

# Teleskope vs BigID

## Overview

As organizations face increasing regulatory, privacy, and governance pressure, selecting a data security platform that delivers both visibility and operational impact is critical.

BigID is positioned as a broad data intelligence and governance platform, however, while BigID excels at breadth and audit readiness,

translating that coverage into continuous, day-to-day risk reduction requires approval-heavy workflows, professional services, and significant involvement from the customer.

[Teleskope](#) provides continuous, measurable reduction of data risk with significantly less operational effort.

## Why Teleskope

Governance-heavy DSPM tools, such as BigID, catalog and label data but rely on approval-heavy workflows to act. Teleskope reduces risk by intelligently enforcing your policies. Here is why it's different:



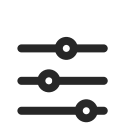
### Relevant, Prioritized Risk

- Finds risks across petabytes of any type of data 10X faster
- Prioritizes exposure that matters specifically to your business
- Enables high-confidence automation instead of manual triage



### Native, Automated Remediation

- Resolves risk directly instead of routing to tickets or external tools
- Mitigates existing exposure and new risk as it occurs
- Shortens time to risk reduction, not just time to insight



### Auditable, Intelligent Controls

- Enforces your existing policies and follows your workflows
- Humans stay involved where validation is required
- Actions are safe, auditable, and reversible

# How Telescope Compares to BigID

Telescope and BigID both address data risk, but from different starting points. BigID is built around broad data discovery and governance workflows; Telescope is built to continuously reduce risk through prioritization and automated policy

enforcement. The comparison below focuses on where those differences matter most: Risk Assessment & Prioritization, Risk Reduction & Policy Enforcement, Risk Prevention & AI Agents, Deployment, and Customer Support.

## RISK ASSESSMENT & PRIORITIZATION



**Highly accurate classification** (low false positive or negatives) that scales across structured and unstructured data of various formats, which enables high-confidence automation of risk reduction.

- Multi-stage AI pipeline: lightweight ML models route to specialized SLMs and LLMs, which combine contextual reasoning, semantic understanding, and business-specific policy signals
- Classifies a broad array of entity types (PII/PHI/PCI, credentials/secrets, custom data types)
- Classifies document types (e.g., IP, payroll, etc.) and provides redacted AI-generated summaries
- Differentiates dormant sensitive data from actively used or broadly accessed data, enabling prioritization
- Associates classified data with business relevance (e.g., customer vs employee data) to drive enforcement.



Customers obtain very broad classification inventories suited for **compliance** and **governance** initiatives, but struggle to operationalize results for continuous risk reduction due to workflow complexity and limited prioritization logic.

- Strong coverage across many data types and sources
- Classification primarily driven by regex and pattern matching
- Limited ML beyond out-of-the-box models (English and Spanish)
- Moderate noise levels that increase at scale
- Outputs optimized for reporting and labeling rather than enforcement
- Less precision around “what matters now” versus “what exists”

## RISK REDUCTION & POLICY ENFORCEMENT



Reduces risk **automatically** and **continuously**, without tickets, external tools, or manual follow-through, resulting in materially faster time to risk reduction and lower operational burden on security teams.

- Native actions: access revocation/scoping, sharing restriction, redaction/masking, encryption, cleanup of overexposed/stale sensitive data
- Embedded into existing workflows
- Works for existing exposure and in real time
- Supports full automation or human-in-the-loop based on risk and confidence



Remediation is **governance-driven** and **relatively slow**, making it suitable for compliance workflows but less effective for continuous, operational risk reduction.

- Remediation executed through governance applications (retention, deletion, labeling)
- Strong approval and review mechanisms before action
- Limited real-time or automated enforcement
- If-then posture violation model rather than dynamic prioritization
- Actions are often irreversible (e.g., deletion)
- Best suited for episodic compliance events rather than continuous operations

## RISK PREVENTION & AI AGENTS

Organizations can **safely adopt AI tools and agentic workflows** without increasing data exposure, because sensitive data is cleaned up in **real time** as it is used by AI systems.

- Detects and controls access to data at rest and in use by AI tools, copilots, and agents
- Prevents overexposed or non-compliant data from being used in AI workflows
- Enables AI adoption without requiring manual approvals or separate governance tools
- Supports continuous enforcement as AI usage evolves

Customers can document and govern AI-related data usage for compliance purposes, but **cannot enforce controls dynamically** as AI systems operate.

- Classifies and labels data intended for AI use
- Supports policy review and approval for AI datasets
- Limited real-time enforcement once AI workflows are live
- Human-driven governance over automated control
- Better suited for audit readiness than continuous AI risk reduction

## DEPLOYMENT



Deploys in hours to days across cloud, SaaS, and on-prem without agents, enabling faster time to value and consistent risk reduction across hybrid environments.

- Agentless, API-driven architecture across SaaS, cloud, and AI data flows
- Flexible deployment (SaaS or self-hosted) with on-prem scanning
- Single control plane across hybrid environments



Customers can deploy across a wide range of data sources, but often experience **longer** rollout cycles, higher dependency on services, and **inconsistent** time to value due to platform complexity.

- SaaS deployment only, no on-prem Connector-heavy, multi-module architecture
- Broad structured and unstructured data source coverage
- Multiple services components increase upgrade complexity
- Higher dependence on professional services for rollout and tuning
- QA and configuration overhead increases with scale

## CUSTOMER SUPPORT

Support model is tied to **business outcomes**: every engagement starts with the outcome alignment.

- Every customer is paired with a hands-on customer engineer who actively helps define use cases, configure policies, and drive outcomes.
- Customer work is structured around business objectives (e.g., insider threat reduction, IP protection, audit streamlining) and measured through POC discovery, kickoff plans, and quarterly outcome reviews.

Onboarding has a limited defined scope. After that, it requires additional **billable** services or third-party partners, and ongoing support is largely break/fix.

- Support model is tightly coupled with professional services
- Significant time spent on tuning, suppression, and alert management
- Ongoing changes (new data stores, new users, new permissions) frequently require renewed engagement
- Supports troubleshooting, but ownership of outcomes remains with the customer