teleskope

Teleskope + Purview:
Better Together

Overview

Microsoft Purview provides foundational compliance tooling tightly integrated with the Microsoft ecosystem. However, organizations operating beyond Azure or Microsoft 365 often find themselves constrained by Purview's limited flexibility and generalized classification approach.

Teleskope provides continuous, measurable reduction of data risk with significantly less operational effort.
Together, they transform labeling into enforcement and posture into measurable risk reduction.

Why Teleskope

Data Security and Governance tools, such as Purview, classify and label data but produce millions of false positives, leaving security teams without a path to operationalize risk reduction.
Teleskope reduces risk automatically by 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 Makes Microsoft Purview Operational

Microsoft Purview delivers powerful data protection capabilities across Information Protection, DLP, Insider Risk, Records Management, and eDiscovery. For many enterprises, it is deeply embedded within Microsoft E5 and central to security strategy.

However, customers consistently report operational challenges:

- ⚠ Built-in classifiers are regex based and produce millions of false positives
- ⚠ Custom classifiers are difficult to build and maintain
- ⚠ Labeling requires extensive tuning
- ⚠ Retention and disposition workflows are difficult to automate at scale
- ⚠ Automation across third-party systems is limited

CLASSIFICATION

⊗ Without Teleskope

- Long and tedious production integration process and no autodiscovery, even for Azure
- Custom SITs, EDM, and trainable classifiers require extensive setup and ongoing tuning
- Built-in classifiers are regex based and produce inconsistent precision at scale
- Limited to files under 20MB
- Millions of labeled files still require manual validation
- Low confidence in accuracy limits automated enforcement.

Classification becomes a maintenance burden rather than a scalable control.

✓ With Teleskope

- AI-driven, context-aware scanning across millions of files in hours, not weeks
- Understands what data represents (contracts, IP, HR records), not just patterns
- Business-level categorization via advanced ML
- Higher precision enables confident automation
- Prioritizes what matters instead of surfacing raw volume

Classification becomes actionable and trusted.

LABELING

Without Teleskope

- MIP labels are based on regex classifier and are generic and inaccurate
- Inconsistent labeling across large data estates
- Manual oversight required to maintain confidence
- Silent declassification risks remain
- Enforcement policies limited by trust in metadata

Labels exist, but enforcement is constrained.

With Teleskope

- Automatically applies and updates MIP labels with high-confidence detection
- Labels travel with documents across Microsoft and third-party systems
- Activates DLP, SASE, and CASB controls immediately
- Detects and alerts on unauthorized classification changes
- Turns labeling into a dynamic enforcement signal

Labels become operational and reliable.

REMEDIATION

- Purview alerts flow into SIEM and SOAR workflows; only specific actions are supported (vs an entire workflow)
- Remediation depends on tickets, scripts, and analyst capacity
- No interactive / UX based remediation interfaces; users can’t find what’s flagged
- Reducing exposure across millions of files takes months
- Retention and disposition processes are approval-heavy

Risk visibility improves, but reduction lags.

- Automatically enforces policy in real time
- Revokes access, restricts sharing, and cleans up exposure continuously
- Supports scalable retention automation
- Reduces material exposure without proportional headcount growth
- Shifts from reactive alerts to measurable risk reduction

Risk reduction becomes continuous, not episodic.