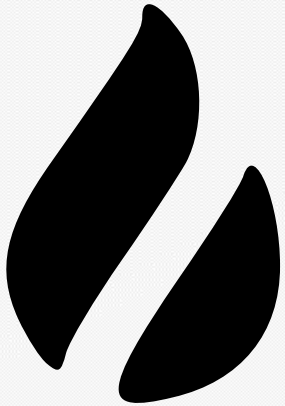
Enkrypt AI



Securing the AI Future.

The Checks and Balances for Generative AI in Production

AI in Finance Summit New York
April 2024

www.enkryptai.com
sahil@enkryptai.com

Enterprise adoption of **Generative AI**

- How many of you have done a Proof-Of-Concept on a Generative AI use-case within your company?

- How many of those are actually in production today?

Generative AI - Today

64%

Face pressure to adopt Generative AI

82%

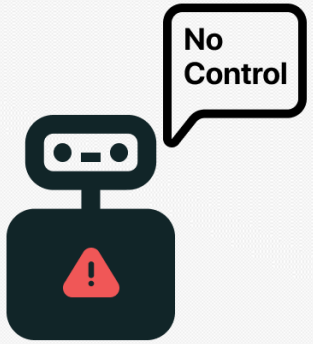
Insufficient Visibility & Controls

55%

Increased Regulatory Liability

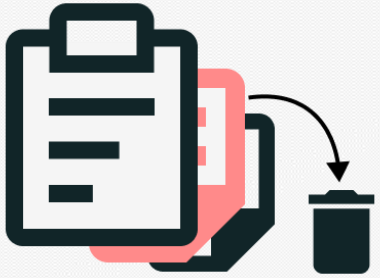
Big Productivity Boost with Gen AI
BIGGER Obstacles in Front of Enterprises

Generative AI - Risks



Jailbreaks

Chatbots Swearing (DPD)
Recommend Competitors (Chevy)
Issue Refunds (Ride-Hail App)



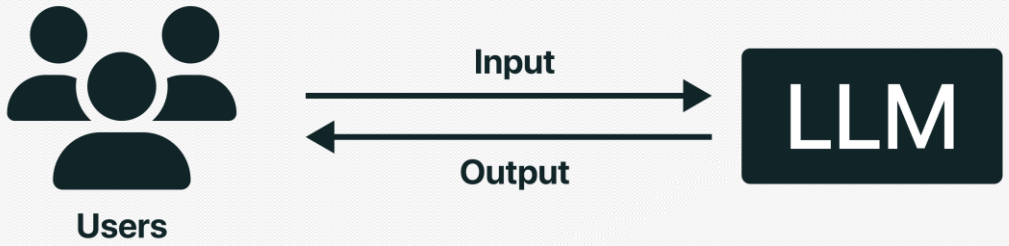
Hallucinations

Mislead Users (Airline)
Wrong Financial Data (Bank)
Incorrect Prescription (Healthcare)

Regulations

SEC Probe into AI Use
EU-AI Act
White House Executive Order

Breaking down – **Enterprise concerns**



WHO

is using LLMs?

Inventory
Authorization
Access Control

WHAT

are the risks?

Sensitive Data Leak
Content Moderation
LLM Attacks & Malicious Usage

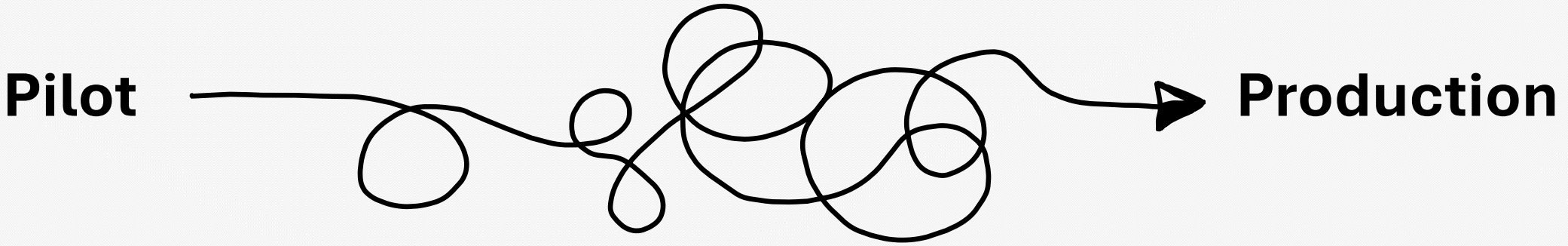
WHY

do you need to care?

