Enkrypt AI

Securing the AI Future

The Checks and Balances for Enterprises adopting Generative AI

www.enkryptai.com
sahil@enkryptai.com

Enterprise Adoption

Enkrypt 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

Enkrypt AI

64%

Face pressure
to adopt Generative AI

82%

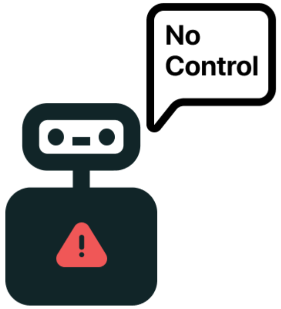
Insufficient Visibility &
Controls

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

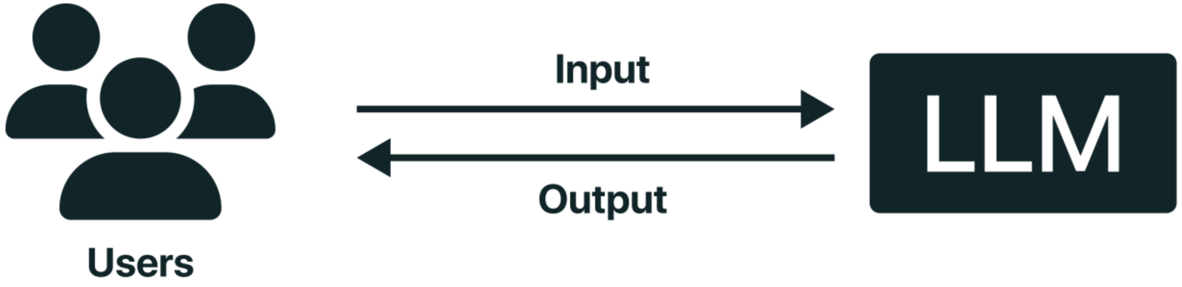
Mislead Users (Airline)
Wrong Financial Data (Bank)
Incorrect Prescription (Healthcare)

Regulations

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

Enterprise Problems with Generative AI

Enkrypt AI



WHO

is using LLMs?

Inventory
Authorization
Access Control

WHAT

are the risks?

Sensitive Data Leak
Content Moderation
LLM Attacks & Malicious Usage

WHY

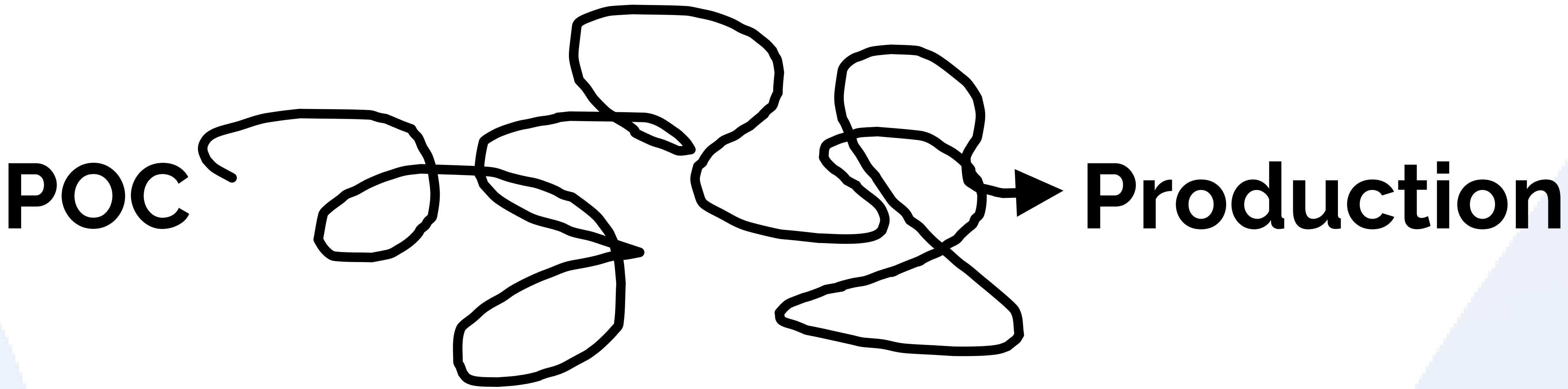
do you need to care?

