



Best Practices for Accelerating Your AI Journey with Secure and Powerful Agents

KEVIN KILEY

DECEMBER 2024

Create & Maximize AI Value

ADOPT EXISTING

MODEL

DATA

PROMPTS

GOVERNANCE

SECURITY



LOWER VALUE
HIGHER RISK



Effort & Complexity



HIGHER VALUE
LOWER RISK

CREATE & CONTROL

MULTIPLE MODELS

DOMAIN MODELS

COMPANY MODELS

TOOLS & TECHNOLOGIES

DEPLOYMENT STRATEGIES

GOVERNANCE POLICIES

SECURITY FRAMEWORKS

PROMPTS & FINE-TUNING

Speed Bumps to Realize Higher Value & ROI



Data Integration



Security



Cost



Legal and IP



Regulatory and Governance
Challenges



Brand and Reputational Risk

Entirely New Security Threat Vectors

New attack surfaces across the AI lifecycle



- Training data poisoning
- Data theft
- Untrusted inference infrastructure
- Model theft
- Uncertain model provenance

- Shadow AI
- Data leakage
- Model denial-of-service attacks
- Prompt injections
- Insecure tool calls

TikTok owner sacks intern for sabotaging AI project

9 hours ago

Share  Save 

João da Silva
Business reporter



Getty Images

The firm said its commercial online operations, including its large language AI models, were unaffected

