and automated remediation for high-risk exposures. The rise of ransomware attacks targeting critical databases further accelerates adoption.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by early cloud adoption, stringent data privacy regulations, and high cybersecurity spending. The United States hosts major DSPM vendors and has mature enterprises across BFSI, healthcare, and technology sectors. Frequent data breach disclosures have pushed organizations to adopt proactive posture management. Government initiatives like FedRAMP and state-level privacy laws (CCPA, NYDFS) mandate robust data discovery. Strong venture capital funding for security startups also fuels innovation.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, supported by rapid digital transformation, cloud adoption, and emerging data protection laws. Countries like Australia, India, Singapore, and Japan are implementing GDPR-style regulations such as India's DPDP Act and China's PIPL. Enterprises are investing in data security to support cross-border data flows and global compliance. The region's expanding BFSI, e-commerce, and manufacturing sectors generate massive sensitive data volumes. Governments are promoting local data sovereignty, increasing demand for DSPM.

Key players in the market

Some of the key players in Data Security Posture Management (DSPM) Market include Varonis Systems, Inc., Imperva, Normalyze, Inc., Cyera, Dig Security, Laminar, BigID, Securiti.ai, Symmetry Systems, Microsoft Purview, AWS Macie, Google Cloud Data Security, Palo Alto Networks, CrowdStrike, and SentinelOne.

Key Developments:

In March 2026, BigID announced it has achieved Federal Risk and Authorization

Management Program (FedRAMP) certification in partnership with Knox Systems (Knox), the largest federal AI-managed cloud provider. This milestone authorizes U.S. federal agencies to use BigID's platform to discover, classify, and protect sensitive data across cloud, on-prem, and AI environments under rigorous federal security standards.

In December 2025, Thales launches its new AI Security Fabric, delivering the first runtime security capabilities designed to protect Agentic AI, LLM-powered applications, enterprise data, and identities. AI is one of the fastest-growing technologies in the history of modern business, with the ability to revolutionize industries, optimize operations, and drive innovation, but it is also introducing security gaps, risks, and vulnerabilities. According to McKinsey, 78% of organizations are using AI in at least one business function, up from 55% two years ago.

#### Data Environments Covered:

Public Cloud

Private Cloud

Hybrid Cloud

SaaS Applications

Data Lakes and Data Warehouses

#### Components Covered:

Data Discovery and Classification Engine

Data Risk Assessment and Prioritization

Access Governance and Entitlement Management

Data Activity Monitoring

Remediation and Orchestration

Reporting and Compliance Dashboards

#### Organization Sizes Covered:

Small and Medium Enterprises (SMEs)

Large Enterprises

Government and Public Sector

#### Data Sensitivity Levels Covered:

Highly Sensitive

Sensitive Business Data

Public / Non-Sensitive Data

#### Applications Covered:

Data Security Posture Assessment

Compliance Automation

Shadow Data Discovery

Insider Risk Detection

Ransomware Exposure Analysis

Data Leak Prevention (DLP) Integration

AI Data Pipeline Security

#### End Users Covered:

Banking, Financial Services & Insurance (BFSI)

Healthcare & Life Sciences

Retail & E-commerce

Technology & Software

Government & Defense

Manufacturing & Industrial

Telecommunications

Energy & Utilities

#### Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

#### Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

#### South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of 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 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

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

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances



## Contents

### **1 EXECUTIVE SUMMARY**

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

### **2 RESEARCH FRAMEWORK**

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
  - 2.4.1 Data Collection (Primary and Secondary)
  - 2.4.2 Data Modeling and Estimation Techniques
  - 2.4.3 Data Validation and Triangulation
  - 2.4.4 Analytical and Forecasting Approach

### **3 MARKET DYNAMICS AND TREND ANALYSIS**

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

### **4 COMPETITIVE AND STRATEGIC ASSESSMENT**

- 4.1 Porter's Five Forces Analysis
  - 4.1.1 Supplier Bargaining Power
  - 4.1.2 Buyer Bargaining Power
  - 4.1.3 Threat of Substitutes
  - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

## **5 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY DATA ENVIRONMENT**

- 5.1 Public Cloud
- 5.2 Private Cloud
- 5.3 Hybrid Cloud
- 5.4 SaaS Applications
- 5.5 Data Lakes and Data Warehouses

## **6 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY COMPONENT**

- 6.1 Data Discovery and Classification Engine
- 6.2 Data Risk Assessment and Prioritization
- 6.3 Access Governance and Entitlement Management
- 6.4 Data Activity Monitoring
- 6.5 Remediation and Orchestration
- 6.6 Reporting and Compliance Dashboards

## **7 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY ORGANIZATION SIZE**

- 7.1 Small and Medium Enterprises (SMEs)
- 7.2 Large Enterprises
- 7.3 Government and Public Sector

