

# BigID for AI Security & Governance



## EXECUTIVE SUMMARY

Discover, secure, and control AI risk across data, models, and usage. BigID unifies AI security posture management, prompt monitoring, data preparation, and access governance — connecting data risk to AI risk so teams can take action, not just gain visibility.

## Solution Overview

AI adoption is accelerating faster than organizations can control it — introducing shadow AI, data exposure, and new forms of access risk. BigID enables organizations to discover, secure, and govern AI across models, data, prompts, and access — all in one platform. It unifies AI security posture management, prompt monitoring, data preparation, and access governance with deep data context. Unlike fragmented tools, BigID connects data risk to AI risk — so teams can take action, not just gain visibility.

## Business Outcomes

### Eliminate Shadow AI Risk

Discover unsanctioned models, copilots, and AI usage across your environment before they introduce exposure.

### Reduce AI Data Exposure

Identify and control sensitive data flowing into AI models, prompts, and training pipelines.

### Enforce AI Governance at Scale

Apply consistent policies across AI models, data, and usage to meet regulatory and internal requirements.

### Secure AI Access and Usage

Govern who — and what — can access data through AI systems, including agents and copilots.

## Key Capabilities

- Discover shadow AI across cloud, SaaS, code, and AI environments
- Assess AI security posture and prioritize risk across models and data
- Monitor and protect sensitive data shared in AI prompts and copilots
- Prepare and curate high-quality, compliant AI training data

- Govern access to AI systems for users, applications, and agents
- 

## Why BigID for AI Security & Governance

### Data + AI Context Together

Connect data discovery, classification, and lineage directly to AI models and pipelines — not just surface-level AI visibility.

### First to Discover Shadow AI

Identify unsanctioned AI tools, copilots, and vendor models across the enterprise.

### Unified AI TRiSM Platform

Combine AI security posture management, risk assessment, and governance in one platform.

### Govern Models + Data Together

Bridge the gap between AI governance and data governance — control both in a single system.

### End-to-End AI Lifecycle Coverage

Secure everything from training data to prompts to model access and outputs.

### Enterprise-Scale, Agentless Deployment

Deploy across cloud, on-prem, SaaS, and AI environments with speed and scale.

---

## The Challenge

### AI Is Expanding Faster Than Security Can Keep Up

AI introduces a new attack surface that most organizations can't see or control. Shadow AI, sensitive data in prompts, ungoverned training data, and non-human access create compounded risk across security, privacy, and compliance. Traditional tools lack visibility into AI models, pipelines, and usage — leaving gaps in governance and control. As AI adoption grows, so does the urgency to understand how data flows into and through AI systems — and who can access it.

---

## The Solution

### Bring Control to AI — Across Data, Models, and Usage

BigID delivers a unified platform to discover, secure, and govern AI across its entire lifecycle. It identifies shadow AI, assesses AI risk, monitors prompt activity, prepares safe training data, and enforces access controls across human and non-human identities. By connecting data intelligence with AI security, BigID enables organizations to reduce exposure, enforce policy, and operationalize responsible AI — with continuous visibility and control.

---

## How It Works

BigID connects to AI systems, data sources, and environments across cloud, SaaS, and development stacks. It scans and classifies AI data objects — including datasets, models, vectors, and prompts — to identify sensitive data and risk. The platform enriches this data with context, lineage, and access intelligence to understand how data flows through AI systems.

Policies are applied to detect risk, trigger alerts, and prioritize remediation. Teams can then take action — from masking and restricting access to enforcing guardrails across AI usage.

---

## **Platform Capabilities**

### **Shadow AI Discovery**

Discover unsanctioned AI models, copilots, and vendor tools across your environment. Identify where AI is being used in code, SaaS, and enterprise systems, and map sensitive data flowing into these tools to reduce hidden risk.

### **AI Security Posture & Risk Management**

Continuously assess AI risk across models, datasets, and pipelines. Identify sensitive data exposure, over-permissioned access, and vulnerabilities, and prioritize remediation through policy-driven workflows.

### **AI Prompt Security**

Monitor and control data shared in prompts across copilots and AI applications. Detect sensitive data exposure, apply masking and labeling, and enforce policies to prevent data leakage before it leaves the enterprise.

### **AI Data Preparation & Pipeline Security**

Classify, curate, and cleanse data used for AI training and inference. Ensure datasets are accurate, compliant, and free of sensitive or risky data before they are used in models.

### **AI Access Governance**

Control access to AI systems and the data they use. Govern both human and non-human identities — including agents — to ensure only authorized access to sensitive data through AI.

### **AI Governance & Compliance**

Catalog AI models and data, enforce policies, and monitor compliance with evolving AI regulations. Maintain audit trails, accountability, and governance across the AI lifecycle.

**To learn more about how BigID secures your AI environment, visit [bigid.com](https://bigid.com)**

#### 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](http://www.bigid.com/demo)

► [www.bigid.com/risk-assessment](http://www.bigid.com/risk-assessment)

► [info@bigid.com](mailto: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.