Riscosity

Modern LLM Governance

Always Know What, When, And Where Data Is Being Sent

Riscosity is the data flow security platform built to equip teams with the tools needed to maintain full visibility of data in transit and to remediate any risks before they reach a 3rd party. Within seconds, teams get continuous and accurate visibility into where data is going and can redact or redirect sensitive data, simplifying how they meet security and privacy requirements.

How It Works

Deploy Riscosity's zero-agent solution seamlessly in your existing technology stack. Riscosity combines code scanning, network scanning, and DNS scanning to detect, classify, and secure network traffic bound for LLMs and AI tools.

LLM Cataloging

Build an accurate catalog of all LLM endpoints that are operating in your environment and being referenced by your software code base.

In-Transit Data Guardrails

Map LLM endpoints and the information shared with them within minutes in order to restrict flows as per business and model quality needs.

Data Posture Management

Continuously monitor and block API data transfer to LLMs to ensure that only quality data is used for model creation, training.

In-Flight Data Redaction

Automatically replace detected sensitive data, tuned to your business logic, with redacted inputs.

Benefits

- **Automatically Identify LLM Endpoints** - Programmatically detect which LLM endpoints (IP, DNS) data is being shared with.
- **Training Data Attestation** - Implement custom rules to send alerts if low-quality training data is being sent for model creation.
- **Prevent Accidental Non-Compliance** - Adhere to the contractually agreed upon SCCs and automatically redact sensitive data before it's sent to LLMs.
- **Automate Record-Keeping** - Use Books by Riscosity to demonstrate thqat up-to-date and accurate evidence-collection processes are in place when training LLMs to meet compliance requirements.

Get Started with Riscosity

Riscosity enables security and compliance for any 3rd party data in transit, including traffic to AI tools. Visit **www.Riscosity.com** to learn more.