

Data Security in the Age of AI: DSPM, AI-SPM, and the Case for a Unified Approach



DSPM and AI-SPM are not parallel tracks. As AI adoption accelerates, organizations need more than visibility: they need a unified platform that turns data intelligence into action, governs agentic access in real time, and extends security posture across every AI system, pipeline, and model in the enterprise. BigID delivers both.

Visibility Was Never the Finish Line

For years, the promise of DSPM was simple: know where your sensitive data is. Visibility was a meaningful step forward. Organizations were flying blind across cloud, SaaS, and on-prem environments, with no clear picture of what data existed, where it lived, or who could touch it.

But visibility without action is just a longer list of problems to worry about. Today's threat landscape, accelerated by AI adoption, cloud sprawl, and compounding regulatory pressure, demands that DSPM evolve from a discovery tool into a remediation engine. BigID was built for exactly that evolution.

DSPM That Actually Reduces Risk

The most mature DSPM programs are not just finding sensitive data. They are doing something about it. BigID moves beyond dashboards and into workflows that close real risk.

Risk-based prioritization that cuts through noise. Not every finding is equal. BigID ranks exposure by sensitivity, access, regulatory context, and business impact, so security teams focus on what actually matters instead of chasing volume.

Access intelligence and least privilege enforcement. Knowing data exists is not enough if anyone can reach it. BigID surfaces who has access, who should not, and

what toxic combinations of permissions create hidden risk — including service accounts, third-party integrations, and automated processes, not just human users.

Policy enforcement at scale. In BigID, discovery triggers action: automated retention enforcement, tagging, quarantine, deletion workflows, and de-identification, without requiring a ticket queue and a team of engineers to execute on every finding.

Continuous posture monitoring. Data environments change constantly. A DSPM that runs quarterly is not a security control; it is an audit artifact. BigID monitors continuously and responds in near real-time as data moves, changes, and accumulates new risk.

Remediation that closes the loop. The gap between 'we found a risk' and 'we fixed it' is where breaches happen. BigID integrates with ticketing systems, SOAR platforms, and enforcement controls to drive issues all the way to resolution, not just identification.

Governing the Agents: A New Access Problem

AI agents are changing the access governance problem in fundamental ways. Traditional access controls were designed for humans and later extended, imperfectly, to service accounts and APIs. Agentic AI systems break that model entirely.

An AI agent does not just access data. It reasons over it, combines it with other sources, and acts on it autonomously. That creates a new class of risk:

- Agents access far more data than any human user would, because they are designed to be comprehensive, not selective.
- Agent actions are often opaque. It is difficult to audit what data an agent consumed, what it inferred, and what it passed downstream.
- Agents operate at machine speed. By the time a risk is detected, the action may already be taken.
- Least privilege does not map cleanly to agentic workflows. Agents need dynamic, context-sensitive access that traditional RBAC was not built to handle.

Governing agentic access requires knowing not just what data an agent can reach, but what it should reach, based on the task, the sensitivity of the data, the regulatory context, and the downstream action being taken. BigID provides the data intelligence foundation that makes context-aware agentic governance possible, connecting data classification, access history, and risk posture to the agent layer in real time.

AI-SPM: Security for the AI Layer

As organizations deploy LLMs, copilots, RAG pipelines, and autonomous agents, they inherit a new layer of data risk that sits above the traditional DSPM scope. BigID's AI-SPM addresses that layer directly.

AI asset discovery across sanctioned and shadow deployments. You cannot govern what you cannot see. BigID surfaces every AI tool, model, and pipeline in use across the organization, including the ones IT never approved.

Data-to-AI lineage that answers the hard questions. The critical question is not just 'what AI systems do we have?' It is 'what sensitive data is feeding them?' BigID traces lineage from data source to AI input, so organizations understand exactly what is at risk if a model is compromised, jailbroken, or over-shares.

RAG pipeline visibility and control. Retrieval-augmented generation introduces a high-risk exposure surface: the knowledge base. If sensitive documents are indexed without classification, any authorized user or agent can surface them through a natural language query. BigID makes the knowledge base classified and governable before that happens.

Shadow AI detection and response. Employees are connecting company data to AI tools that IT never approved. BigID surfaces that activity so organizations can decide to block, govern, or formally sanction, rather than discover the exposure after the fact.

AI output risk monitoring. BigID can detect when models surface data they should not: PII in generated content, regulated data in AI responses, and confidential IP in copilot suggestions.

Regulatory alignment built in. The EU AI Act, NIST AI RMF, and a growing body of AI-specific regulation require organizations to classify AI systems by risk tier, document data inputs, and demonstrate governance controls. BigID provides the evidentiary foundation to meet those requirements without starting from scratch.

One Platform, One Risk Picture

DSPM and AI-SPM are not parallel tracks. They are a stack. AI risk is fundamentally a data risk problem, and you cannot govern the AI layer without a strong foundation underneath it.

BigID is built as a unified platform, which means DSPM and AI-SPM share the same discovery engine, classification layer, and risk context. That integration produces outcomes that siloed tools cannot match:

Unified classification across data and AI. The same sensitivity labels that govern data retention and access also govern what feeds AI systems. There is no gap between how data is classified and how AI risk is assessed.

A single, prioritized risk view. Instead of two separate tools generating two separate alert streams, BigID gives security and compliance teams one place to understand, prioritize, and act on risk across the entire data and AI estate.

Agentic governance that scales. As AI agents proliferate, BigID's combination of data intelligence and AI asset visibility creates the foundation for dynamic, context-aware access controls that keep pace with how fast AI is actually moving in the enterprise.

The organizations that navigate AI adoption with the least friction are the ones that treat data security and AI security as a single discipline. BigID makes that possible.

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.