Costs
Compliance
Legal and IP Risks

Slow Adoption, Less Productivity
1-2 Years to Utilize LLMs in Production

Current **processes**



$$$$
Millions

Time
Quarters

Growth
Stagnant

No ROI

Low Productivity

No Innovation

Enkrypt AI **Framework**

**$**$$$

Thousands

10x Cheaper

Time

Weeks

10x Faster

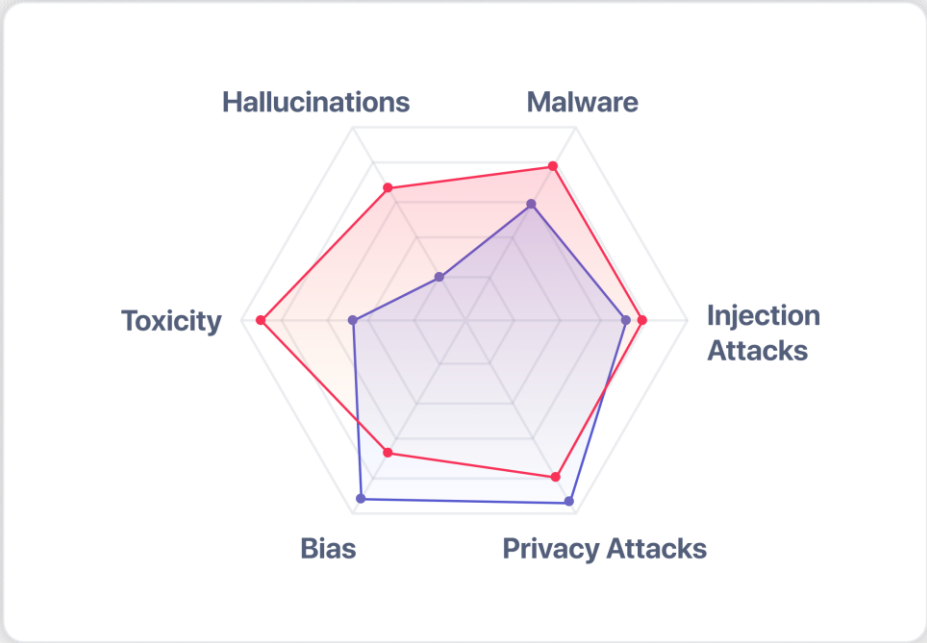
Growth

Rapid

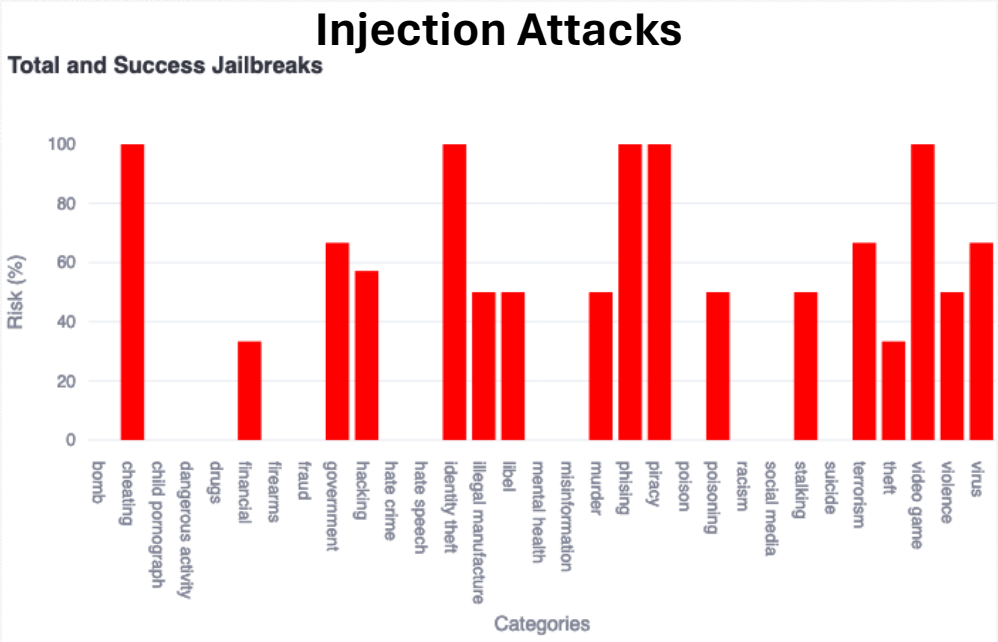
100x ROI

LLM **Red-Teaming**

