

What to Look for in a DSPM From a Product Security Lens

EXECUTIVE SUMMARY

A DSPM platform is not just a feature decision — it is an architectural decision. This checklist helps CISOs evaluate DSPM platforms through the lens of product security: the foundational controls that separate enterprise-ready platforms from those still growing into it.

Choosing a DSPM platform is not just a feature decision. It is an architectural decision.

DSPM platforms operate deep inside your most sensitive environments — across cloud, SaaS, and the data center. They scan critical systems, interact with sensitive data, store classification metadata, connect to privileged infrastructure, and increasingly drive automated remediation.

That level of access introduces a fundamental truth: you are not just evaluating what the platform discovers — you are evaluating how the platform itself is built. And that is why product security is one of the clearest signals of platform maturity.

Product Security Is Not a Feature — It's the Architecture

The strongest DSPM platforms do not treat product security as a bolt-on capability. They embed it into foundational design decisions:

- How customer data is isolated
- How credentials are managed and secured
- How scanning operates under least privilege
- How telemetry and auditability are captured
- How APIs and RBAC are structured
- How the platform scales across hybrid and regulated environments

These are not secondary concerns. They are core architectural choices that directly shape **risk exposure**, **operational trust**, **scalability**, and **enterprise readiness**. A platform can look compelling in a demo — and still fail under real-world conditions. The difference almost always comes down to these underlying decisions.

Why Product Security Is a True Maturity Signal

Many of the most important security controls in a DSPM cannot be easily added later. They are deeply tied to how the system was originally designed:

- Whether data is isolated or pooled
- Whether encryption supports customer-controlled keys from the start
- Whether scanning was designed for least-privilege access
- Whether the platform depends on copying or moving sensitive data
- Whether observability is built into the control plane
- Whether APIs and RBAC were designed for enterprise workflows — not retrofitted

These are not cosmetic differences. They determine whether a platform can actually operate in large-scale, regulated, hybrid environments — or whether it was optimized for simpler use cases. And this is where immaturity shows up quickly: over-privileged access requirements, weak credential governance, limited support for on-prem or sovereignty constraints, poor visibility into scan behavior, and rigid deployment models. In enterprise environments, these are not inconveniences — they are blockers.

The Reality of Modern Scanning Environments

A modern DSPM platform must operate across fundamentally different environments: cloud-native systems with API-driven scale, SaaS platforms with rate limits and delegated permissions, on-prem and data center systems with strict residency and access constraints, and hybrid architectures spanning all of the above.

A mature platform cannot compromise security posture to operate across these environments. That's why controls like **no unnecessary data copying**, **no backhauling of sensitive data**, **customer-controlled encryption**, **password vault integration**, **granular RBAC**, **full audit logging**, and **scan telemetry and transparency** are not “nice to have.” They are the difference between a platform that works in a demo and a platform that works in enterprise reality.

Why These Controls Are Hard to Retrofit

There is a common assumption that vendors can “add” enterprise-grade controls over time. In practice, many of these capabilities depend on foundational design decisions:

- **Data isolation** depends on tenancy and storage architecture
- **BYOK** depends on how encryption was designed from the beginning
- **Least-privilege scanning** depends on connector and control-plane design
- **No data copying** depends on where computation happens
- **Granular RBAC** depends on deeply embedded authorization models
- **Auditability** depends on observability being built into workflows
- **APIs and automation** depend on whether the platform was designed as an open control surface

In other words: these are not features you add. They are decisions you make early — or live without later.

DSPM Product Security Criteria

Below are the core capabilities that signal true platform maturity — not just functionality.

1. Data Isolation

Strong customer isolation reduces cross-customer risk and is essential for regulated environments.

Maturity signal: Designed into the platform — not layered onto shared infrastructure.

2. Customer-Controlled Encryption (BYOK)

Preserves control over encryption and reduces dependency on vendor-managed trust. **Maturity signal:**

Native crypto separation, not an afterthought.

3. Least-Privilege Scanning

Scanning should not require elevated admin access. **Maturity signal:** Built into connector and access design — not just guidance.

4. No Unnecessary Data Copying

Minimizes exposure and governance overhead. **Maturity signal:** Indicates architecture designed for control — not convenience.

