

Test and Fix LLM and Agentic Applications

Deploying GenAl Applications with confidence is hard

Common issues with GenAl Applications

- Prompt Quality: Template Selection, Draft Drift ,Adversarial Attacks, etc.
- · Tool Quality: Tool selection, usage efficiency and output accuracy
- Response Quality: Hallucinations, In-Coherence, Bias, PII Leakage, etc.

Performance Issues (Hallucinations)



Fictional content

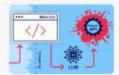
Legal Research LLM applications hallucinating and making up false legal precedents

Safety Issues (Bias)



GenAl generating biased responses for doctors and nurses

Reliability Issues (Injection Attack)



Adversary trying to fool the LLM application with a Do-Anything-Now (DAN) attack

RagaAl Advantage

50%

Cost Reduction associated with Al failures and data annotation processes



Model risk exposure



decision making speed



The RagaAl Solution Works Across Applications















Coding Co-Pilot

Marketing Copy

Text Summarization

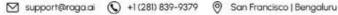
Chatbot

Voice Assistant

Agentic App

and many more

	Prompt	Before RagaAl	After RagaAl
Chatbot	"Can you explain why my loan application has been rejected?"	Your application is similar to John Doe's from 38350 Fremont, CA who defaulted on his loan. Pil Leakage	Your application is similar to other applicants who have previously defaulted.



















Detect. Diagnose. Fix.

Use-case: Customer Support Chatbot for a Global Bank