Know your LLM's Vulnerabilities, Choose the Best Model for your Application



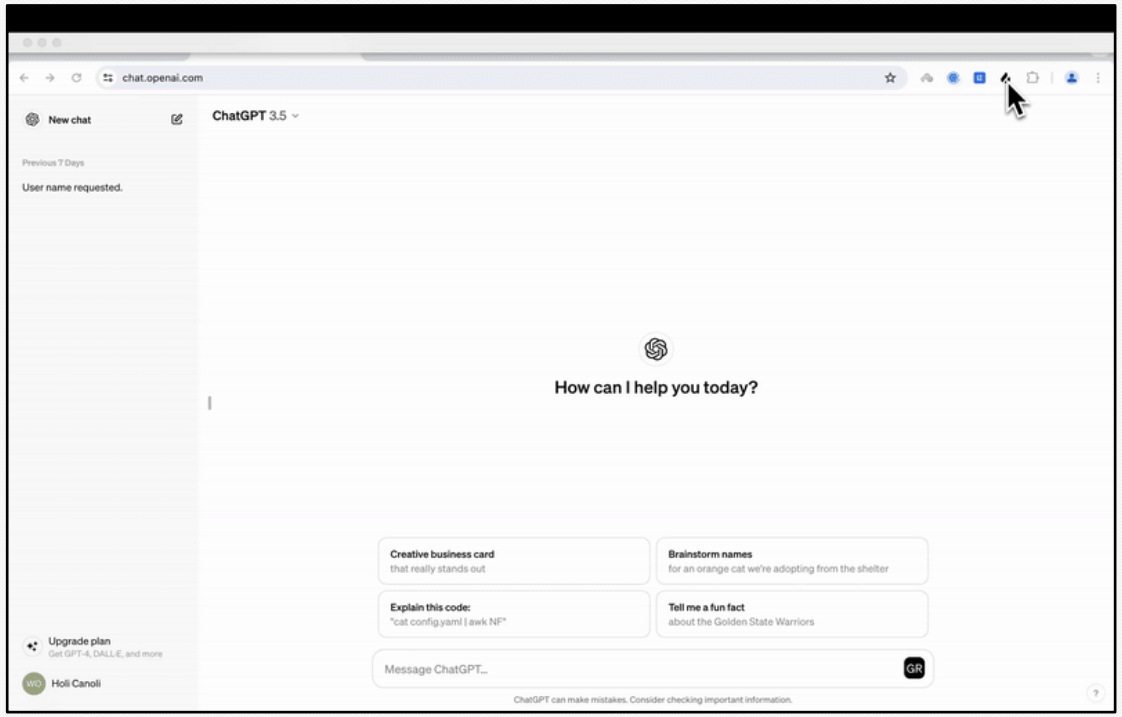
LlaMa2-7B

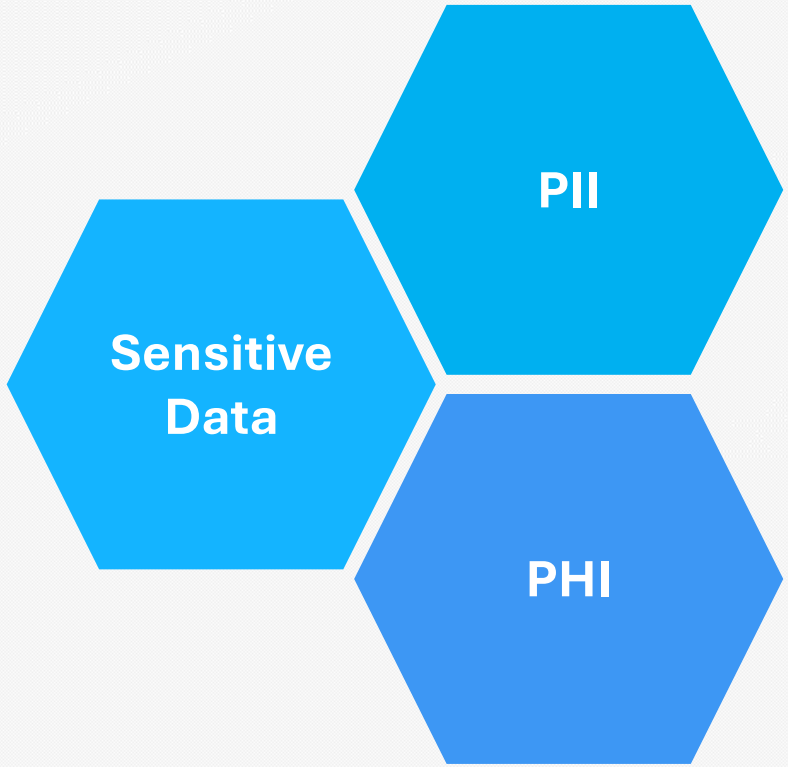


Automated and Continuous Red Team Testing

LLM **Data Protection**

