Secuvy AI Data Governance

In the ever-changing world of digital innovation, artificial intelligence (AI) has rapidly become a critical driver of growth and efficiency for modern businesses. However, as companies increasingly rely on AI, there's an urgent need for effective data governance strategies that prioritize compliance, security, and the ethical handling of information.

Secuvy is leading the charge in this area by offering an all-encompassing AI Data Governance solution. This solution is designed to help organizations manage their data with precision, safeguard it with cutting-edge security technologies, and ensure seamless compliance with international regulations.

The Need for AI Data Governance

AI Data Governance is crucial in today's landscape, especially when dealing with large language models (LLMs).

- Data isolation with LLMs is challenging.
- Sensitive information may be exposed to unauthorized users or LLMs.
- API keys and similar secrets are at risk of being leaked.
- Prompts can inadvertently expose methods for collecting sensitive data.
- Data sprawls in unstructured formats are difficult to manage.
- LLMs are prone to model failures, impacting reliability.
- External data inputs can alter application behavior, especially with RAG/Plugins.
- Outputs can easily leak data through plugins, RAG, or logs.
- Existing guardrails are supplementary, often ineffective, and limited in scope.

The Challenges of AI Data Governance

- Exposure from the rise of mix mode data sprawls across multiple environments.
- Incomplete data visibility, classification and linkage.
- Lack of tools for data associations.
- Absence of data observability based on data context and data drift.
- Synchronizing data in motion with data at rest.
- Leveraging a unified single platform for data intelligence.

Secuvy's Approach to AI Data Governance

Unified Data Intelligence Platform:

Secuvy's platform integrates data governance, security, and compliance into a single, cohesive system. Key features include:

Comprehensive Model Inventory:

- Maintain a detailed inventory of all AI models with associated risk profiles.
- Use these profiles to create Model Cards that fulfill compliance requirements and demonstrate AI readiness.

Personal Data Scrubbing:

- Automatically identify and remove linked or referenced Personally Identifiable Information (PII) and sensitive data.
- Customize the scrubbing process based on criteria like data subject types, residency, consent, and retention policies.
- Ensure compliance with global data protection regulations.

Automated Data Discovery and Classification:

Secuvy's AI-powered tools streamline data governance with automated processes:

Efficient Data Management:

- Automatically identify, categorize, and manage sensitive data across your organization.
- Save time and enhance the accuracy of data governance efforts.

User Identity Anonymization:

- Delink user identities across multiple data sources with a single click.
- Protect privacy and reduce the risk of re-identification.

Custom Policy Definition:

- Implement custom policies for each AI model to minimize bias and improve fairness.

Fairness and Bias Metrics:

- Establish and monitor Quality of Service (QoS) metrics to measure and improve fairness and bias in AI systems.

Seamless Integration:

Secuvy's solution integrates effortlessly with existing AI and data infrastructures, providing:

Easy Compatibility:

- Works seamlessly with major cloud services and collaboration platforms.
- Implement governance measures without disrupting current operations.

Data Minimization Strategies:

- Optimize training datasets to reduce storage costs, improve training times, and enhance model quality.
- Use clean, minimized input data to boost AI efficiency and accuracy.

Key Benefits of Secuvy's AI Data Governance

Enhanced Compliance and Risk Management:

- **Model Card Compliance:** By maintaining a comprehensive inventory of AI models with associated risk profiles, Secuvy ensures that your organization meets compliance requirements with ease.
- **Personal Data Protection**: Automated scrubbing of PII and sensitive data ensures compliance with global data protection regulations, reducing the risk of fines and legal complications.

Increased Data Privacy and Security:

- **User Identity Anonymization:** The ability to delink user identities across data sources protects individual privacy and minimizes the risk of data breaches.
- **Custom Policy Implementation:** Define and enforce policies that reduce bias and promote fairness, ensuring ethical AI practices that build trust with stakeholders.

Operational Efficiency and Cost Reduction:

- **Automated Data Management:** Save time and resources by leveraging AI to automatically discover, classify, and manage sensitive data, reducing the manual workload for your teams.
- **Data Minimization:** Optimize your training datasets to decrease storage costs, accelerate training times, and improve the overall quality of AI models, leading to better business outcomes.

Improved AI Model Quality and Fairness:

- **QoS Metrics for Fairness:** Monitor and improve the fairness and bias of AI models with QoS metrics, ensuring that your AI systems produce equitable outcomes and maintain ethical standards.
- **Clean Input Data:** By minimizing and cleansing training data, Secuvy enhances model accuracy and efficiency, leading to more reliable and effective AI solutions.

Seamless Integration and Flexibility:

- **Effortless Integration:** Implement robust governance measures without disrupting your existing AI and data infrastructures, thanks to Secuvy's seamless compatibility with major cloud services and collaboration platforms.
- **Scalable Solutions:** Whether your organization is large or small, Secuvy's platform scales to meet your specific governance needs, allowing for flexible and customizable data management.

Next steps

Today, companies cannot afford to neglect developing a data governance strategy. If they truly wish to utilize their data with confidence then implementing AI data governance will allow them to leverage accurate, reliable, and secure data. Good data governance practices and data stewardship can foster a culture of trust in data and enable faster decision-making and unlock new opportunities for growth.

Contact us today for a Demo of Secuvy's AI Data Governance solution

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.