

Understanding DSPM: The Foundation of Modern Data Security

EXECUTIVE SUMMARY

DSPM has evolved from protecting data to securing how that data is used across AI systems. As AI becomes embedded in business workflows, organizations need visibility and control over how sensitive data is accessed, used, and exposed across both data and AI.

Introduction to DSPM

Market Context

The digital transformation of business has led to an explosion of data—and now, an explosion of AI systems that depend on that data. Organizations are rapidly adopting copilots, LLMs, and AI-driven applications that consume enterprise data in new ways.

This creates a new challenge: data is no longer just stored and accessed—it is continuously ingested, learned from, and exposed through AI interactions.

As a result, organizations must not only protect where data lives, but also:

- What data is used to train AI models
- What data is exposed through prompts and outputs
- How AI systems access and interact with sensitive data

Evolution of Data Security

The journey to DSPM reflects the evolution of enterprise data security:

- First Generation: Perimeter-based security focused on protecting network boundaries
- Second Generation: Data Loss Prevention (DLP) aimed at controlling data movement

- Third Generation: Cloud Access Security Brokers (CASB) extended security to cloud services
- Current Generation: DSPM provides comprehensive data-centric security across all environments

Why DSPM Matters Now

Several factors make DSPM essential in today's digital landscape:

- Multi-cloud complexity has created new blind spots in data security
- Regulatory requirements demand greater control over sensitive data
- AI adoption introduces new risk surfaces across training data, prompts, and model outputs
- Shadow AI and unsanctioned model usage create blind spots for sensitive data exposure
- AI systems require governed, high-quality data to avoid risk, bias, and leakage
- Data is now actively used—not just stored—requiring continuous visibility and control
- Remote work has dissolved traditional security perimeters
- The cost of data breaches continues to rise dramatically

Core DSPM Capabilities

Data + AI Discovery

DSPM must extend beyond discovering where data lives to understanding how it is used by AI systems. This includes identifying data flowing into models, prompts submitted to AI tools, and outputs generated by AI systems.

Key discovery capabilities include:

- Automated scanning of cloud storage and databases
- Deep inspection of SaaS applications
- Analysis of data warehouses and lakes
- Discover data used for AI training, fine-tuning, and retrieval (RAG)
- Identify sensitive data exposed through AI prompts and copilots
- Map data flows between enterprise systems and AI models
- Detect shadow AI usage across SaaS and developer environments

AI-Aware Risk Assessment

Risk assessment in DSPM represents a multi-dimensional approach that goes far beyond traditional security scanning. Risk assessment must account for how data is used in AI—not just where it is stored. By correlating these various risk factors, DSPM enables security teams to prioritize remediation efforts effectively and allocate resources where they will have the greatest impact.

Key risk dimensions include:

- Security risks from improper access controls or configurations
- Compliance risks related to regulatory requirements
- Exposure of sensitive data through AI prompts and outputs
- Over-permissioned AI agents and copilots
- Use of unapproved or unsanctioned AI tools
- Training models on sensitive, regulated, or low-quality data
- Data leakage through embeddings, vector DBs, or model responses
- Privacy risks concerning personal data handling
- Sovereignty risks regarding data location and transfer

AI Risk Mitigation

One of DSPM's most powerful features is its ability to automate remediation actions across the enterprise data landscape. Rather than simply identifying issues, these platforms can take immediate action to address security concerns—including risks introduced by AI systems.

Core remediation capabilities include:

- Automatic correction of misconfigurations
- Dynamic adjustment of access permissions
- Remove or mask sensitive data before AI training or ingestion
- Enforce policies on what data can be used in AI systems
- Restrict AI access to sensitive or regulated datasets
- Alert and block risky prompt activity
- Application of encryption or masking
- Enforcement of data lifecycle policies

Continuous Data + AI Monitoring

DSPM provides continuous visibility into both data and AI risk—monitoring how data is accessed, shared, and used across AI systems. The platform constantly assesses risk levels and adapts security controls as the environment changes.

Essential monitoring features include:

- Monitor prompt activity and data exposure in AI tools
- Track changes in AI data access and permissions
- Continuously assess AI-related risk posture

- Maintain audit-ready visibility across data and AI usage
- Automated policy enforcement
- Adaptive security controls

DSPM for AI Security & Governance

AI introduces a new layer of risk that traditional data security approaches were not designed to address. DSPM must evolve to secure not just data at rest, but data in use by AI systems.

Key areas where DSPM extends to AI include:

AI Data Security

- Identify and control sensitive data used in training and inference
- Prevent exposure of regulated or confidential data in AI systems

AI Prompt & Output Security

- Monitor prompts submitted to copilots and LLMs
- Detect and reduce sensitive data leakage in AI outputs

AI Access Governance

- Control what data AI agents and copilots can access
- Enforce least-privilege access for AI-driven workflows

Shadow AI Detection

- Discover unsanctioned AI tools and usage across the enterprise
- Reduce risk from uncontrolled data sharing with external models

AI Data Preparation

- Cleanse, classify, and curate data before it is used for AI
- Improve model quality while reducing risk

Business Benefits

Risk Reduction

Organizations implementing DSPM experience a significant decrease in their overall risk profile. By providing comprehensive visibility and control over sensitive data, these platforms effectively reduce the likelihood of data breaches and minimize the attack surface available to potential attackers.

Key risk reduction benefits include:

- Decreased likelihood of data breaches
- Reduced attack surface
- Minimized insider threat risks
- Lower third-party risk exposure
- Enhanced data governance

Compliance Automation

DSPM transforms the traditionally labor-intensive process of regulatory compliance into a streamlined, automated workflow. Organizations can continuously monitor their compliance status across multiple regulations and automatically generate required reports.