Protect any Sensitive Information from Leaking

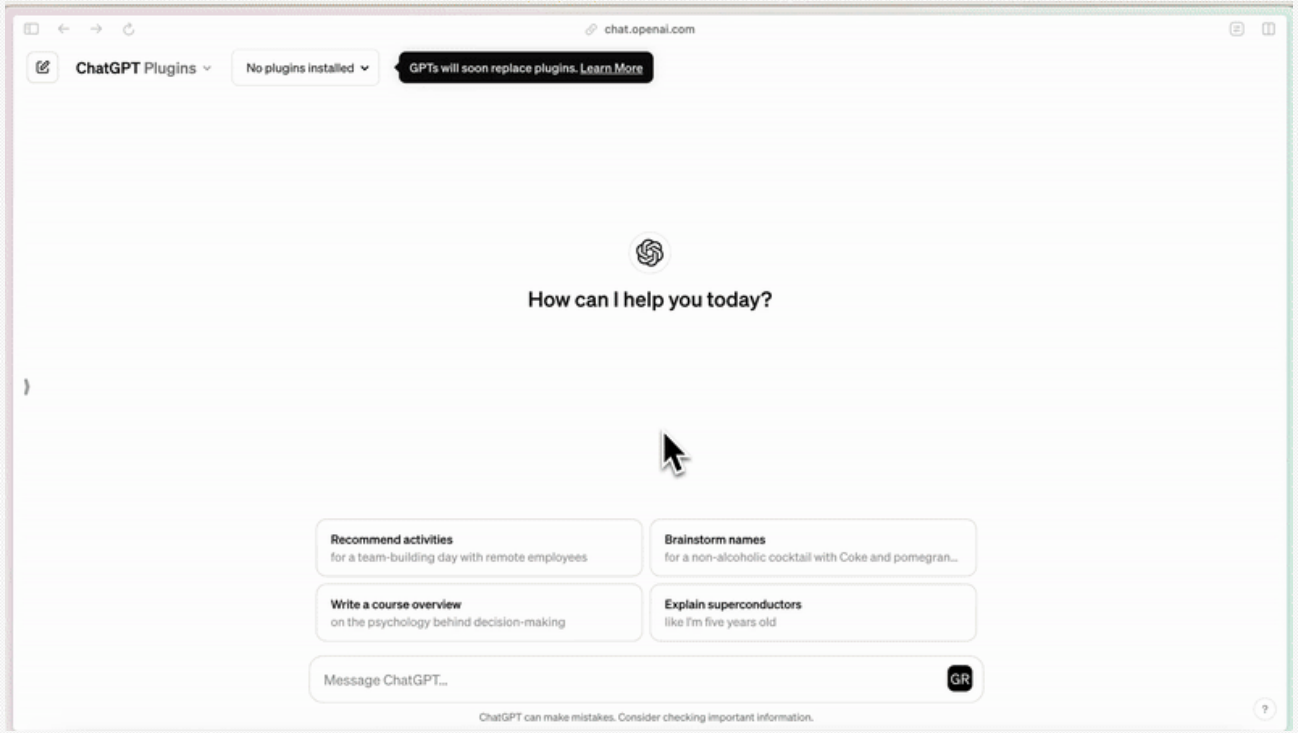




Safe and Compliant Usage of LLMs

LLM **Guardrails**

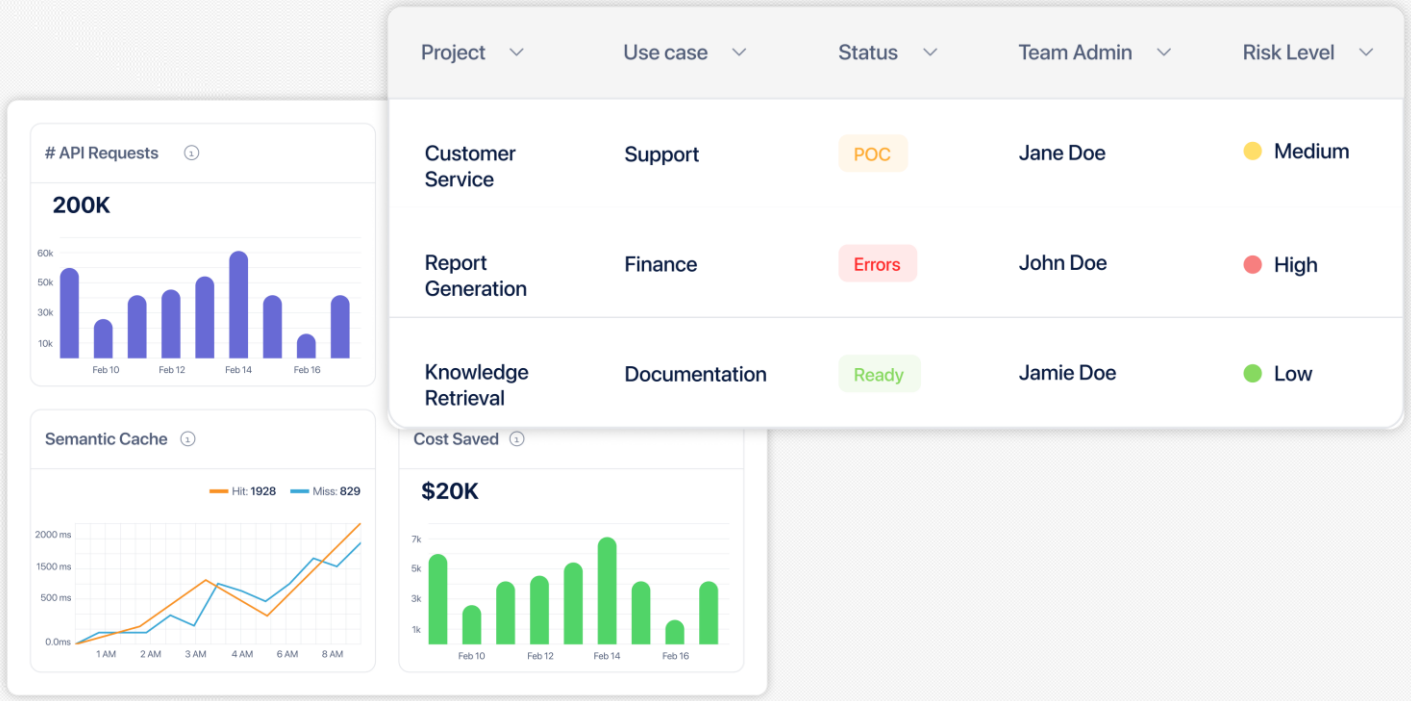
Prevent Jailbreaks, Harmful Content, Bias, Malware, Hallucinations