93% of hackers believe enterprise AI tools create a new attack vector

By Jordyn Alger, Managing Editor

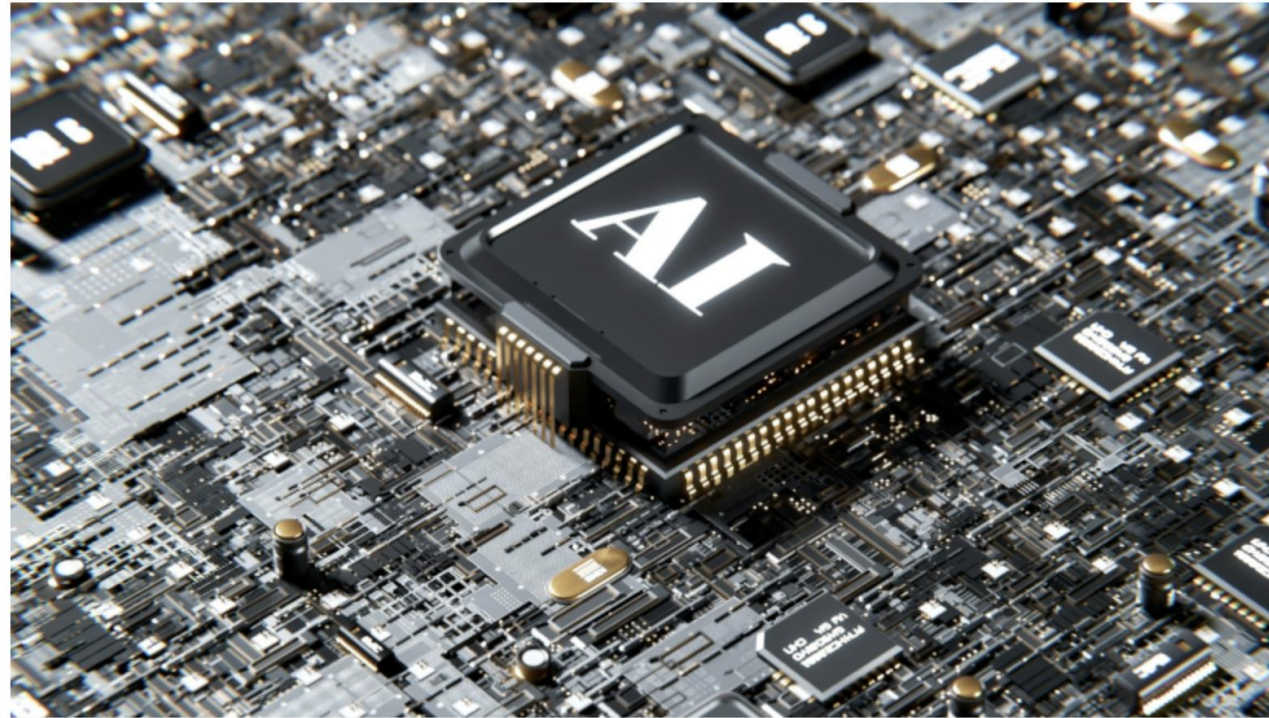


Image via Unsplash

October 18, 2024





Model Security



Superpowered Hacks & Exploitations

Data Poisoning





Data Security & Poisoning

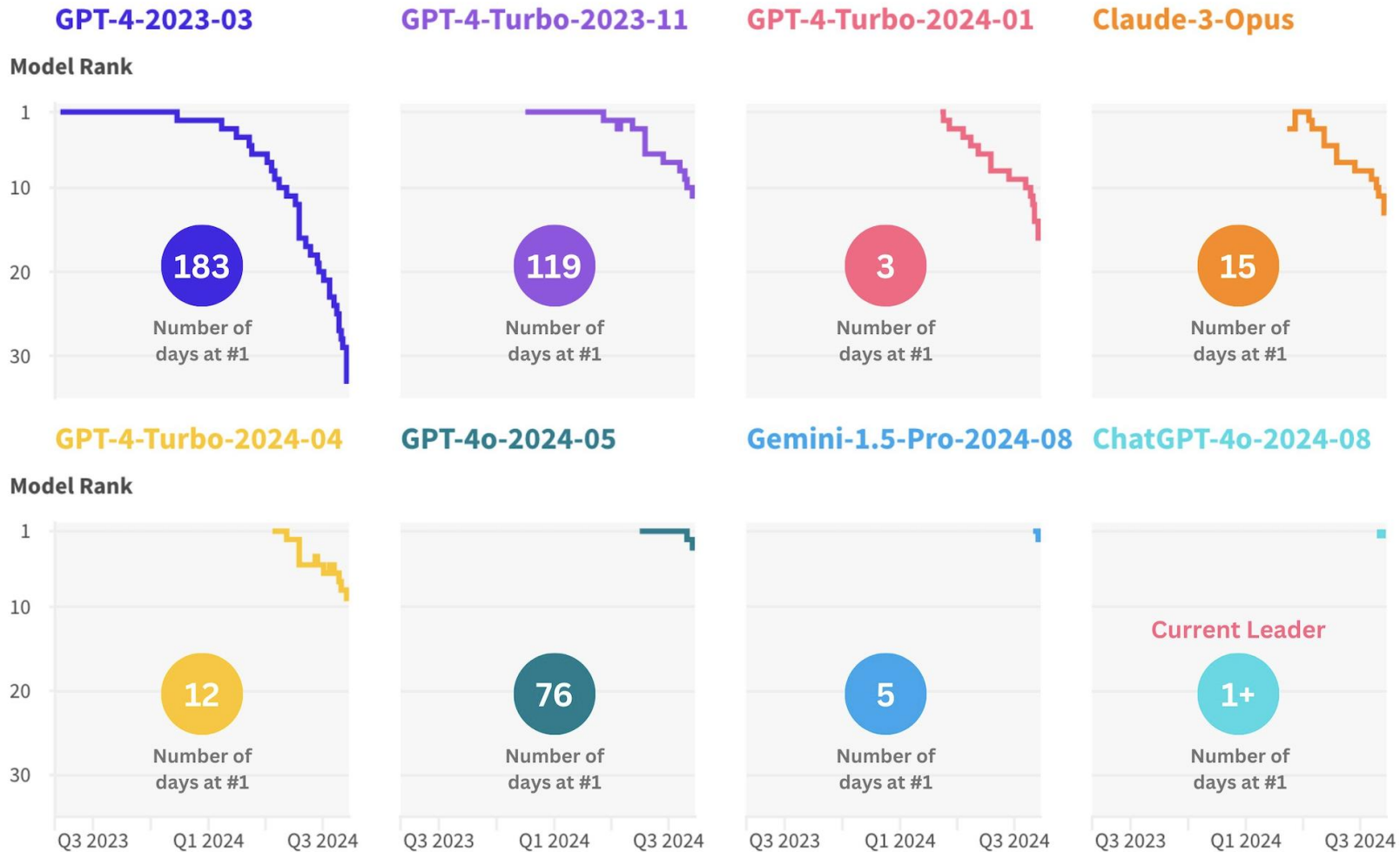


Operational Security

AN EXPLOSION OF MODELS

How long do models last on top?

