secuvyai

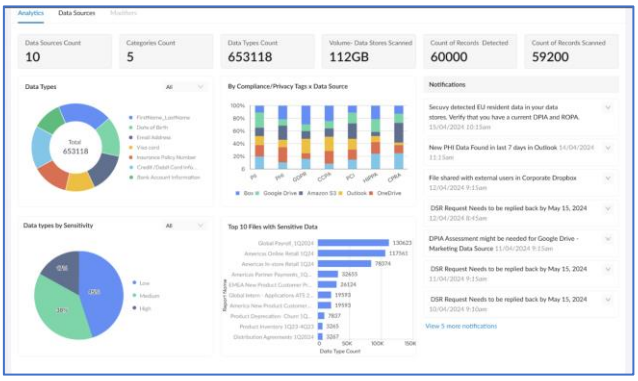
Automate Security, Privacy & Compliance for GenAI Products

Data Governance & Security for Trustworthy AI Systems

Secuvy.ai is at the forefront of data security, using cutting-edge machine learning to enable usage and design of trustworthy AI products. Our platform helps you protect and secure enterprise data for GenAI use cases.

Discover, Inventory, Classify AI Models

- **AI Data Inventory:** Quickly locate and manage sensitive data within your AWS environment using Secuvy's automated discovery tools.
- **Automated Data Classifications:** Gain comprehensive visibility into the data types available for AI model training.
- **Single Pane of Data Views:** Access a unified interface for unstructured, structured, and semi-structured datasets, providing richer context.
- **Central Repository:** Store all model metadata, documentation, and artifacts in one central location.



Data Sources Count	Categories Count	Data Types Count	Volume- Data Stores Scanned	Count of Records Detected	Count of Records Scanned
10	5	653118	112GB	60000	59200

Notifications

Secuvy detected EU resident data in your data stores. Verify that you have a current DPIA and ROPA. 15/04/2024 10:15am

New PHI Data Found in last 7 days in Outlook 14/04/2024 11:15am

File shared with external users in Corporate Dropbox 12/04/2024 9:15am

DSR Request Needs to be replied back by May 15, 2024 12/04/2024 8:45am

DPIA Assessment might be needed for Google Drive - Marketing Data Source 11/04/2024 9:15am

DSR Request Needs to be replied back by May 15, 2024 11/04/2024 9:15am

DSR Request Needs to be replied back by May 15, 2024 10/04/2024 9:10am

View 5 more notifications

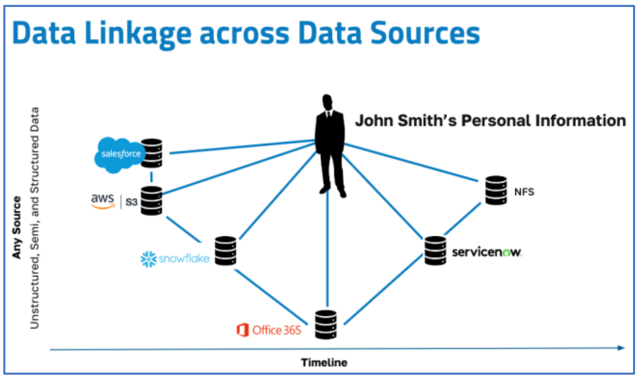
Ensuring Robust AI Security

- **Data Categorization:** Enhance security measures by effectively categorizing underlying data to prevent breaches and misuse.
- **Enhanced Privacy:** Anonymize personal and sensitive data to improve security posture.
- **Policy-Driven Alerts:** Create actionable policies to receive alerts on privacy, security, and operational violations, boosting overall AI security.

Data Linkage and Associations

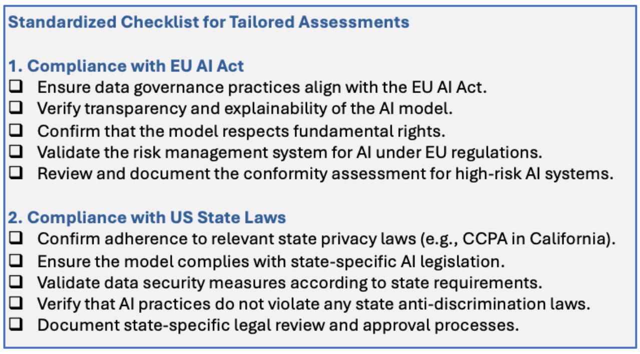
Secuvy's linkage graph offers detailed tracking and accountability of your data's origin and journey, supporting effective governance. Our data mapping offers:

- **Data Observability:** Identify Sensitive Data Category Sprawl across sources.
- **Mask/Delink/Obfuscate:** Data Scrubbing workflows to securely erase sensitive data


Data Linkage across Data Sources
John Smith's Personal Information
salesforce
aws | S3
NFS
snowflake
servicenow
Office 365
Any Source
Unstructured, Semi, and Structured Data
Timeline

Ensuring Compliance and Fairness

- **Tailored Assessments:** Utilize standardized checklists to ensure models are release-ready, complying with EU AI Act, AI RMF, ISO 42001, and other regulations.
- **Model Certification:** Validate models through essential process gates, including legal reviews, explainable AI validation, and assessments for ethics, bias, and fairness.



