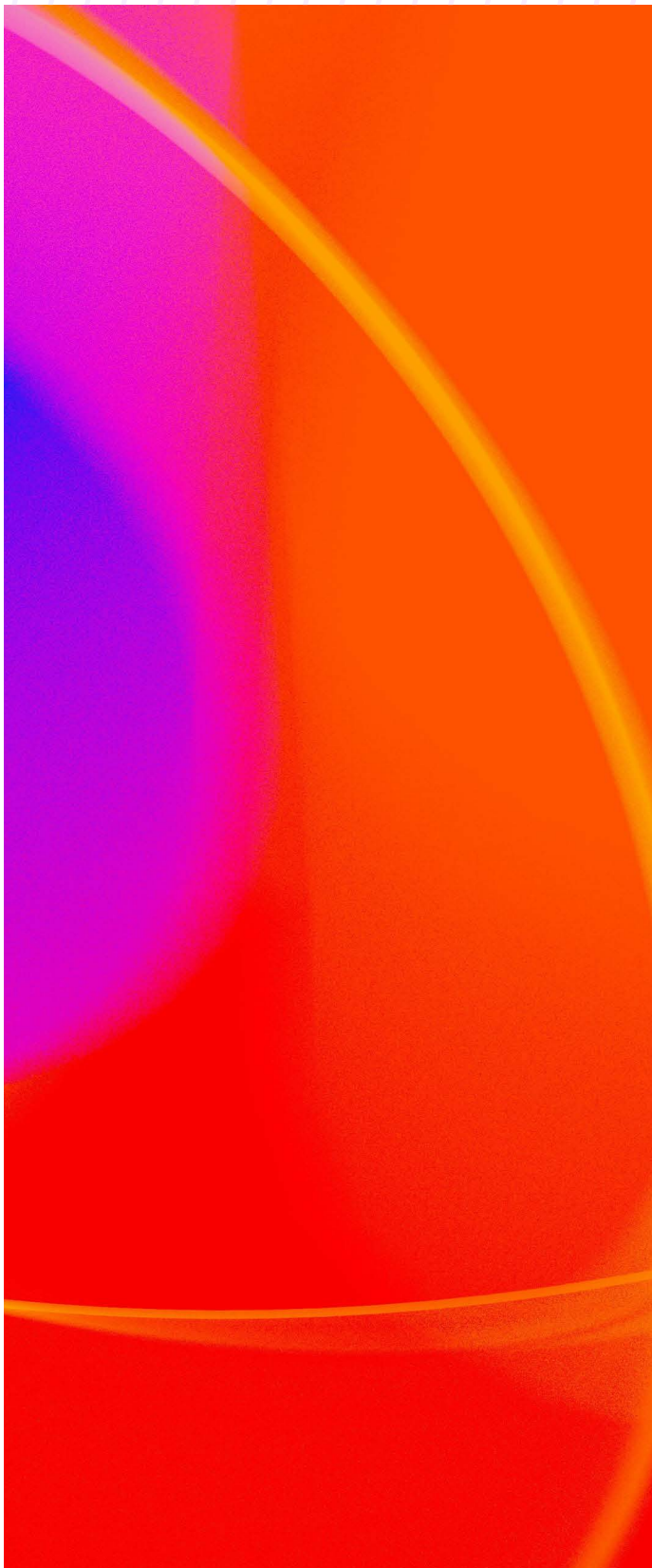
2025 GUIDE

The Ultimate Guide to a Data Security Platform

For CISOs Navigating Risk, Regulation, and AI-Driven Complexity

---

In today's high-stakes data landscape, CISOs are charged with more than perimeter defense—they're accountable for data and AI risk across an expanding, interconnected environment. Cloud migration, AI enablement, insider threats, and regulatory pressure all converge at one common denominator: data.



2025 Guide
The Ultimate Guide to a Data Security Platform

2025 Guide

The Ultimate Guide to a Data Security Platform

This guide provides a comprehensive blueprint for building and operationalizing a modern Data Security Platform (DSP). It outlines the foundational components, critical capabilities, and business outcomes required for resilient, compliant, and future-ready data protection.

Core Components of a Modern DSP

1. Data Discovery & Contextual Classification

Visibility is the first step to control. BigID offers unmatched discovery across structured, unstructured, and semi-structured data, powered by advanced ML classifiers and contextual analysis of the data itself. This gives you clarity into what sensitive data exists, whose it is, where it lives, and how it's at risk.

Core discovery classification requirements include:

- Automated, deep discovery of sensitive, personal, regulated, and high-value data—across cloud, on-prem, SaaS, and structured/unstructured sources.
- Contextual classification based on data type, policy, sensitivity, and business context.
- The ability to differentiate between sensitive, personal, regulated, high-risk, and high-value data.

2. Data Security Posture Management (DSPM)

DSPM extends visibility into action. BigID continuously monitors your data estate, uncovering overexposure, misconfigurations, privilege creep, and shadow data. Risk is prioritized with rich metadata and behavioral signals, so teams focus where it matters most.

Core DSPM requirements include:

- Continuous monitoring of security posture across multi-cloud and hybrid environments.
- Identification of shadow data, toxic combinations, overexposure, misconfigurations, and privilege creep.
- Actionable insights & alerts for prioritized remediation and policy enforcement.
- Ability to take action and mitigate risk on critical issues

3. AI Security and GenAI Readiness

AI introduces new risks around training data, model leakage, and prompt misuse. BigID enables discovery, classification, and policy control for AI data pipelines—protecting sensitive data inputs and outputs in GenAI workflows.