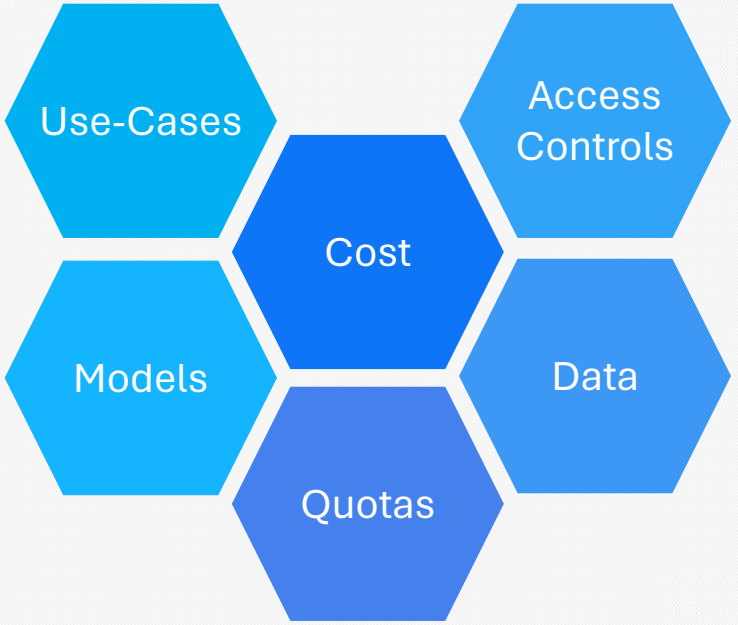


Context-Aware Guardrails for Security

LLM **Visibility**

Implement Controls, Monitor Cost and Govern Usage of AI

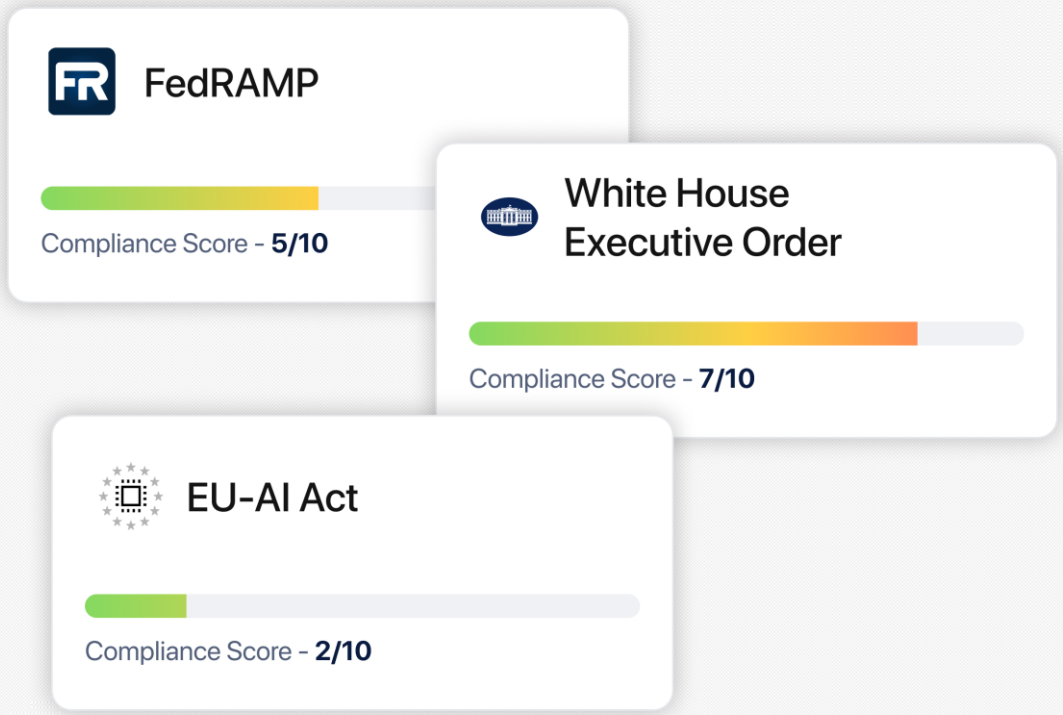


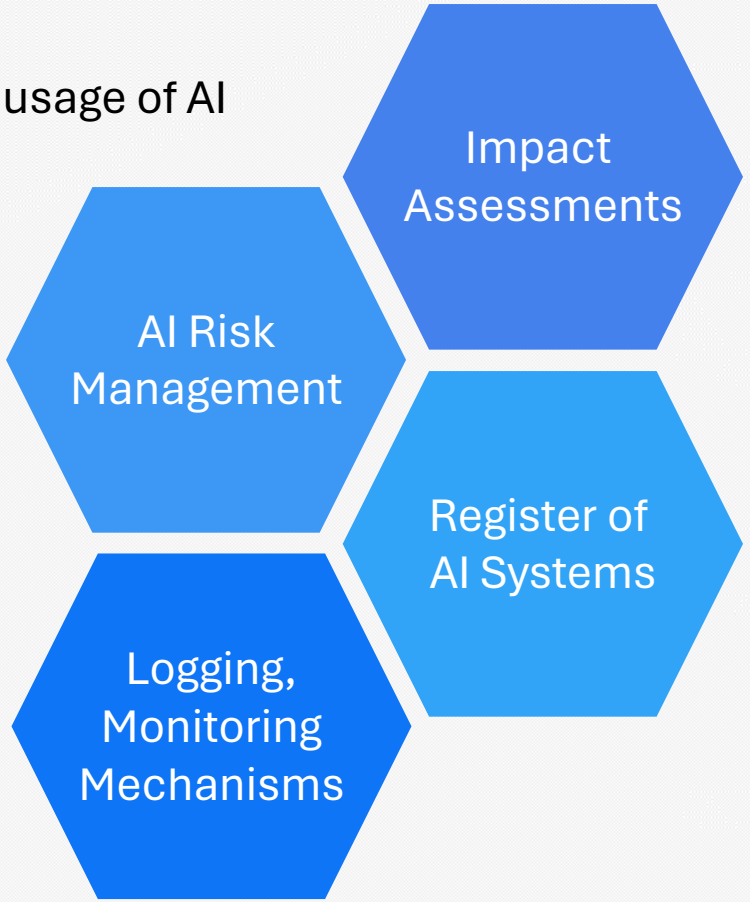


Operational Transparency and Monitoring

LLM **Compliance**

Manage and Reduce Risk, Map Regulatory Controls, Ensure compliant usage of AI





Automated Policy Enforcement and Auditing for AI Governance

Enkrypt **Solution**

- **Threat Detection -** Know your Vulnerabilities
- **Threat Mitigation -** Mitigate these Vulnerabilities
- **Data Protection -** Protect any sensitive information from leaking
- **Visibility -** Monitor Cost, Govern Usage of AI, and Implement Controls
- **Compliance -** Map Regulatory Controls, and ensure compliant usage of AI

Expedite Generative AI Pilots into Production

Generative AI in Production

Enkrypt AI

Enable 10x Faster & Safer Adoption of Generative AI within Enterprises

With a Structured & Actionable Generative AI Governance Framework

Contact us to schedule a Demo

sahil@enkryptai.com