

Evaluating DSPMs Through a Third-Party Risk Lens



EXECUTIVE SUMMARY

When procurement evaluates a DSPM, the question is not just whether the platform can discover sensitive data—it's whether adopting that platform introduces new third-party risk to the firm. This checklist helps procurement teams assess enterprise architecture, customer control, and vendor maturity.

Why This Matters to Procurement

A DSPM can expand third-party risk in several ways: by requiring highly privileged access into production systems, by moving or copying sensitive data into vendor-controlled environments, by limiting customer control over encryption keys and credentials, by exposing reports and metadata to vendor personnel, by operating as a black box with weak auditability, by creating long-term dependence on vendor-managed services, and by lacking the maturity needed to operate safely across both cloud and data center environments.

These are classic procurement concerns because they affect not just security, but also legal risk, contractual leverage, compliance obligations, and the firm's ability to maintain operational control.

What "Enterprise-Class Architecture" Means for Procurement

From a procurement perspective, mature architecture means the product was designed to preserve customer control from the beginning. That includes control over keys, credentials, scanned data, reports and findings, access rights, audit evidence, and deployment models.

Many of these controls are hard to add later. If a product was not originally architected for customer-controlled keys, segregated storage, least-privilege connectors, in-product reporting, or strong RBAC, those gaps usually reflect deeper product immaturity rather than missing surface features.

Procurement Checklist for DSPM Third-Party Risk

1. Customer Control Over Encryption and Crypto Trust

- Does the platform support customer-controlled encryption keys such as BYOK?
- Can the customer retain control over key ownership and lifecycle?
- Does the platform support key rotation?
- Is the encryption model aligned with enterprise and regulated-environment expectations?

Why procurement should care: This affects dependency on vendor-managed trust, contractual exposure, and risk acceptance for sensitive or regulated data.

2. Customer Control Over Credentials

- Does the platform integrate with approved enterprise password vaults?
- Can the customer keep service account credentials in its own vault?
- Does the vendor require direct possession of privileged credentials?
- Is secrets handling aligned with enterprise credential governance?

Why procurement should care: If the vendor must directly hold or manage critical credentials, the firm is accepting a materially larger third-party risk surface.

3. Control Over Scanned Data

- Does the platform avoid unnecessary copying of sensitive data?
- Can the vendor clearly document what data is copied, staged, cached, or stored?
- Does the architecture avoid backhauling on-prem or data center content into vendor infrastructure?
- Can scanning occur without expanding the firm's sensitive-data footprint?

Why procurement should care: Every additional copy of sensitive data increases breach exposure, discovery burden, and contractual risk.

4. Control Over Metadata, Findings, and Reports

- Where are scan results, metadata, and findings stored?
- Are customer reports generated and retained inside the customer's controlled environment or in vendor-managed infrastructure?
- Can vendor personnel access customer findings, analytics, or reports?
- Does the customer have direct access to in-product reporting and evidence?

Why procurement should care: Reports and findings can themselves contain highly sensitive information about regulated assets, exposures, and internal control gaps.

5. Least-Privilege Access Into the Environment

- Can the platform operate without elevated admin rights for scanning?

- Are permissions narrow and scoped by design?
- Can the vendor prove least-privilege operation in a live evaluation?
- Is the scanning model appropriate for both cloud and data center systems?

Why procurement should care: The broader the required privileges, the higher the potential blast radius if the product, its credentials, or vendor operations are compromised.

6. Data Isolation and Tenant Separation

- Are customer environments, metadata, and findings isolated from other customers?
- Is segregation preserved in multi-tenant deployments?
- Is the architecture appropriate for sensitive and regulated data?

Why procurement should care: Weak isolation increases cross-customer exposure risk and can undermine assurances around privacy, confidentiality, and incident containment.

7. Auditability and Oversight

- Are access logs available for customer review?
- Are policy and configuration changes logged?
- Can the customer independently audit platform usage and change history?
- Can the vendor demonstrate evidence of who accessed what and what changed?

Why procurement should care: A third party operating in sensitive systems must be auditable. Without strong logs, oversight becomes weaker and incident response becomes harder.

8. Self-Service Versus Vendor Dependency

- Can the customer control setup, configuration, reporting, and operations directly?
- Or does the product depend heavily on vendor-managed operations?
- Can the customer administer the platform without permanent vendor involvement?
- Does the operating model preserve customer autonomy?

Why procurement should care: Heavy vendor dependence increases operational risk, weakens customer control, and can create switching costs and contract leverage issues later.

9. Regulated and Sovereign Deployment Readiness

- Does the platform support deployment models that align with the firm's regulatory and residency requirements?
- Can it support cloud, single-tenant, sovereign, hybrid, or data center-aligned deployments where needed?
- Is support available for frameworks or environments associated with FedRAMP, HIPAA, PCI, FIPS, or similar requirements?

Why procurement should care: A platform that cannot align with regulatory or regional constraints may create legal and compliance issues regardless of technical merit.

10. APIs, Automation, and Future-Proofing

- Does the platform provide real product APIs?
- Is MCP or similar modern automation support available?
- Can the product be integrated into enterprise workflows without relying on vendor-managed exports or manual workarounds?

Why procurement should care: Mature products are easier to govern, automate, and integrate. Closed products often create long-term vendor dependence and higher operating cost.

What Procurement Should Look for in a Mature DSPM Vendor

A procurement team should favor vendors whose architecture clearly preserves customer control over the things that matter most: keys, credentials, scanned data, reports and findings, access rights, deployment options, and audit evidence.

These are all indicators that the product was built to be enterprise class. They also signal something else important: maturity. Products that preserve customer control in these areas are usually the result of deliberate, foundational architecture choices made early in the life of the platform.

Products that do not often require the customer to compensate through higher trust, more contract negotiation, more oversight, or acceptance of structural risk. From a procurement perspective, that means architecture is not just a technical issue—it is a commercial and risk issue.

Top Procurement Questions to Ask Every DSPM Vendor

- Can we keep our own encryption keys under our own control?
- Can we keep credentials in our own approved vault?

- Can you prove sensitive data is not copied or backhauled unnecessarily?
- Where are metadata, findings, and reports stored, and who can access them?
- Can you demonstrate least-privilege scanning live?
- Can we operate the product ourselves without ongoing dependence on vendor personnel?
- Can you demonstrate tenant isolation, audit logs, and policy change tracking?
- Was this architecture designed this way from the start, or added later?

Bottom Line for Procurement

When evaluating DSPMs, procurement should think like a third-party risk team: If this product were compromised, what would it expose about our data, our network, our credentials, and our operations?

The best answers usually come from products with mature, enterprise-class architecture that preserve customer control over keys, credentials, scanned data, reports, and governance workflows. Those controls do more than reduce technical risk—they reduce contractual exposure, operational dependence, and long-term risk to the firm.

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.