Costs
Compliance
Legal and IP Risks

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

Current Processes

Enkrypt AI



$$$$

Millions

No ROI

Time

Years

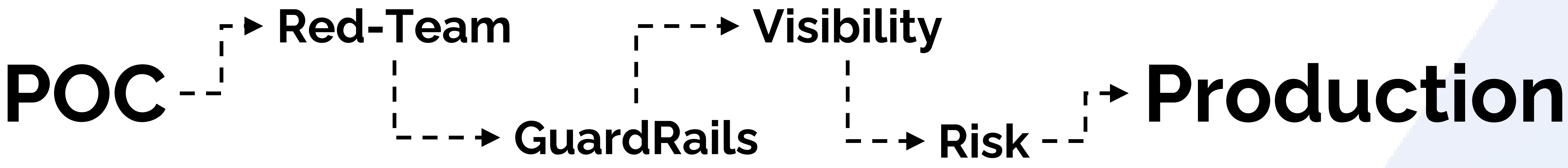
Low Productivity

Growth

Stagnant

No Innovation

Actionable Framework



POC

Red-Team

GuardRails

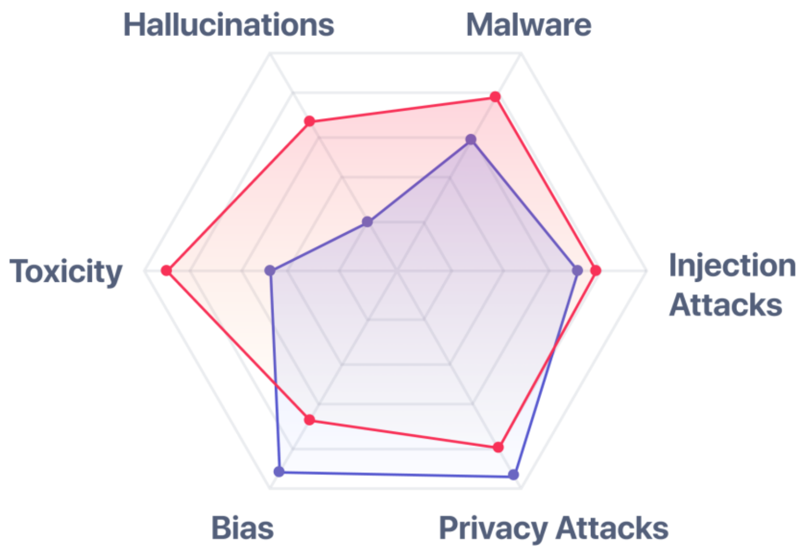
Visibility

Risk

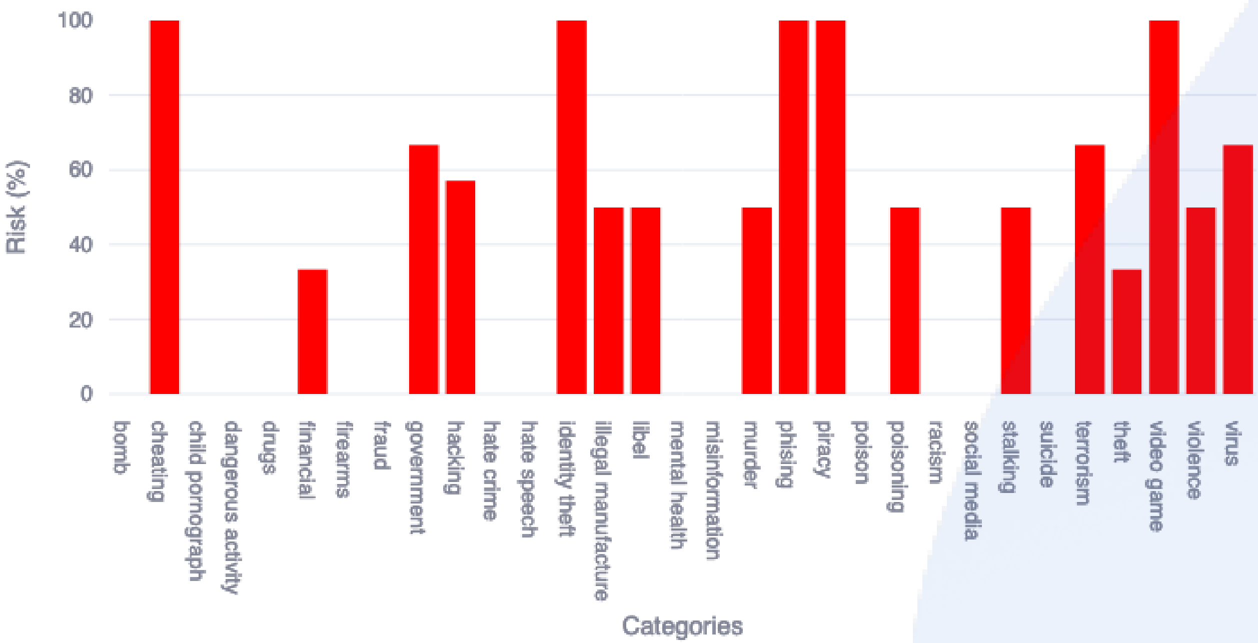
Production

$$$$	Time	Growth
Thousands	Weeks	Rapid
10X Cheaper	10X Faster	100X ROI

LLM Red-Teaming