Core AI Governance and Security requirements include:

- Automated inventory of AI data and AI models
- Access management for AI models
- The ability to govern what data AI can see, access, train on, and generate.
- Actionable alerting on AI risk

4. Remediation and Risk Reduction

Most platforms surface issues. BigID solves them. Built-in remediation actions include access revocation, deletion, quarantine, and workflow escalation - directly from the platform or through integrations with ITSM and orchestration tools.

Core remediation requirements for a data security platform include:

- Ability to revoke excessive permissions, delete risky or redundant data, or quarantine data at risk—all natively.
- Alignment to risk, ownership, and compliance policies.
- Automated workflows across data owners, security teams, and governance stakeholders.

5. Insider Risk Management

BigID correlates data sensitivity with user access patterns to surface insider risks, giving teams the context needed to reduce dwell time and prevent accidental or malicious misuse.

Core insider risk management requirements include:

- Monitoring data access for anomalous or excessive activity.
- Connecting user access to data sensitivity and business role.
- Detection of overexposed data and overprivileged users

6. Cloud Data Loss Prevention (Cloud DLP)

Unlike legacy DLP tools that rely on static rules and signatures, BigID's cloud-native DLP is dynamic, content-aware, and risk-contextual. It spans IaaS, SaaS, and PaaS—surfacing exfiltration risks and enabling real-time policy enforcement.

Core Cloud DLP requirements include:

- Content-aware, context-driven controls to minimize noise and false positives
- Automation to enforce policies across SaaS, IaaS, and PaaS.
- Labelling and tagging to extend enforcement across your existing tech stack

7. Policy Management & Enforcement

BigID provides centralized, flexible policy management with support for Zero Trust principles. Define policies based on role, regulation, data type, region, purpose, and more—and enforce them across your entire ecosystem.

Core policy management requirements include:

- Fine-grained, cross-domain policies for access, retention, minimization, and transfer.
- Native and customizable policies that extend to regulatory compliance, business policies, retention management, and risk.
- Automated application of policies across tools and data estates.

8. Data Minimization & Retention Governance

Reduce data liability and cost with automated retention workflows. BigID identifies ROT (redundant, obsolete, trivial) data and enforces minimization based on risk, regulatory requirements, and business value.

Core data minimization requirements include:

- Retention policies to regulation, data type, and risk.
- Automated deletion workflows across source systems.
- Reduction of data sprawl and ROT (redundant, obsolete, trivial) data.

9. Privacy & Regulatory Compliance

BigID supports global privacy mandates like GDPR, CPRA, HIPAA, and more. With automated data mapping, DPIAs, RoPAs, consent tracking, and subject rights fulfillment, you can operationalize compliance at scale.

Core privacy requirements include:

- Data mapping and alignment with regulatory obligations (GDPR, CPRA, HIPAA, etc.).
- Privacy management including DPIAs, RoPAs, SARs, and consent tracking.

Critical Capabilities for a Modern DSP

Beyond individual tools, a data security platform must demonstrate:

Scalability: Operate across petabytes of data, thousands of sources, and dynamic environments.

- **Automation:** From classification to response, reduce manual effort through AI-driven automation.
- **Contextual Awareness:** Understand the business context, data lineage, ownership, and regulatory scope.
- **Extensibility:** Open APIs, modular design, and integrations with cloud, security, and data ecosystems.
- **Real-Time Intelligence:** Live insights into data risk, exposure, and policy violations.
- **Cloud-Native Compatibility:** Built for hybrid/multi-cloud, supporting containers, data lakes, SaaS, and more.
- **AI Governance:** Discover and secure AI training data, monitor for hallucinations and sensitive leakage.

BigID is differentiated by its ability to turn insights into action—with native enforcement, automation, and end-to-end coverage from discovery through remediation.

Outcomes That Matter

When fully realized, a Data Security Platform isn't just a set of tools—it's a **strategic force multiplier**. A best-in-class DSP doesn't just check boxes—it delivers measurable business value:

☑ Reduced Risk Exposure: Fewer breaches, fewer incidents, faster time to detect and respond.

☑ Operational Efficiency: Lower cost of compliance, minimized manual effort, automated workflows.

☑ Cloud Confidence: Accelerated cloud adoption with continuous visibility and control.

☑ Compliance at Scale: Meet regulatory mandates (GDPR, HIPAA, PCI, etc.) with defensible audit trails.

☑ Proactive Security Posture: Stay ahead of threats with real-time monitoring and prioritized remediation.

☑ AI Risk Mitigation: Secure training sets, monitor model inputs/outputs, and maintain explainability.

Final Word: Investing in What Comes Next

A Data Security Platform is not just a product—it's a strategy. It represents the unification of discovery, risk intelligence, and remediation into a single, scalable system.

BigID is redefining what a Data Security Platform can and should be. Unlike legacy DSPs stitched together from point solutions, BigID is:

- **Built for scale** across hybrid environments
- **Integrated by design**, not bolted-on
- **Actionable**, with controls tied to insight
- **AI-ready**, not AI-retrofitted

BigID uniquely delivers on this vision with a platform that combines security, privacy, and governance—turning risk visibility into real-world action.

To learn how to operationalize data security at scale—or see BigID in action—connect with our team today.

About BigID

BigID enables security, compliance, privacy, & AI data management for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining overnance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 4 consecutive years; the Deloitte 500 for 4 consecutive years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at https://bigid.com.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • AI Data Management

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

> **Tools like BigID are the future.**
> **Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.**
>
> IDC
> Ryan O'Leary
> Future of Trust: Battling Data Discovery Confusion