

Shift Left in DSPM for DevSecOps & AI



EXECUTIVE SUMMARY

Modern applications are built fast—and increasingly powered by AI. As development accelerates, so does the risk of exposing sensitive data in code, pipelines, and AI systems. BigID enables organizations to shift left by embedding data security directly into the development lifecycle—identifying, governing, and remediating sensitive data risks before they reach production.

Data Risk Starts in Development—and Now Fuels AI

Data security is no longer just a runtime concern—it's a development problem. Applications are built using real data, shared across repos, and increasingly integrated with AI services. This creates new risks that traditional security tools don't see early enough—and they don't understand the data itself.

- Sensitive data embedded in source code, logs, and test datasets
- Secrets, tokens, and credentials exposed across dev environments
- Training data pipelines using uncurated or regulated data
- Developers unknowingly exposing data through AI prompts and copilots
- AI models and agents accessing data without proper governance

To reduce risk, organizations need to bring data awareness into AppSec and DevSecOps workflows.

Built for the Development Pipeline

BigID extends DSPM into the development lifecycle—giving AppSec and engineering teams visibility and control over sensitive data before deployment. Using APIs and native integrations, BigID embeds directly into CI/CD pipelines, repositories, and developer workflows.

Pipeline-Integrated Scanning

Scan code, data, and storage as part of build and deployment workflows to catch issues before they move forward in the pipeline.

Context-Aware Classification

Identify PII, secrets, regulated data, and high-risk data exposures across structured and unstructured sources with deep data intelligence.

Pre-Production Risk Detection

Catch sensitive data issues before code is merged or applications are released—preventing risk rather than detecting it after the fact.

Developer-Native Integrations

Push findings into tools like Jira with precise context, examples, and remediation guidance so developers can act immediately.

From Findings to Fixes: Developer-Driven Remediation

Security only works if developers can act on it. BigID operationalizes data security for developers by delivering actionable, in-context insights directly into their workflows.

- Route issues to the right developer automatically
- Provide exact location, data type, and risk context
- Deliver clear remediation guidance
- Track resolution with full auditability

Instead of vague alerts, developers get: "Here's the sensitive data. Here's where it lives. Here's why it matters. Here's how to fix it." BigID then re-validates fixes to ensure issues are resolved—creating a closed-loop remediation cycle.

Extending Shift Left to AI Security & Governance

Shifting left now must include AI. AI systems introduce entirely new data risks—because they don't just store data, they learn from it, generate from it, and expose it. BigID extends data security into AI pipelines and usage:

Secure AI Training Data

Discover and classify sensitive data used for model training. Remove or mask regulated data before it's learned by models, ensuring only appropriate data enters training pipelines.

Govern AI Data Access

Understand what data AI models and agents can access. Enforce least privilege for AI systems and copilots, and monitor and reduce overexposure of sensitive data.

Protect Against Prompt-Based Exposure

Identify sensitive data shared in prompts to LLMs. Monitor how data is used in AI interactions and reduce the risk of data leakage through AI outputs.

Detect Shadow AI in Dev Environments

Discover unsanctioned AI tools used by developers and assess risk of data exposure across AI services before it becomes a breach.

From Dev to AI to Prod: Continuous Control

BigID doesn't stop at the pipeline—it connects development, production, and AI systems with continuous visibility and control. By shifting left with BigID, organizations can:

- Prevent sensitive data exposure before release
- Reduce secrets sprawl across code and pipelines
- Govern data used in AI training and inference
- Align AppSec, DevOps, and data security teams
- Reduce security friction while accelerating delivery

Data-Aware DevSecOps Starts Here

BigID bridges the gap between data security and application security—bringing sensitive data awareness directly into the tools and workflows developers already use. From code to pipelines to AI, BigID enables teams to find sensitive data early, fix issues faster, govern AI responsibly, and reduce risk continuously.

Don't wait for production—or AI incidents—to uncover data risk. Find it. Fix it. Control it—before it spreads.

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.