teleskope

Teleskope vs Cyera

Overview

As organizations accelerate cloud adoption and AI initiatives, selecting a data security platform that moves beyond visibility to sustained risk reduction is critical.

Cyera delivers fast, clean visibility into sensitive data in cloud-first environments. However, remediation and enforcement are not core to the platform and typically require integrations or manual workflows.

Teleskope provides continuous, measurable reduction of data risk with significantly less operational effort, even as data usage, sharing, and AI adoption accelerate.

Why Teleskope

DSPM tools, such as Cyera, show you posture but rely on customers and integrations to resolve risk. 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 Teleskope Compares to Cyera

Teleskope and Cyera both address data risk, but from different starting points. Cyera is built around visibility; Teleskope 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

teleskope

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.

CYERA

Fast, relatively low-noise visibility into sensitive data across cloud environments, but **classification is primarily optimized for discovery** rather than enforcement. As a result, findings require additional interpretation before action can be confidently automated.

- Cloud-native, agentless architecture optimized for SaaS API scanning
- Sampling-based scanning approach to accelerate time to insight, which however may lead to false negatives
- Machine learning combined with metadata analysis for classification
- Lower false positives compared to legacy, regex-heavy DSPM tools, however true positives may be irrelevant to the business
- Limited built-in prioritization based on business criticality
- Classification outputs primarily feed dashboards and external workflows

RISK REDUCTION & POLICY ENFORCEMENT

teleskope

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.

- Robust library of 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

CYERA

Remediation is largely dependent on **integrations** and **customer-built workflows**, which can delay consistent risk reduction after discovery.

- Limited native remediation actions
- Most enforcement executed through external orchestration tools (e.g., SOAR, Tines)
- Integrations require custom logic, scripting, and ongoing maintenance
- Revocation and access changes limited to supported cloud permissions
- No deeply embedded, policy-driven automation

RISK PREVENTION & AI AGENTS

teleskope

Organizations can safely adopt AI tools and agentic workflows because sensitive data is automatically controlled and cleaned up as it is accessed and used.

- 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

CYERA

Customers receive visibility into AI-related data exposure and AI readiness posture, but **enforcement of AI data usage policies relies on external workflows** rather than native, real-time control.

- Identifies sensitive data that may be accessed by AI systems
- Provides AI posture dashboards and reporting
- No native, in-platform control of AI prompt or response behavior
- Remediation of AI-related exposure handled via integrations

DEPLOYMENT

teleskope

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

CYERA

Customers benefit from rapid onboarding and quick time to insight in cloud-first environments, but **hybrid or on-prem expansion can introduce additional architectural complexity**.

- Agentless, SaaS-first architecture leveraging cloud APIs
- Rapid deployment in supported cloud and SaaS environments
- Minimal infrastructure footprint for initial rollout
- On-prem environments require additional components (e.g., outposts)
- Architecture optimized for fast discovery rather than hybrid depth
- Expansion into complex enterprises may require phased deployment

CUSTOMER SUPPORT

teleskope

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.

CYERA

Customers receive onboarding support, but long-term operational success often depends on the **customer's ability to build and maintain remediation workflows independently**.

- High-touch engagement during proof of value
- Focus on accelerating time to initial discovery
- Less structured outcome-driven engagement post-deployment
- Assumes customers operationalize insights via integrations
- Remediation workflows typically customer-built or partner-led
- Support model more reactive than continuous partnership