On average ~60 days, down to ~20 days in the last 6 months



LMSYS Chatbot Arena, @AmebaGPT

Rapid Deprecation of “Old” Models

Subject: Final Deprecation Reminder: gpt-3.5-turbo-0301, gpt-3.5-turbo-0613, and gpt-3.5-turbo-16k-0613



This is a final reminder that the following models will **no longer be available** starting next Friday, September 13, 2024:

- [gpt-3.5-turbo-0301](#)
- [gpt-3.5-turbo-0613](#)
- [gpt-3.5-turbo-16k-0613](#)

We have noticed that your organization has recently used at least one of these models. To avoid any disruption, we encourage you to migrate to [gpt-4o-mini](#), our new small model that will give you higher performance at lower cost.

Thanks for building with OpenAI. If you have any questions about model migration, feel free to reach out on the [OpenAI Developer Forum](#).

—The OpenAI Team

Subject: Deprecation Reminder: GPT-4 Vision Preview will be shut down on December 6, 2024



In **June 2024** we announced the deprecation of the following models, with a planned shutdown date of December 6, 2024:

- [gpt-4-vision-preview](#)
- [gpt-4-1106-vision-preview](#)

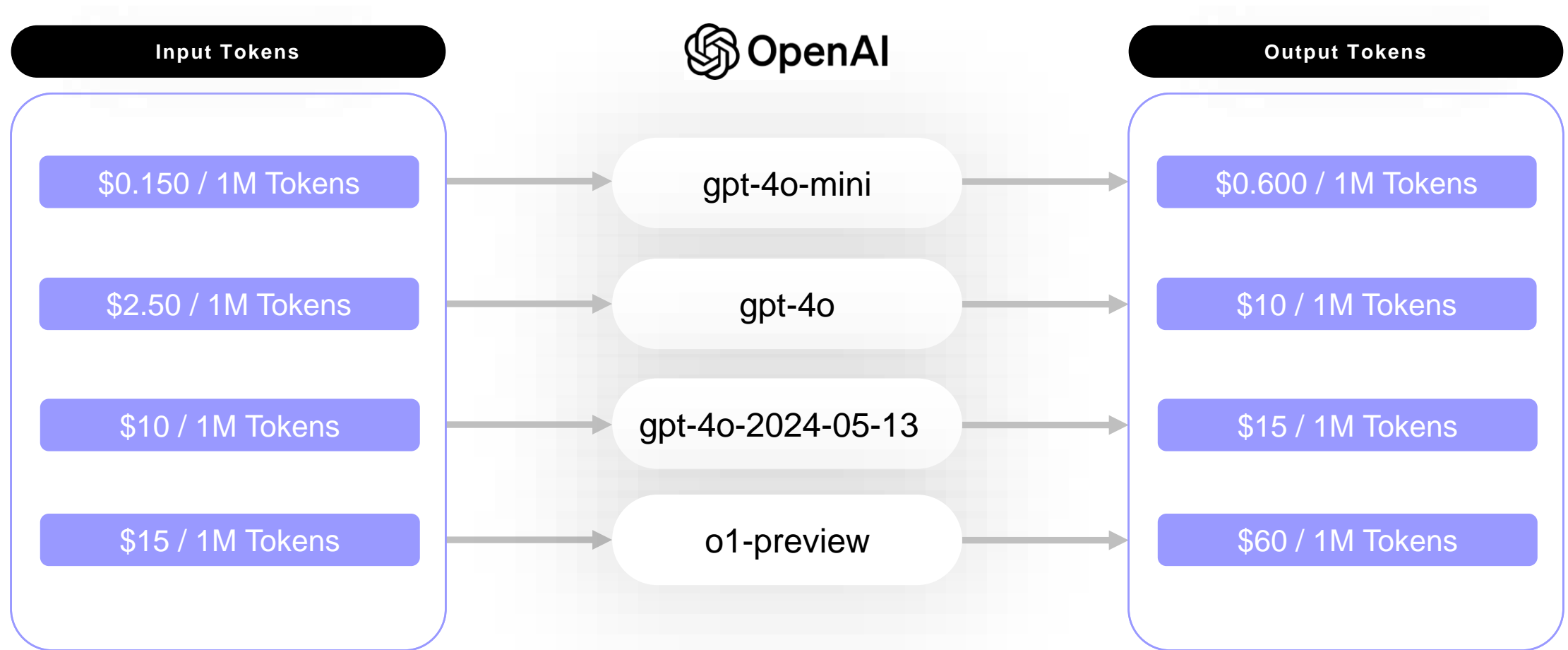
We have noticed that your organization has recently used one of these models. We encourage you to migrate to [GPT-4o](#), our latest flagship model, as a replacement.

