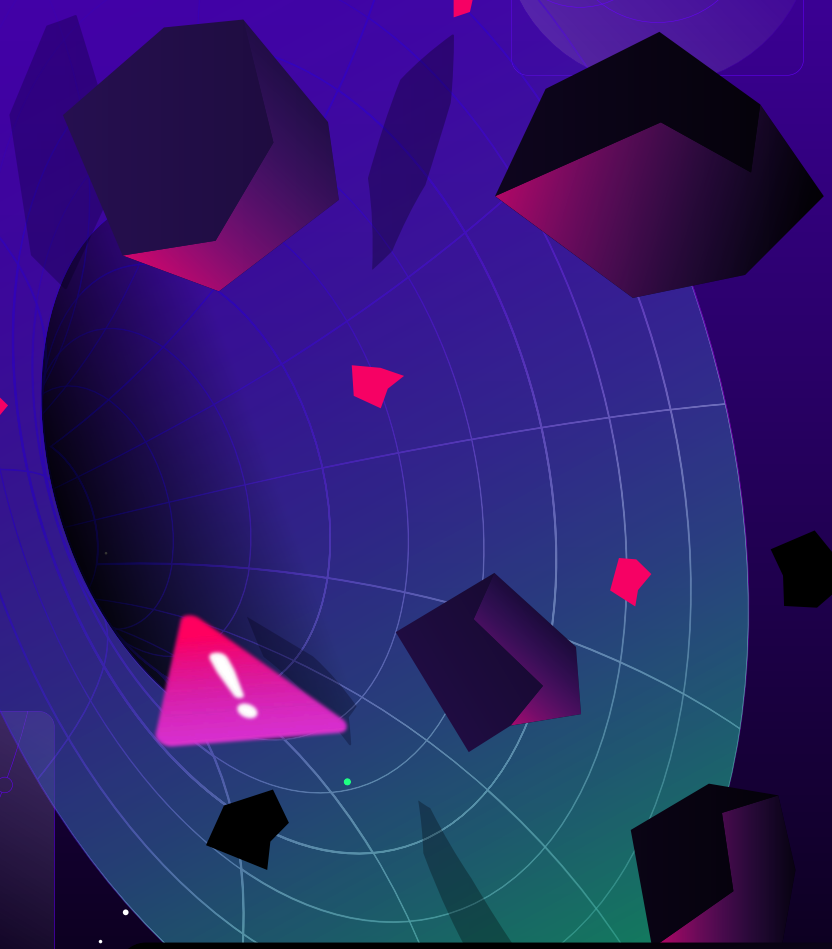
CYERA

Securing Generative AI

Did you know that nearly **35% of data** being input into AI tools is sensitive?

AI is only as secure, compliant, and ethical as the data that powers it.



The Unseen Challenges of Generative AI

Generative AI tools carry hidden risks of data loss. Information can leak through prompts, outputs, or chatbot interactions, without users even realizing it.

A staggering 71% of AI tools fall into the "high or critical risk" categories. Inaccurate AI responses have already caused issues for organizations, emphasizing the need for strict validation and oversight. Unintentional internal policy violations, such as oversharing or misuse, is responsible for data leaks, making it clear that strong governance is essential.

Why a Data-Led Approach Matters

Cyera's data-led approach is essential to managing the risks and responsibilities of generative AI.

It starts with visibility:
knowing what data you have, where it resides, who can access it, and how it's being used.
With that insight, you can establish control by applying consistent policies that protect sensitive data wherever it flows.

Check out the entire guide to Securing GenAI Adoption here!