komprise

Solution Brief

Protect Sensitive Unstructured Data with Komprise

Komprise Smart Data Workflow Manager helps IT quickly find and remove sensitive data from non-compliant locations.

In enterprise IT, security is now everyone's responsibility. Storage IT professionals need to ensure that sensitive data — such as PII and IP—are protected from unauthorized access and unavailable for ingestion into AI. However, as unstructured data has exploded across many different silos in the enterprise, the task has become increasingly difficult and impossible to do manually.

The risks are irrefutable: attempts to input PII into GenAI platforms represent over half (55%) of data loss prevention (DLP) events, according to research by Menlo Security. Roughly 80% of data breaches involve sensitive data, according to Verizon's Data Breach Investigations report and other sources.

Komprise Smart Data Workflow Manager, a simple interface for configuring and automating the discovery, tagging and classification, and movement of data between different storage platforms, includes built-in scanners for PII and other sensitive data.

Find Sensitive Data Across Hybrid Storage Silos

Komprise can search within file contents across all storage, for specific information. Our standard PII detection covers national IDs, credit card numbers and email addresses. You can also conduct custom searches using keyword and regular expressions (regex) search to identify specific data formats like employee IDs, machine or instrument IDs, product or project codes, or PHI data like patient record IDs. Komprise processes all data locally in your own data center, so sensitive data stays in place.

Key Benefits of Komprise Sensitive Data Management

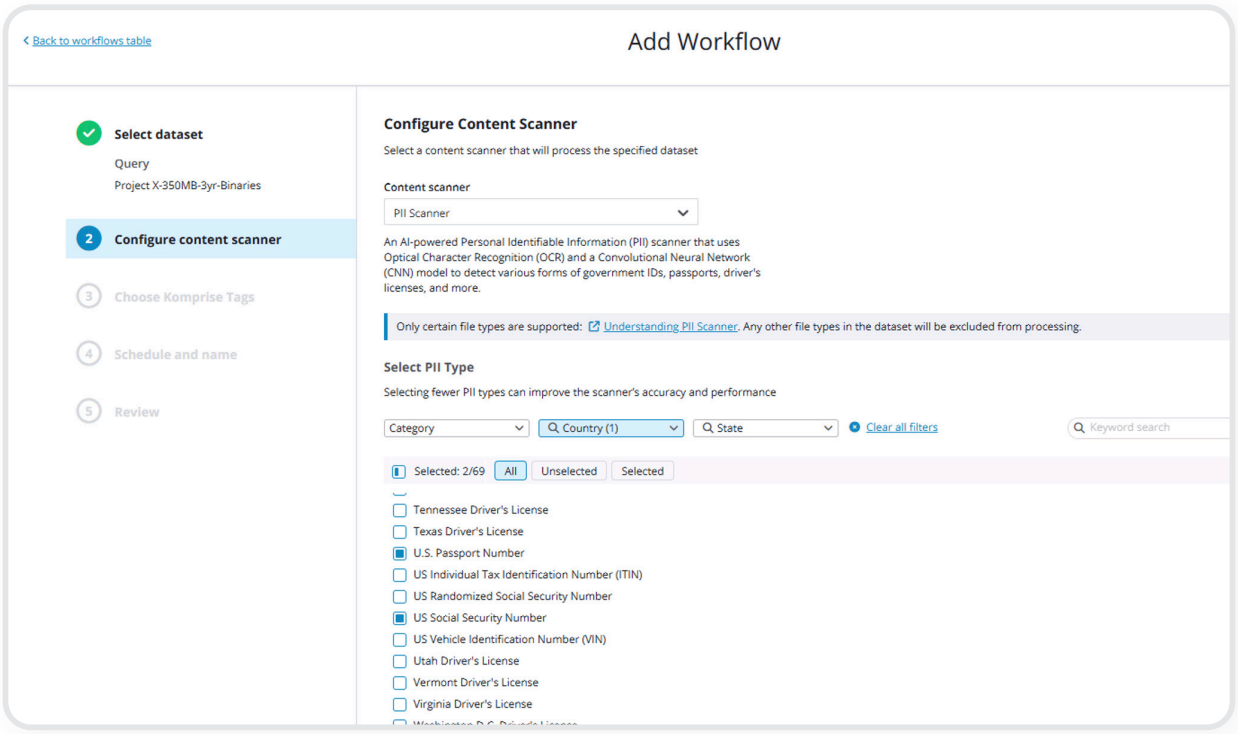
- Supports both standard PII detection and custom sensitive data detection;
- Scans sensitive data in place so that data doesn't leave your data center;
- Tag and move sensitive data to a safe location;
- Set up continuous, automated workflows to find and move sensitive data;
- Support safe AI use in your organization by eliminating sensitive data leakage;
- Obtain full auditing for data workflows to monitor data governance and security.

Tag, Move and Remediate Sensitive Data

Once Komprise detects sensitive data, it is automatically tagged in our metadatabase: the **Komprise Global File Index**. Data classification brings context and structure to unstructured data without any modification to the original data. Next, you can set policies to act on what you find and automate ongoing workflows to ensure that no sensitive data is left behind. You may choose to confine the data for review and/or move data to a safe location.

Exclude Data and Audit Workflows for AI

Data governance for AI is a top enterprise priority. You can set up automated workflows in Komprise to identify and exclude sensitive data from the data copied to AI. Komprise automatically finds and acts on any new sensitive data for ongoing detection, tagging and mitigation. The solution maintains a full audit record of all data processed by any workflow, so that IT can investigate any issues or concerns that may arise on AI outcomes.



Learn More

Komprise Smart Data Workflows and the sensitive data detection and regex search are included in the Intelligent Data Management platform. Visit **komprise.com/whatsnew** to learn more.

Komprise, Inc.
1901 S. Bascom Ave. Suite 500
Campbell, CA 95008
United States

For more information:
Call: 1-888-995-0290
Email: **info@komprise.com**
Visit: **komprise.com**

For media requests email
marketing@komprise.com