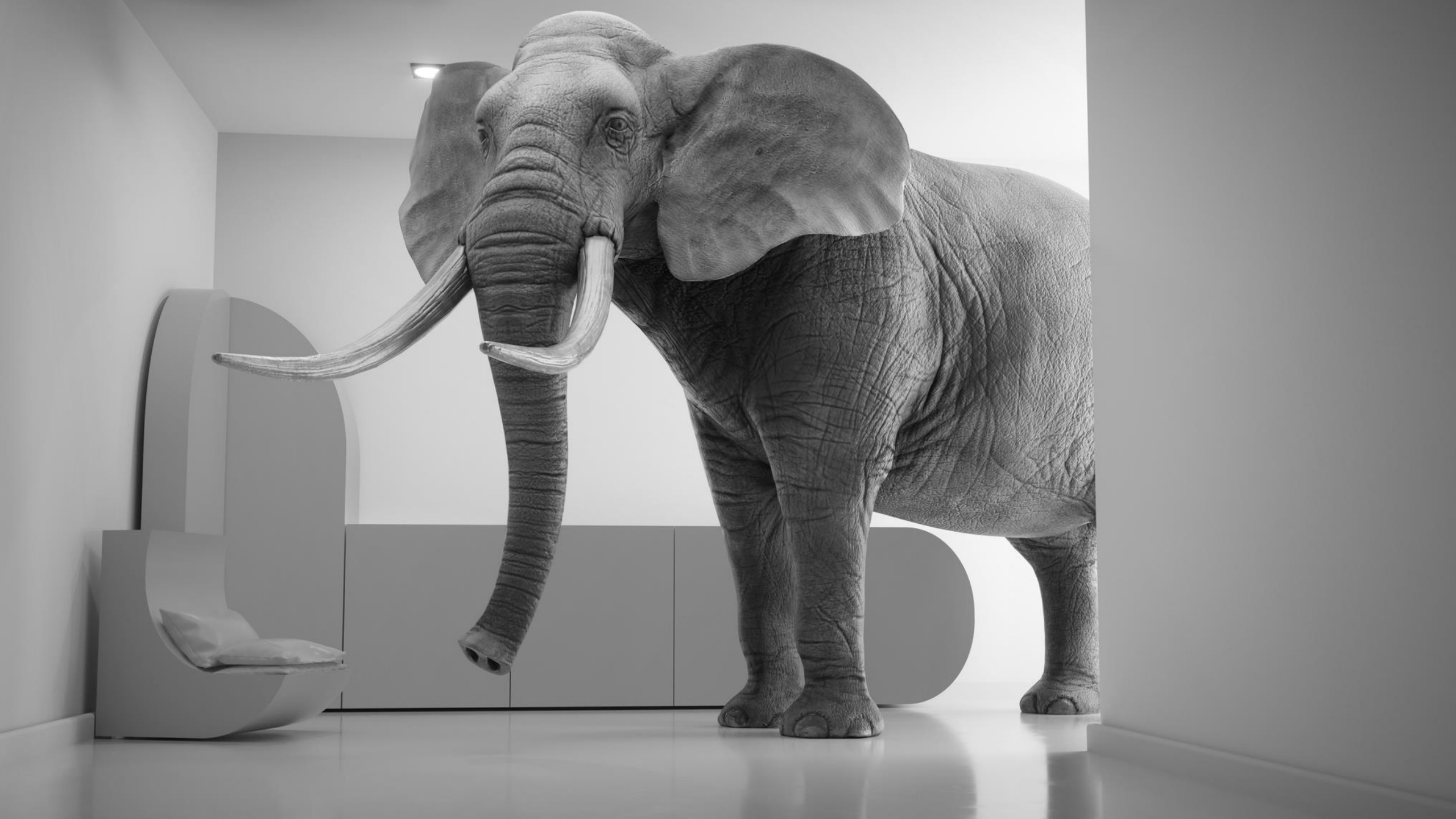
Thanks for building with OpenAI. If you have any questions about model migration, feel free to reach out on the [OpenAI Developer Forum](#).

