secuvyai

Prevent data leakage by aligning security policies between data at rest and data in motion

The Use Case

Creating and executing effective DLP/CASB policies between data at rest and data in motion is hard. The inability to detect data elements, imprecise scoping, and lack of context about authorized users can lead to both false positives and false negatives. This lowers confidence in ability of the solution to prevent data leakage.

How Secuvy Can Help

Secuvy's AI-driven technology integrates with and analyses your CASB/DLP solution to detect gaps in critical data elements, identify potentially misconfigured DLP/CASB policies, and orchestrate actions to remediate. When integrated with cloud-native security platforms, Secuvy improves DLP and CASB effectiveness by quickly adapting to data environment changes and consistently applying security policies. Secuvy can:

- Automatically detect and resolve classification gaps, ensuring continuous security enforcement.
- Update DLP policies and API protection by reading file classifications, detecting errors, and initiating automatic remediation.
- Reduce manual intervention by integrating with Netskope, providing precise data classifications that enhance DLP accuracy and compliance.

This is especially beneficial for industries like Defense, Critical Infrastructure, Pharma, Life Sciences, Healthcare, and Technology, where data security is crucial.

Contact us to learn how Secuvy can help prevent data leakage by aligning security policies between data at rest and data in motion.

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.