## **8 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY DATA SENSITIVITY LEVEL**

- 8.1 Highly Sensitive
- 8.2 Sensitive Business Data
- 8.3 Public / Non-Sensitive Data

## **9 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY APPLICATION**

- 9.1 Data Security Posture Assessment
- 9.2 Compliance Automation
- 9.3 Shadow Data Discovery
- 9.4 Insider Risk Detection
- 9.5 Ransomware Exposure Analysis
- 9.6 Data Leak Prevention (DLP) Integration
- 9.7 AI Data Pipeline Security

## **10 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY END USER**

- 10.1 Banking, Financial Services & Insurance (BFSI)
- 10.2 Healthcare & Life Sciences
- 10.3 Retail & E-commerce
- 10.4 Technology & Software
- 10.5 Government & Defense
- 10.6 Manufacturing & Industrial
- 10.7 Telecommunications
- 10.8 Energy & Utilities

## **11 GLOBAL DATA SECURITY POSTURE MANAGEMENT (DSPM) MARKET, BY GEOGRAPHY**

- 11.1 North America
  - 11.1.1 United States
  - 11.1.2 Canada
  - 11.1.3 Mexico
- 11.2 Europe
  - 11.2.1 United Kingdom
  - 11.2.2 Germany
  - 11.2.3 France
  - 11.2.4 Italy
  - 11.2.5 Spain
  - 11.2.6 Netherlands
  - 11.2.7 Belgium
  - 11.2.8 Sweden
  - 11.2.9 Switzerland
  - 11.2.10 Poland

- 11.2.11 Rest of Europe
- 11.3 Asia Pacific
  - 11.3.1 China
  - 11.3.2 Japan
  - 11.3.3 India
  - 11.3.4 South Korea
  - 11.3.5 Australia
  - 11.3.6 Indonesia
  - 11.3.7 Thailand
  - 11.3.8 Malaysia
  - 11.3.9 Singapore
  - 11.3.10 Vietnam
  - 11.3.11 Rest of Asia Pacific
- 11.4 South America
  - 11.4.1 Brazil
  - 11.4.2 Argentina
  - 11.4.3 Colombia
  - 11.4.4 Chile
  - 11.4.5 Peru
  - 11.4.6 Rest of South America
- 11.5 Rest of the World (RoW)
  - 11.5.1 Middle East
    - 11.5.1.1 Saudi Arabia
    - 11.5.1.2 United Arab Emirates
    - 11.5.1.3 Qatar
    - 11.5.1.4 Israel
    - 11.5.1.5 Rest of Middle East
  - 11.5.2 Africa
    - 11.5.2.1 South Africa
    - 11.5.2.2 Egypt
    - 11.5.2.3 Morocco
    - 11.5.2.4 Rest of Africa

## **12 STRATEGIC MARKET INTELLIGENCE**

- 12.1 Industry Value Network and Supply Chain Assessment
- 12.2 White-Space and Opportunity Mapping
- 12.3 Product Evolution and Market Life Cycle Analysis
- 12.4 Channel, Distributor, and Go-to-Market Assessment

## **13 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES**

- 13.1 Mergers and Acquisitions
- 13.2 Partnerships, Alliances, and Joint Ventures
- 13.3 New Product Launches and Certifications
- 13.4 Capacity Expansion and Investments
- 13.5 Other Strategic Initiatives

## **14 COMPANY PROFILES**

- 14.1 Varonis Systems, Inc.
- 14.2 Imperva
- 14.3 Normalyze, Inc.
- 14.4 Cyera
- 14.5 Dig Security
- 14.6 Laminar
- 14.7 BigID
- 14.8 Securiti.ai
- 14.9 Symmetry Systems
- 14.10 Microsoft Purview
- 14.11 AWS Macie
- 14.12 Google Cloud Data Security
- 14.13 Palo Alto Networks
- 14.14 CrowdStrike
- 14.15 SentinelOne

## List Of Tables

### LIST OF TABLES

Table 1 Global Data Security Posture Management (DSPM) Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Data Security Posture Management (DSPM) Market Outlook, By Data Environment (2023-2034) (\$MN)

Table 3 Global Data Security Posture Management (DSPM) Market Outlook, By Public Cloud (2023-2034) (\$MN)

Table 4 Global Data Security Posture Management (DSPM) Market Outlook, By Private Cloud (2023-2034) (\$MN)

Table 5 Global Data Security Posture Management (DSPM) Market Outlook, By Hybrid Cloud (2023-2034) (\$MN)

Table 6 Global Data Security Posture Management (DSPM) Market Outlook, By SaaS Applications (2023-2034) (\$MN)

Table 7 Global Data Security Posture Management (DSPM) Market Outlook, By Data Lakes and Data Warehouses (2023-2034) (\$MN)