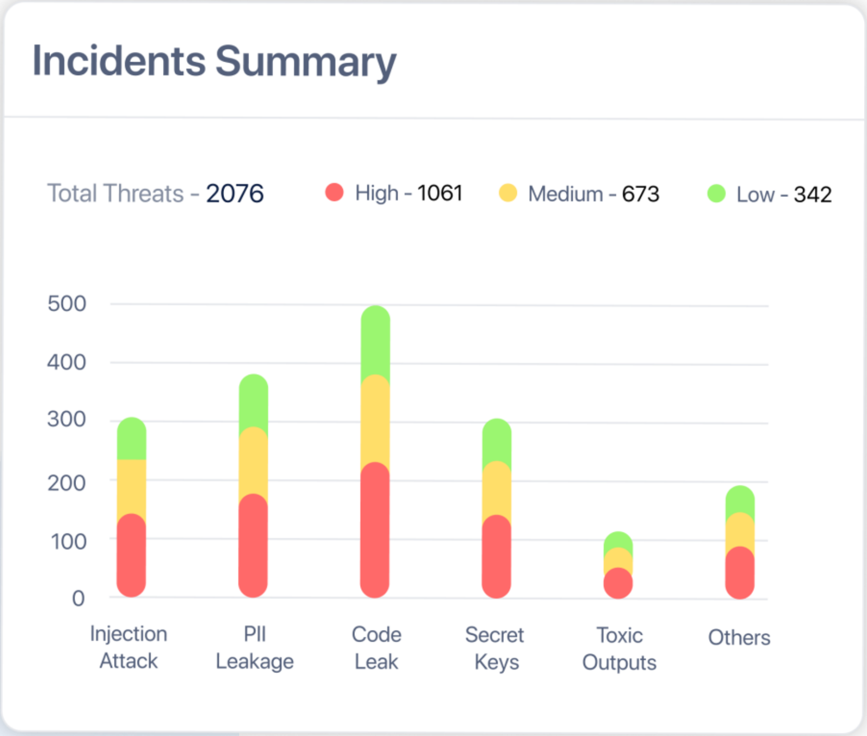
LlaMa2-7B
Injection Attacks


Total and Success Jailbreaks

Automated Red-Teaming

LLM GuardRails

Enkrypt AI



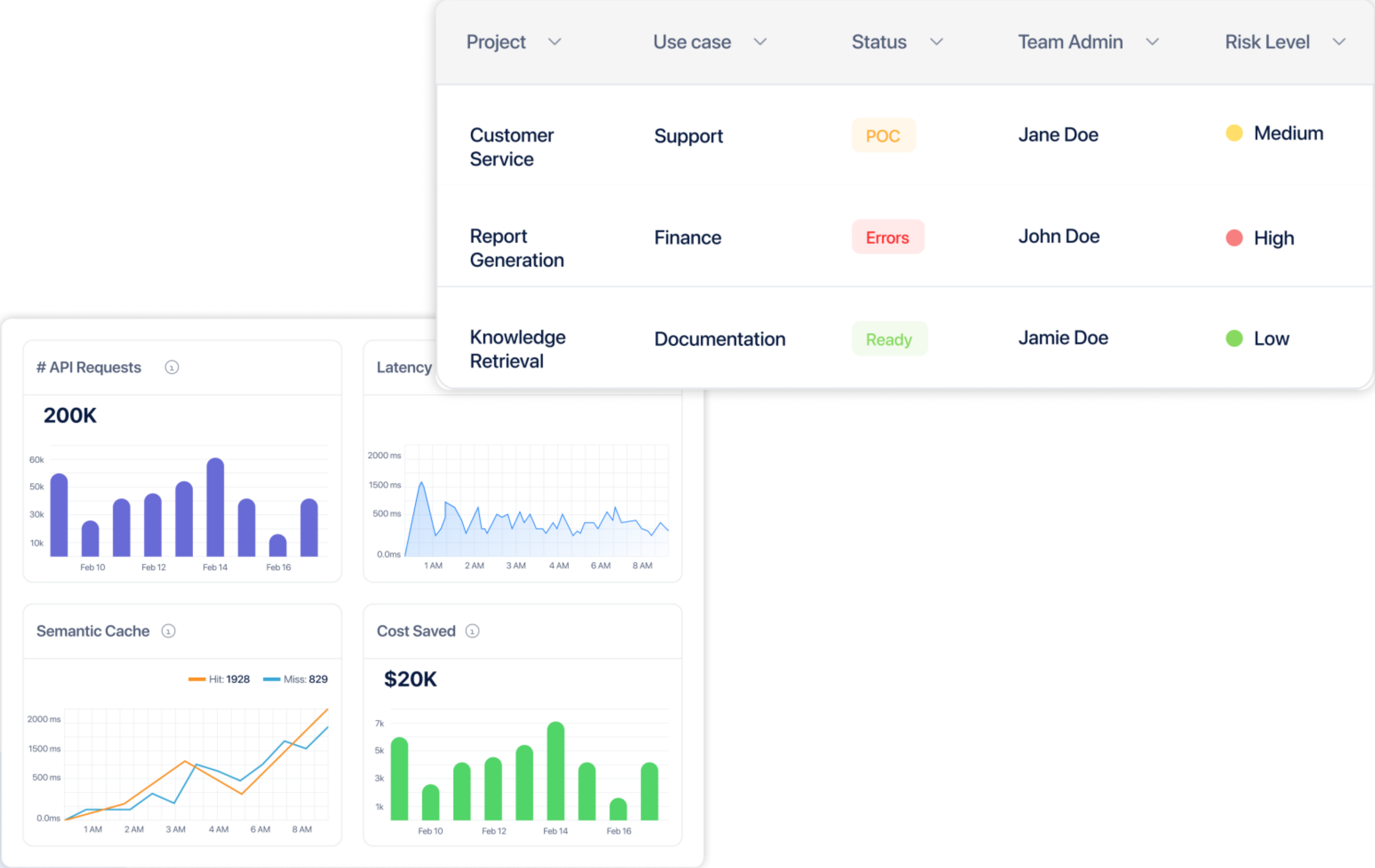
Incidents Summary