Primary compliance benefits include:

- Streamlined regulatory compliance
- Automated compliance reporting
- Reduced audit preparation time
- Improved compliance visibility
- Standardized controls across environments

Operational Efficiency

Beyond its security benefits, DSPM drives substantial operational improvements across the organization. The automation of routine tasks frees up security teams to focus on more strategic initiatives.

Key operational improvements include:

- Automated data discovery and classification
- Reduced manual security tasks
- Faster incident response
- Improved cross-team collaboration
- Enhanced decision-making through better visibility

Cost Savings

The financial benefits of DSPM extend across multiple areas of the organization. Through better data lifecycle management and automated processes, organizations can significantly reduce both direct and indirect costs.

Notable cost benefits include:

- Reduced data storage costs through better lifecycle management
- Lower compliance and audit costs
- Decreased incident response expenses
- Optimized security tool investments
- Prevented breach-related costs

Implementation Considerations

Key Success Factors

Successful DSPM implementation requires careful attention to several critical factors. Executive sponsorship and stakeholder alignment are essential, as the platform touches multiple areas of the organization and may require changes to existing processes.

Critical success factors include:

- Executive sponsorship and stakeholder alignment
- Clear objectives and success metrics
- Phased implementation approach
- Cross-functional team involvement
- Comprehensive change management plan

Common Challenges

Understanding common implementation challenges in advance helps teams prepare effective mitigation strategies and set realistic expectations.

Frequent implementation challenges include:

- Data sprawl across multiple environments
- Legacy system integration
- Resource constraints
- Cultural resistance
- Technical complexity

Best Practices

Drawing from successful implementations, several best practices have emerged that can help organizations maximize the value of their DSPM deployment.

Recommended best practices include:

- Starting with high-risk data areas

- Establishing clear governance structures
- Implementing automated workflows
- Maintaining stakeholder communication
- Regular testing and validation

Future Outlook

Industry Trends

The future of DSPM is tightly coupled with AI security and governance. As organizations embed AI across business processes, DSPM will evolve into a unified control plane for both data and AI risk.

Key emerging trends include:

- Convergence of DSPM and AI Security Posture Management (AI-SPM)
- Increased focus on governing data used by AI systems
- Expansion into prompt security, model risk, and agent governance
- Continuous alignment between data quality, security, and AI outcomes
- Enhanced automation and orchestration
- Greater integration with existing security tools

Evolution Path

Organizations are increasingly seeking solutions that can address both current and emerging challenges across data and AI. The most forward-looking DSPM platforms will serve as a unified foundation for data security and AI governance.

Expected evolution areas include:

- Increased focus on data value alongside risk
- Enhanced support for emerging data types
- Greater emphasis on privacy engineering
- Integration with zero trust architectures
- Advanced predictive capabilities

Emerging Use Cases

As organizations face new challenges and requirements, DSPM platforms are expanding to address new use cases and scenarios. These emerging applications demonstrate the technology's flexibility and ongoing relevance.

Notable emerging use cases include:

- AI model security and data governance
- Data sovereignty compliance
- Privacy-preserving analytics
- Automated data governance
- Real-time risk adaptation

Conclusion

DSPM is no longer just about protecting data—it is about enabling organizations to safely use data in AI. As data becomes the foundation of AI systems, organizations must connect the dots between data security and AI governance.

By extending DSPM to cover AI, organizations gain the visibility and control needed to reduce risk, improve AI outcomes, and confidently scale AI adoption.

CUSTOMER VALIDATION

Proof in Action

"BigID gives me better visibility into sensitive data, helps prioritize security protections, reduces attack surfaces, strengthens compliance, and increases operational efficiency overall — a strategic pillar of our AI-First Cybersecurity Transformation"

- CISO, Global Healthcare Company

"We needed to automate processes and data management across systems for the data of a few million customers across a lot of systems and data. BigID was the one solution that did this in the most efficient and sophisticated way - and had more use cases we could add on moving forward."

- Chief Privacy Officer, Global Telecoms Company

ANALYST RECOGNITION

Validated by Industry Leaders

- 2025 Company of the Year for AI Governance - Frost & Sullivan
- Named a Leader across all DSPM research including Omdia DSPM Universe, CB Insights for DSPM, TAG, GigaOm, Frost & Sullivan
- Named a Leader in all Privacy Management evals including Forrester Privacy Management Wave & IDC Privacy Compliance MarketScape
- BigID named a Leader across 4 GigaOm evals: DSPM, Data Security Platforms, Unstructured Data Management, Data Access Governance
- Named in Gartner's 2025 DLP Market Guide
- Named in Gartner's 2025 AI TRiSM Market Guide
- Represented 30+ times in Gartner's 2025 Hype Cycles for Security, Privacy, AISPM

FREE RISK ASSESSMENT

Discover Your Data & AI Risk

An agentless, cloud-native assessment to enable security, privacy, and compliance: pinpoint where sensitive data and AI risks live - and how to fix them.

What You Get:

- Complementary 2 week engagement on real data to gain visibility on risk across data and AI
- Executive-ready report identifying high-risk data and AI across cloud environments with next-step recommendations

NEXT STEPS

Ready to Connect the Dots in Data & AI?

Schedule your free risk assessment or ask for a deeper demo across DSPM, DLP, AI SPM, Privacy Automation, AI Risk, and Data Lifecycle Management

► www.bigid.com/demo

► www.bigid.com/risk-assessment

► info@bigid.com



BigID Next

"The features they offer are the moat that they have built around the product. This is what makes them the market leader in Data Privacy and Protection."



IT Security & Risk Management Associate - Banking

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.



BigID Next

"Exceptionally powerful and easy to use tool that integrated smoothly into our environment and delivered value from day one. The BigID team is fabulous to work with."



Senior Vice President & Chief Data Officer - Banking

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.