

CISO Checklist: What to Look for in a DSPM



EXECUTIVE SUMMARY

A DSPM platform is not just a discovery tool — it becomes a privileged system operating inside your most sensitive environments. Use this checklist to evaluate whether a DSPM is truly built for enterprise cloud and data center environments.

1. Architecture and Product Maturity

- Was the platform designed from the start for enterprise and regulated environments, or were controls added later?
- Does the architecture reflect core design decisions around security, isolation, auditability, and scale?
- Can the platform operate consistently across cloud, SaaS, and data center environments?
- Does the vendor demonstrate maturity in hybrid and large-scale deployments, not just cloud-only demos?

2. Data Isolation and Customer Trust

- Are customer data stores and metadata clearly isolated?
- Is isolation preserved even in multi-tenant environments?
- Does the platform reduce cross-customer exposure risk?
- Is the product architecture appropriate for highly sensitive or regulated data?

3. Customer Control Over Encryption and Secrets

- Does the platform support Bring Your Own Keys?
- Does it support encryption key rotation?
- Does it integrate with enterprise password vaults?
- Can the customer keep credentials and encryption controls under its own governance model?

4. Least-Privilege Scanning

- Can the platform scan without elevated admin rights?
- Are permissions scoped by design rather than broad and over-privileged?
- Can the vendor prove this live in a POC?
- Is the scanning architecture appropriate for sensitive cloud and data center systems?

5. Data Handling and Exposure Minimization

- Does the platform avoid unnecessary copying of sensitive data?
- Can the vendor prove what is and is not staged, cached, or replicated?
- Does the architecture avoid backhauling on-prem data into vendor-controlled environments?
- Can the platform inspect and govern data without creating secondary repositories?

6. RBAC and Segregation of Duties

- Does the platform support granular RBAC beyond simple admin-versus-user roles?
- Can roles be scoped for admins, analysts, data owners, reviewers, and remediation teams?
- Does RBAC extend to APIs, automation, and AI-driven access?
- Is segregation of duties enforceable at enterprise scale?

7. Auditability and Evidence

- Are full access logs available?
- Are policy and configuration changes logged?
- Can the team review audit evidence directly in the product?
- Can the platform support independent audit and control validation?

8. Scan Telemetry and Operational Transparency

- Does the platform provide telemetry for scan status, failures, skips, and performance?
- Can you verify what was scanned, what was not, and why?
- Does it support differential scanning to reduce operational overhead?
- Does the scan framework appear built for production scale rather than one-time discovery?

9. Actionability and Downstream Control

- Does the platform move beyond visibility into action?
- Can it support integrated labeling, masking, revocation, or remediation workflows?
- Does it align with downstream controls and enforcement systems?
- Is the platform designed to reduce risk, not just report it?

10. Regulated-Environment Readiness

- Can the vendor provide evidence of support for environments requiring FedRAMP, HIPAA, PCI, FIPS, or similar controls?
- Does the architecture support sovereignty and residency-sensitive use cases?
- Does the product appear built for enterprise governance requirements rather than general-purpose deployment?

11. AI Governance and Future Readiness

- Is product AI transparent and governable?
- Can the customer constrain or control AI use where needed?
- Is there support for bring-your-own-AI or governed AI options?
- Does the platform support APIs or MCP for future automation, orchestration, and agentic workflows?
- Does the architecture look future-proofed for AI-driven operating models?

12. Fit for Enterprise Cloud and Data Center Operations

- Can the platform operate securely across both modern cloud environments and traditional data center systems?
- Does the product handle the realities of hybrid architecture without weakening controls?
- Can it scale operationally without forcing risky compromises in privilege, data movement, or auditability?
- Does the platform show signs of enterprise maturity that would be difficult to retrofit later?

Top 5 Validation Questions for a CISO

1. Can you prove scanning works without elevated admin access?
2. Can we keep credentials in our own vault and keys under our own control?
3. Can you prove sensitive data is not copied or backhauled?
4. Can you demonstrate granular RBAC and full audit logging live?
5. Which of these controls were built into the architecture from the beginning versus added later?

Bottom Line

A mature DSPM should show that its product security controls are the result of early architectural decisions, not late-stage patchwork. That is often the clearest sign that the platform is truly enterprise class and ready for sensitive cloud and data center environments.

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.