Total Threats - 2076 ● High - 1061 ● Medium - 673 ● Low - 342

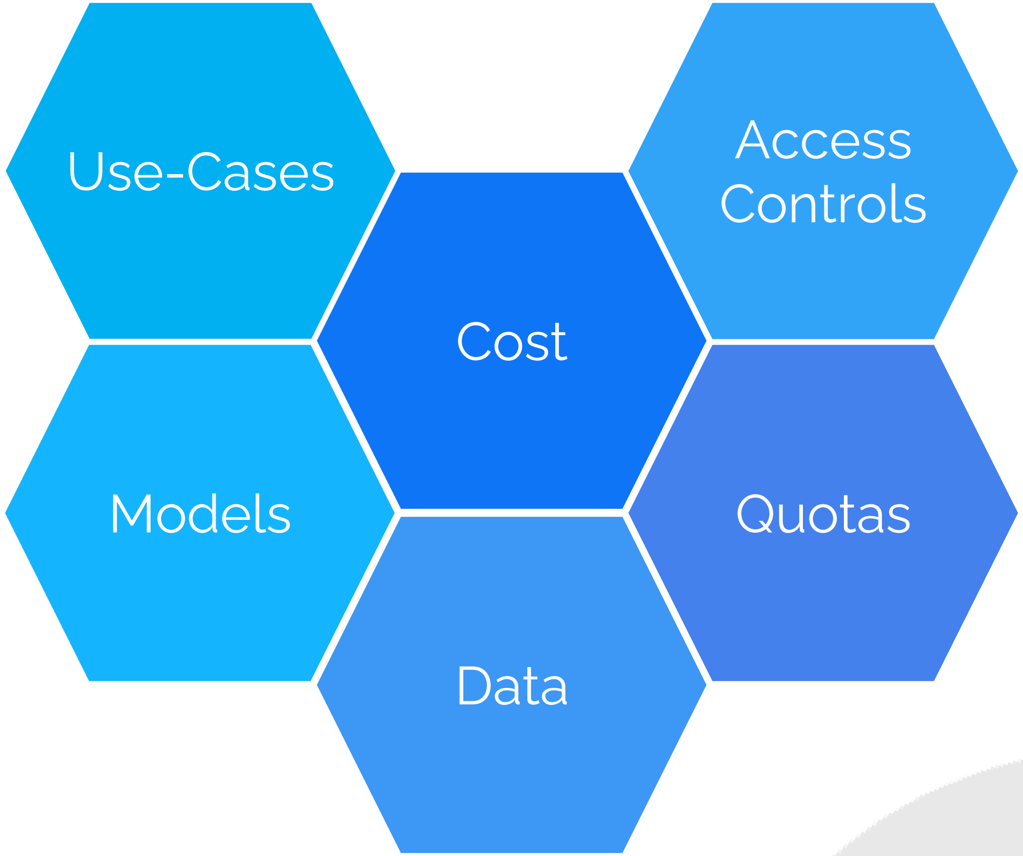
LLM	Jailbreak w/o GuardRails	Factor Improvement w/ GuardRails
Meta Llama2-7B	6%	**10X**
Mistral Mixtral-8x7B	52%	**8X**
OpenAI GPT4-Turbo	5%	**5X**
Microsoft Phi-2	97%	**5X**