Table 8 Global Data Security Posture Management (DSPM) Market Outlook, By Component (2023-2034) (\$MN)

Table 9 Global Data Security Posture Management (DSPM) Market Outlook, By Data Discovery and Classification Engine (2023-2034) (\$MN)

Table 10 Global Data Security Posture Management (DSPM) Market Outlook, By Data Risk Assessment and Prioritization (2023-2034) (\$MN)

Table 11 Global Data Security Posture Management (DSPM) Market Outlook, By Access Governance and Entitlement Management (2023-2034) (\$MN)

Table 12 Global Data Security Posture Management (DSPM) Market Outlook, By Data Activity Monitoring (2023-2034) (\$MN)

Table 13 Global Data Security Posture Management (DSPM) Market Outlook, By Remediation and Orchestration (2023-2034) (\$MN)

Table 14 Global Data Security Posture Management (DSPM) Market Outlook, By Reporting and Compliance Dashboards (2023-2034) (\$MN)

Table 15 Global Data Security Posture Management (DSPM) Market Outlook, By Organization Size (2023-2034) (\$MN)

Table 16 Global Data Security Posture Management (DSPM) Market Outlook, By Small and Medium Enterprises (SMEs) (2023-2034) (\$MN)

Table 17 Global Data Security Posture Management (DSPM) Market Outlook, By Large Enterprises (2023-2034) (\$MN)

Table 18 Global Data Security Posture Management (DSPM) Market Outlook, By

Government and Public Sector (2023-2034) (\$MN)

Table 19 Global Data Security Posture Management (DSPM) Market Outlook, By Data Sensitivity Level (2023-2034) (\$MN)

Table 20 Global Data Security Posture Management (DSPM) Market Outlook, By Highly Sensitive (2023-2034) (\$MN)

Table 21 Global Data Security Posture Management (DSPM) Market Outlook, By Sensitive Business Data (2023-2034) (\$MN)

Table 22 Global Data Security Posture Management (DSPM) Market Outlook, By Public / Non-Sensitive Data (2023-2034) (\$MN)

Table 23 Global Data Security Posture Management (DSPM) Market Outlook, By Application (2023-2034) (\$MN)

Table 24 Global Data Security Posture Management (DSPM) Market Outlook, By Data Security Posture Assessment (2023-2034) (\$MN)

Table 25 Global Data Security Posture Management (DSPM) Market Outlook, By Compliance Automation (2023-2034) (\$MN)

Table 26 Global Data Security Posture Management (DSPM) Market Outlook, By Shadow Data Discovery (2023-2034) (\$MN)

Table 27 Global Data Security Posture Management (DSPM) Market Outlook, By Insider Risk Detection (2023-2034) (\$MN)

Table 28 Global Data Security Posture Management (DSPM) Market Outlook, By Ransomware Exposure Analysis (2023-2034) (\$MN)

Table 29 Global Data Security Posture Management (DSPM) Market Outlook, By Data Leak Prevention (DLP) Integration (2023-2034) (\$MN)

Table 30 Global Data Security Posture Management (DSPM) Market Outlook, By AI Data Pipeline Security (2023-2034) (\$MN)

Table 31 Global Data Security Posture Management (DSPM) Market Outlook, By End User (2023-2034) (\$MN)

Table 32 Global Data Security Posture Management (DSPM) Market Outlook, By Banking, Financial Services & Insurance (BFSI) (2023-2034) (\$MN)

Table 33 Global Data Security Posture Management (DSPM) Market Outlook, By Healthcare & Life Sciences (2023-2034) (\$MN)

Table 34 Global Data Security Posture Management (DSPM) Market Outlook, By Retail & E-commerce (2023-2034) (\$MN)

Table 35 Global Data Security Posture Management (DSPM) Market Outlook, By Technology & Software (2023-2034) (\$MN)

Table 36 Global Data Security Posture Management (DSPM) Market Outlook, By Government & Defense (2023-2034) (\$MN)

Table 37 Global Data Security Posture Management (DSPM) Market Outlook, By Manufacturing & Industrial (2023-2034) (\$MN)

Table 38 Global Data Security Posture Management (DSPM) Market Outlook, By Telecommunications (2023-2034) (\$MN)

Table 39 Global Data Security Posture Management (DSPM) Market Outlook, By Energy & Utilities (2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

## I would like to order

Product name: Data Security Posture Management (DSPM) Market Forecasts to 2034 – Global Analysis By Data Environment (Public Cloud, Private Cloud, Hybrid Cloud, SaaS Applications, and Data Lakes and Data Warehouses), Component, Organization Size, Data Sensitivity Level, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/D7405078C6BCEN.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](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/D7405078C6BCEN.html>