—The OpenAI Team

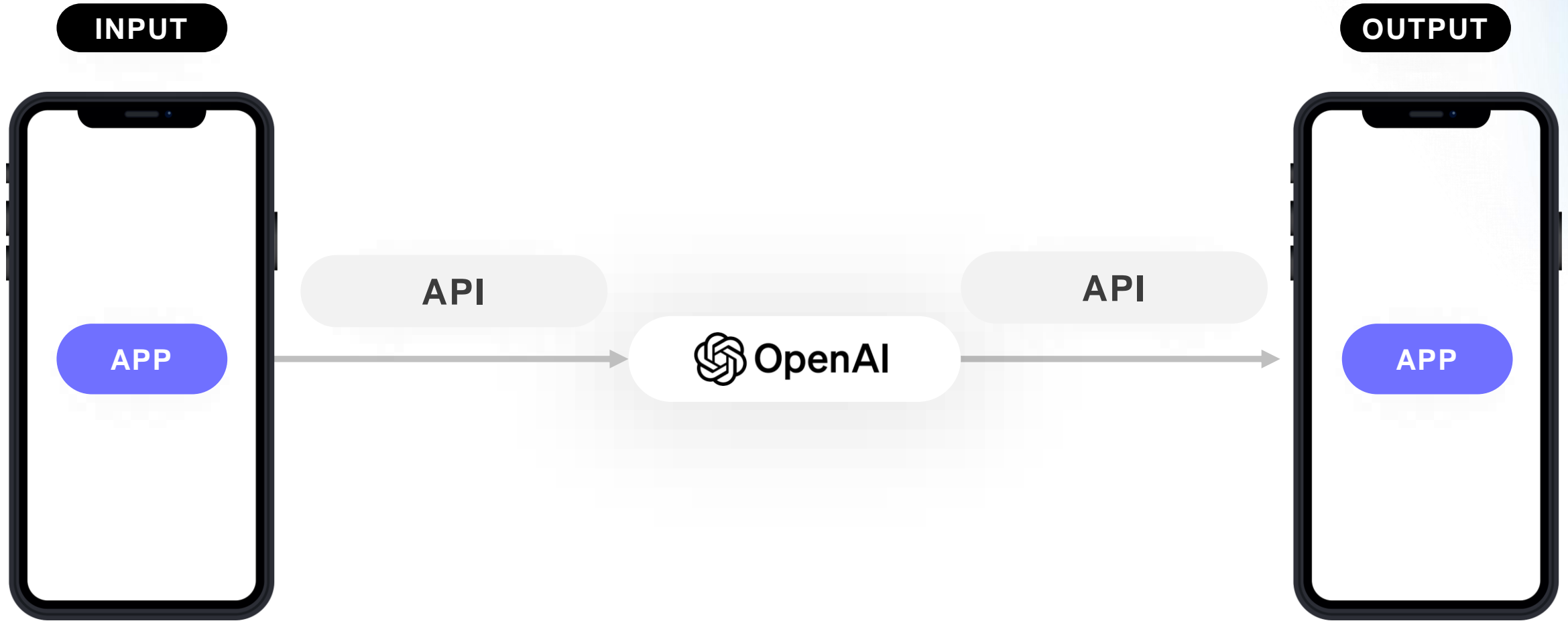
Significant Cost Differences

Same prompt, same model provider, similar