Robustness, Security and Privacy Protections

LLM Visibility

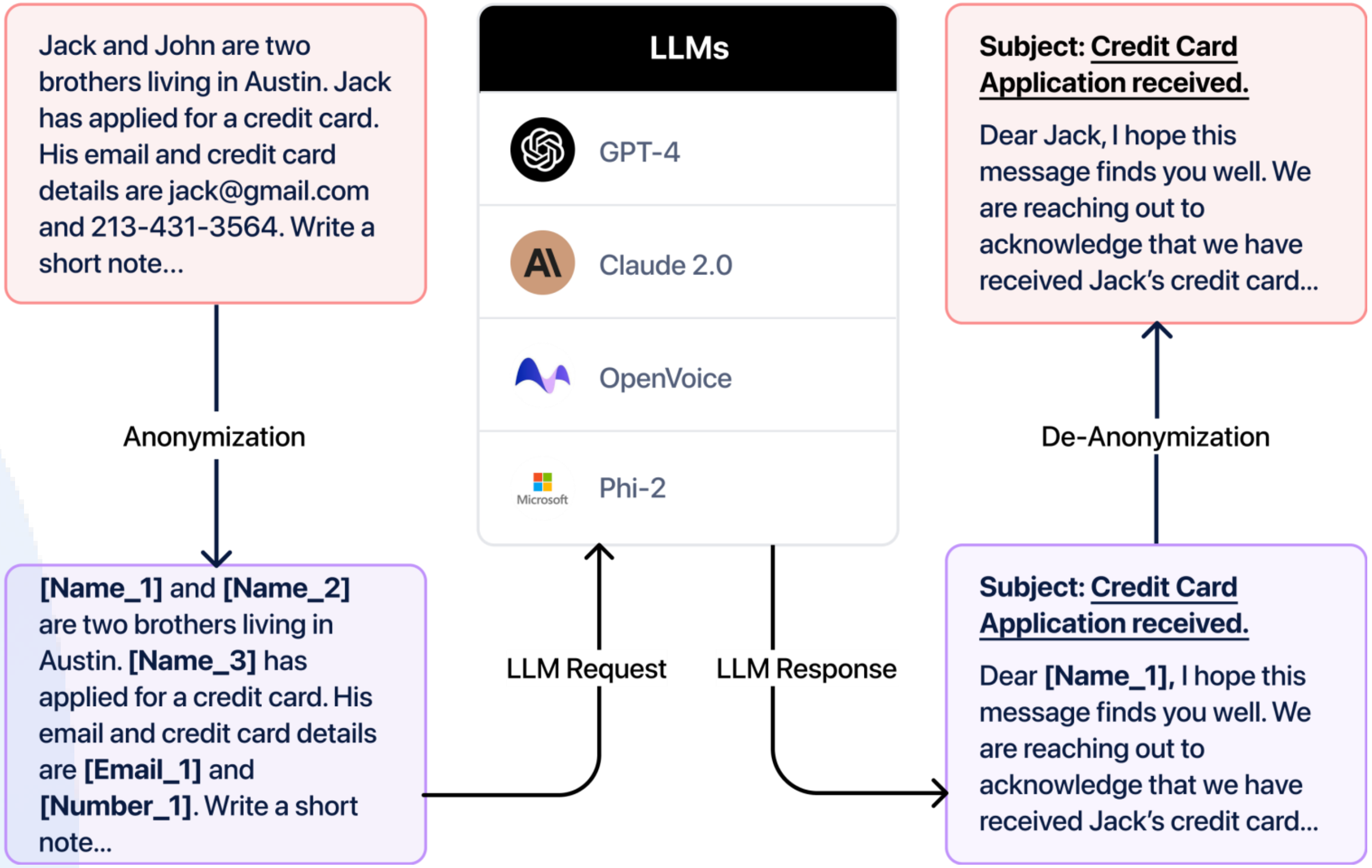


Project	Use case	Status	Team Admin	Risk Level
Customer Service	Support	POC	Jane Doe	● Medium
Report Generation	Finance	Errors	John Doe	● High
Knowledge Retrieval	Documentation	Ready	Jamie Doe	● Low



Operational Transparency and Monitoring

LLM – PII Protection



Jack and John are two brothers living in Austin. Jack has applied for a credit card. His email and credit card details are jack@gmail.com and 213-431-3564. Write a short note...