Standardized Checklist for Tailored Assessments

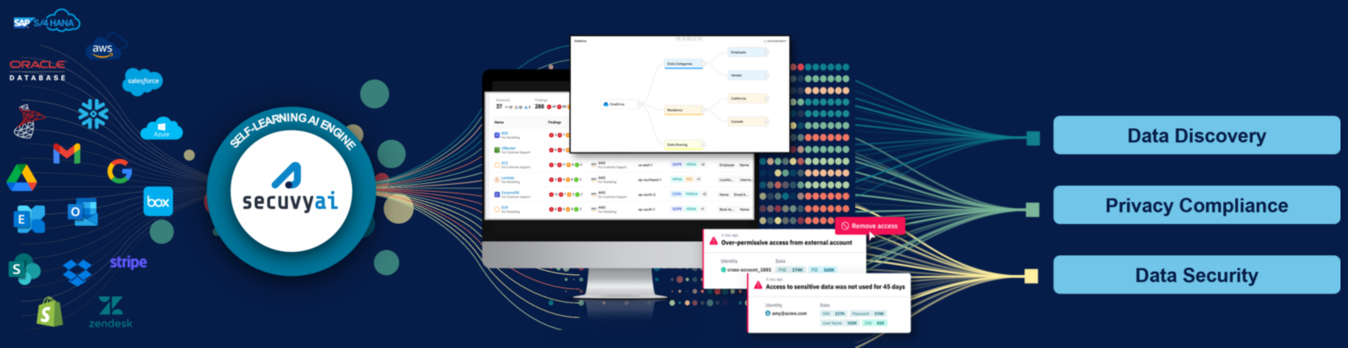
1. Compliance with EU AI Act

□ Ensure data governance practices align with the EU AI Act.
□ Verify transparency and explainability of the AI model.
□ Confirm that the model respects fundamental rights.
□ Validate the risk management system for AI under EU regulations.
□ Review and document the conformity assessment for high-risk AI systems.

2. Compliance with US State Laws

□ Confirm adherence to relevant state privacy laws (e.g., CCPA in California).
□ Ensure the model complies with state-specific AI legislation.
□ Validate data security measures according to state requirements.
□ Verify that AI practices do not violate any state anti-discrimination laws.
□ Document state-specific legal review and approval processes.

The Secuvy Solution



Data Discovery

Privacy Compliance

Data Security

Connect

- API Driven
- SaaS | Databases | Email | File Shares
- Structured | Unstructured

Discover **Classify**

Self-Learning AI Enabled Discovery

- Autonomous operations
- Learns continuously
- Multi-phase classification

Protect **Comply**

Continuous Compliance

- Data Graph for Mappings and Linkages
- Automation of PIAs, ROPAs, DSRs
- Greatly improved accuracy with fewer touchpoints

Why Secuvy

- **Unsupervised Machine Learning** streamlines data discovery and classification without the need for extensive data labeling and training.
- **Unified Platform** for AI governance, security, and privacy compliance, enabling both offensive (AI applications) and defensive (data protection) strategies.
- **A policy engine** for immediate implementation of new global privacy laws, ensuring timely compliance.
- **Integrate** with CrowdStrike, Zscaler, and Netskope, improving overall data security and privacy.
- **Automates** processes using policy and business rules engines, reducing manual intervention and increasing operational efficiency.
- **Near Perfect Accuracy** in identifying and classifying unstructured and semi-structured data, which reduces errors, false alerts and effective controls for data management.

Explore More Resources

Large Language Models (LLMs), Data Privacy and Security: What you Need to Know

Read Blog

Data Security – The Other side of Data Privacy

Read Blog

Distinguishing Data Governance, Security, and Privacy

Read Blog

About Secuvy

Secuvy makes data protection easy, efficient, and trusted with a next-generation privacy, data security, and AI data governance platform. The self-learning AI automates the inventory of any type of data, in any format, in any environment, at record speed and highest accuracy in the market. The era of AI governance is here.

Book your demo with our data privacy experts today

secuvy.ai/demo/

For more information, contact us at info@secuvy.com