responses but wildly different costs

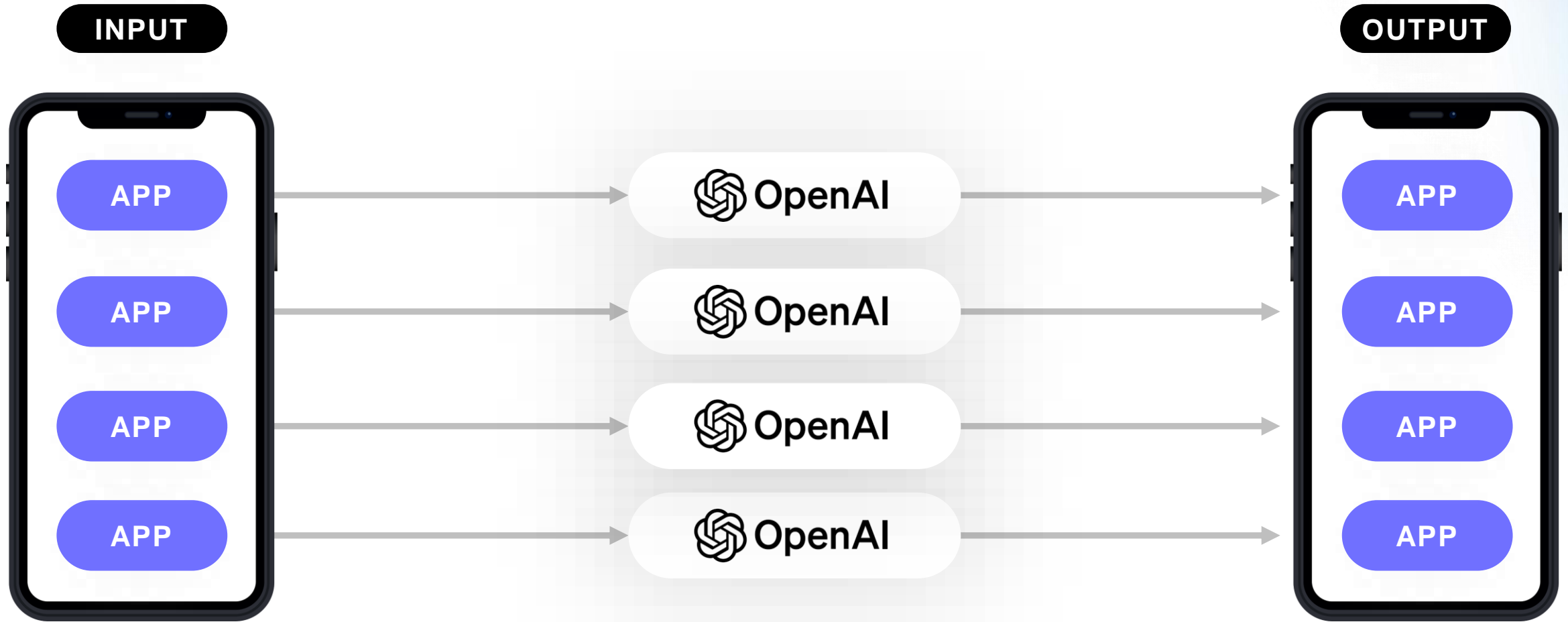




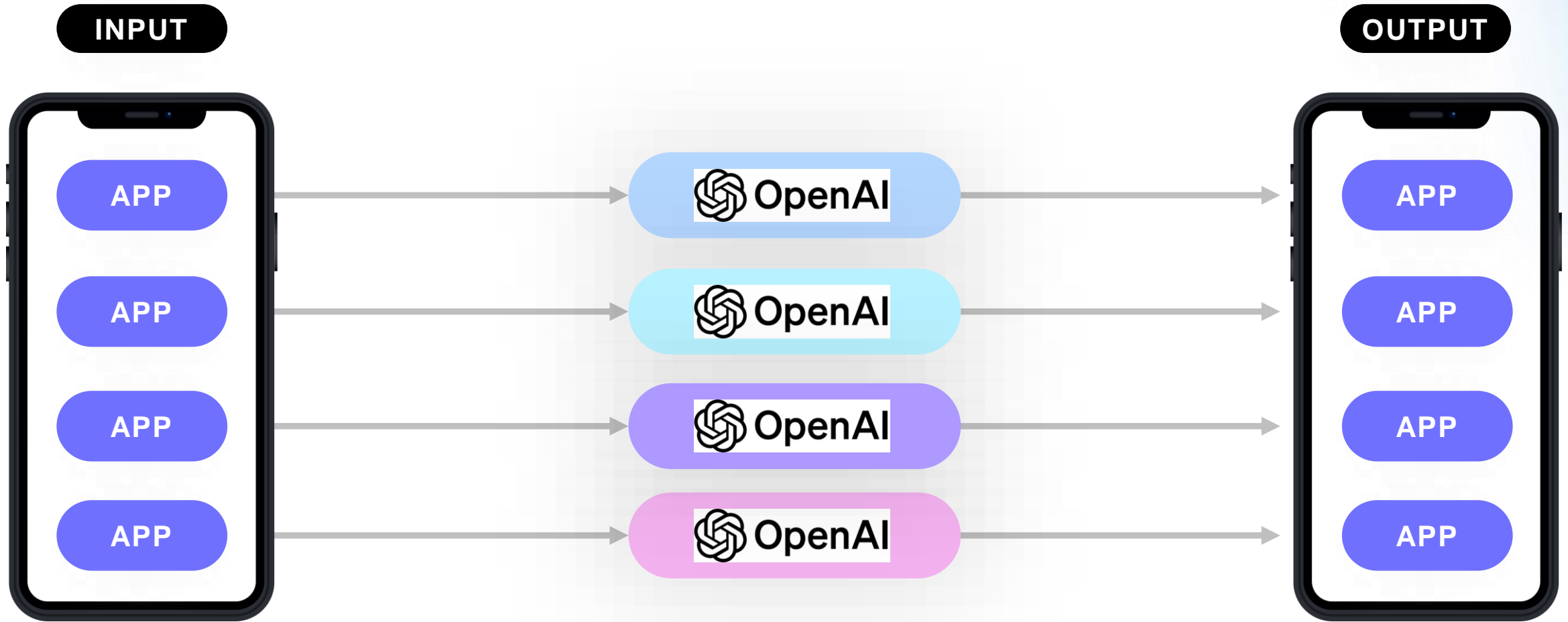