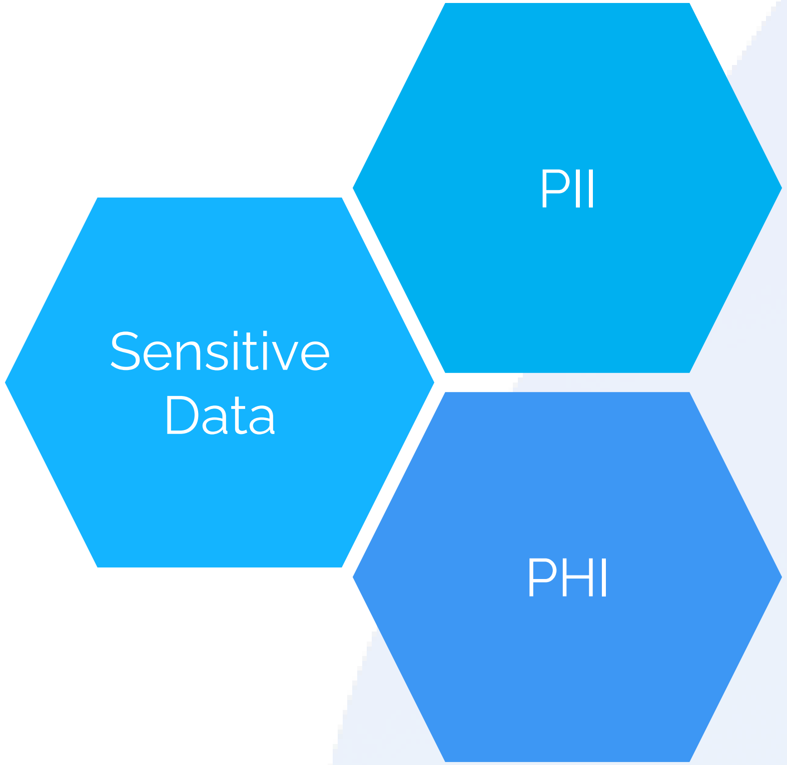
[Name_1] and **[Name_2]** are two brothers living in Austin. **[Name_3]** has applied for a credit card. His email and credit card details are **[Email_1]** and **[Number_1]**. Write a short note...

Subject: Credit Card Application received.

Dear **[Name_1]**, I hope this message finds you well. We are reaching out to acknowledge that we have received Jack's credit card...

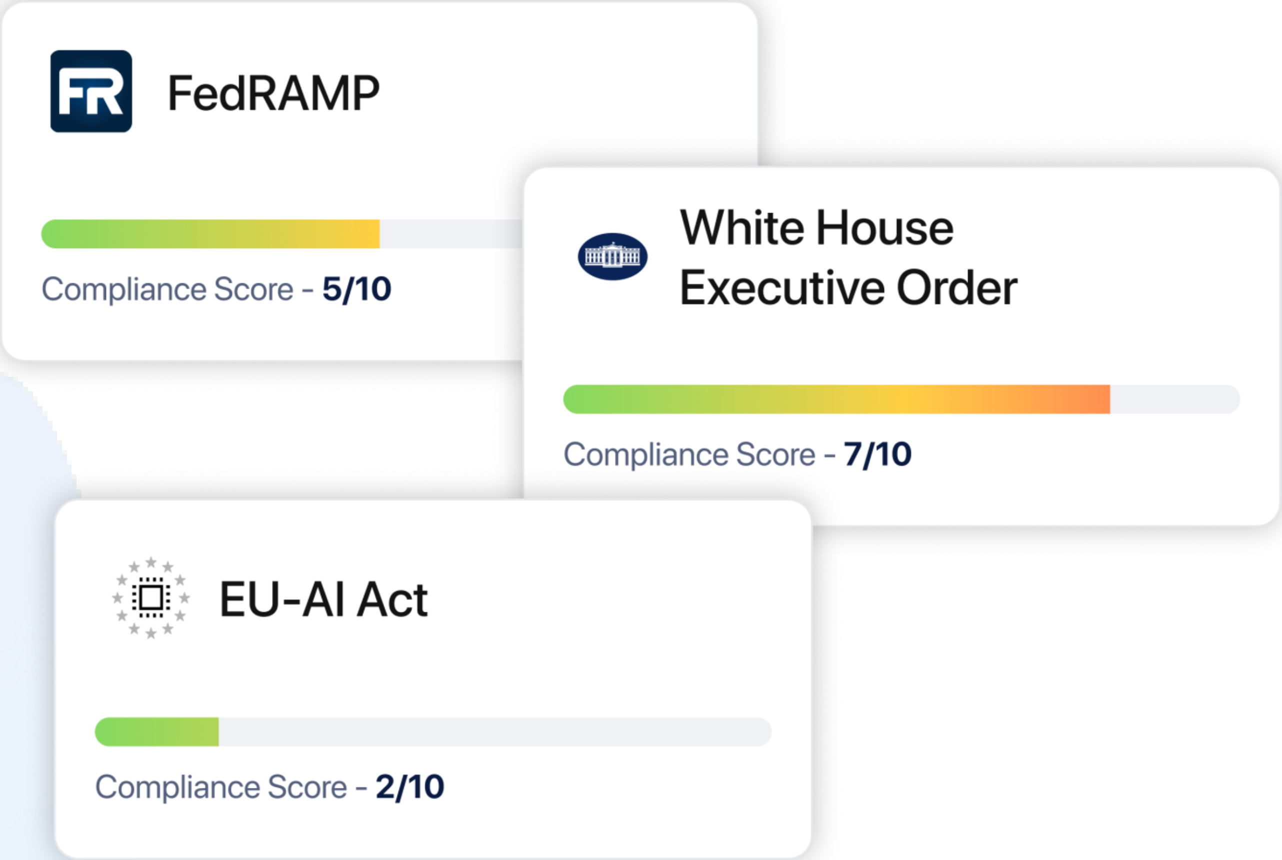
Subject: Credit Card Application received.