5. No Backhauling of Sensitive Data

Especially critical for on-prem and regulated environments. **Maturity signal:** Reflects true hybrid readiness.

6. Password Vault Integration

Supports enterprise credential governance models. **Maturity signal:** Fits into existing security operations — not replacing them.

7. Granular RBAC

Supports real-world enterprise roles and separation of duties. **Maturity signal:** Deep, system-wide authorization — not surface-level roles.

8. Full Audit Logging

Captures both access and configuration changes. **Maturity signal:** Built for governance, not just functionality.

9. Scan Telemetry & Transparency

Provides visibility into scan behavior, quality, and performance. **Maturity signal:** Operational trust is a first-class concern.

10. Integrated Labeling & Control Alignment

Connects discovery directly to action. **Maturity signal:** Designed for outcomes, not just insights.

11. Differential Scanning

Reduces overhead in dynamic environments. **Maturity signal:** Built for production-scale operations.

12. Key Rotation

Supports strong crypto hygiene. **Maturity signal:** Indicates mature security lifecycle management.

13. Dynamic Masking & Access Controls

Enables real risk reduction — not just visibility. **Maturity signal:** Moves beyond detection into control.

14. Regulated Environment Readiness

Supports frameworks like FedRAMP, HIPAA, PCI, FIPS. **Maturity signal:** Proven enterprise and regulatory investment.

15. AI Transparency & Governed AI Options

Provides control and explainability for AI-driven features. **Maturity signal:** Future-ready for AI governance requirements.

16. APIs & MCP Access

Enables automation, integration, and agent-driven workflows. **Maturity signal:** Open, extensible, ecosystem-ready architecture.

What This Means for Buyers

A DSPM platform can be functionally strong — and still be architecturally immature. That's why product security should be treated as a primary evaluation lens. Buyers should look for clear evidence that a platform can:

- Operate under least privilege
- Integrate with existing credential and crypto controls
- Avoid unnecessary data movement
- Support regulated and hybrid environments
- Provide deep operational visibility
- Extend into automation and broader workflows

The strongest platforms show consistency across all of these dimensions: architecture, controls, observability, and deployment model all reflect a deliberate design for enterprise-scale environments.

DSPM Product Security Evaluation Checklist

Use this during demos, security reviews, and POCs.

Architecture & Isolation

- ☐ Is customer data fully isolated?
- ☐ How are metadata and findings segregated?
- ☐ Does the model support regulated or sovereign deployments?

Encryption & Secrets

- ☐ Does the platform support BYOK and key rotation?
- ☐ Can credentials remain in your vault?
- ☐ Is crypto control native or layered?

Access & Privilege

- ☐ Can scanning run without admin rights?
- ☐ Is RBAC granular and consistent across APIs and UI?

Data Handling

- ☐ Is sensitive data copied, cached, or replicated?
- ☐ Is on-prem data ever backhauled?

- Can governance happen without creating new data stores?

Auditability

- Are access and configuration logs complete and accessible?
- Can you prove who did what — and when?

Scan Operations

- Is scan telemetry visible and actionable?
- Does it support differential scanning?
- Can scan completeness be validated?

Actionability

- Does the platform drive labeling, masking, or access changes?
- Does it move from insight to control?

Compliance & Regulation

- Does it support required frameworks (FedRAMP, HIPAA, PCI, etc.)?
- Is the architecture aligned with regulated environments?

AI & Automation

- Is AI usage transparent and controllable?
- Does it support governed AI or BYO-AI?
- Are APIs and MCP available for automation?

The Questions That Separate Vendors

Ask every DSPM vendor:

- Can you prove scanning works without elevated privileges?
- Can we retain control of keys and credentials?
- Can you prove sensitive data is not copied or moved?
- Can you demonstrate RBAC and audit logging live?
- Which of these capabilities were designed from the start vs. added later?

The answers will tell you more than any feature list.

Final Takeaway

When evaluating DSPM, don't just ask: **"What can it find?"** Also ask: **"What do its product security controls reveal about how it was built?"** Because that question exposes the real difference — between platforms designed for enterprise reality, and platforms still growing into it.

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.