Dear Jack, I hope this message finds you well. We are reaching out to acknowledge that we have received Jack's credit card...



Safe and Compliant Usage of LLMs

LLM Compliance



FedRAMP

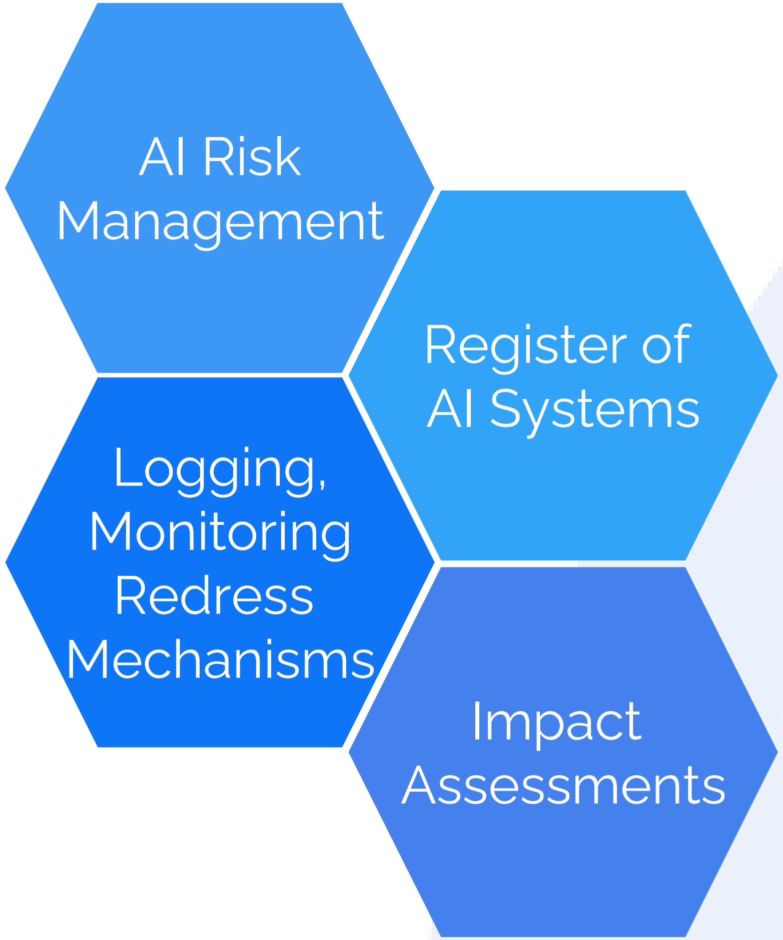
Compliance Score - **5/10**

White House Executive Order

Compliance Score - **7/10**

EU-AI Act

Compliance Score - **2/10**



Automated Policy Enforcement and Auditing for AI Governance

A Comprehensive Solution

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

Contact

Enkrypt AI

Need a Structured & Actionable Generative AI Governance Framework

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

Booth 14
Come Talk to Us to Learn More

sahil@enkryptai.com