A Common Starting Point



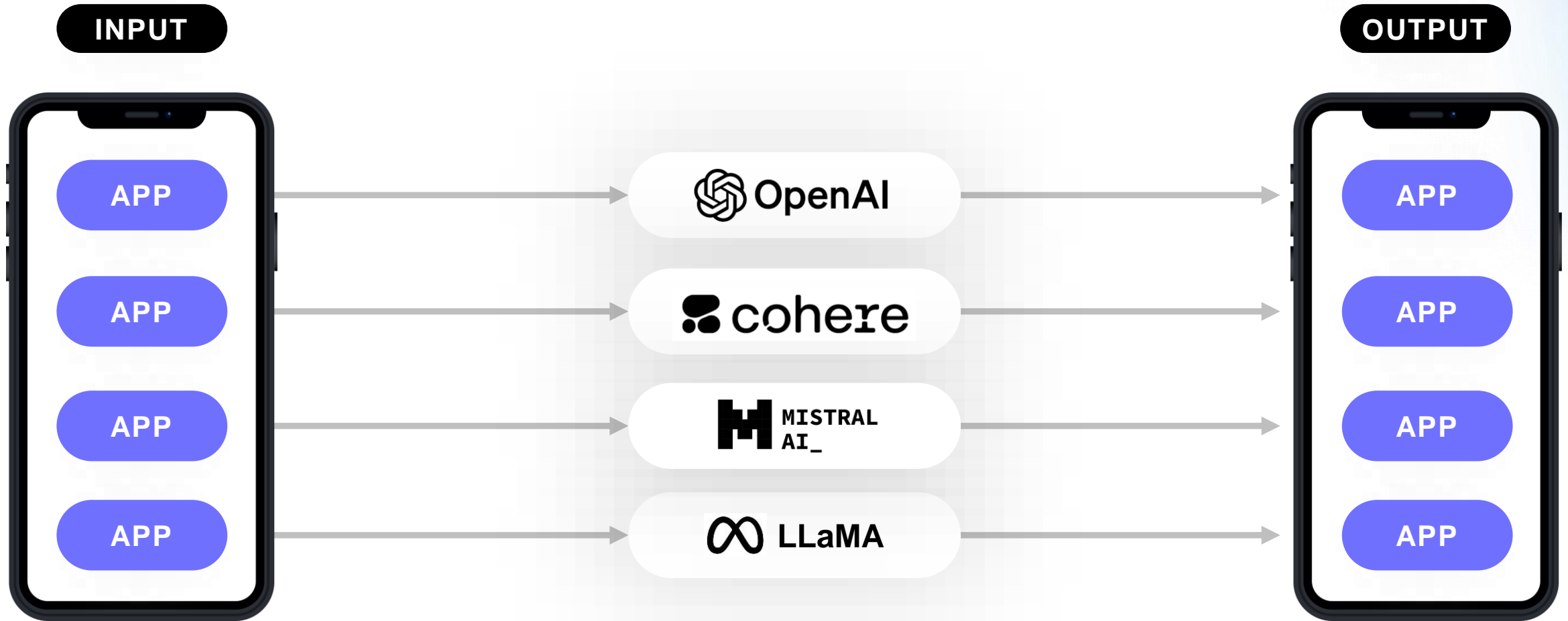
Use Cases Expanded



Version Proliferation from LLMs

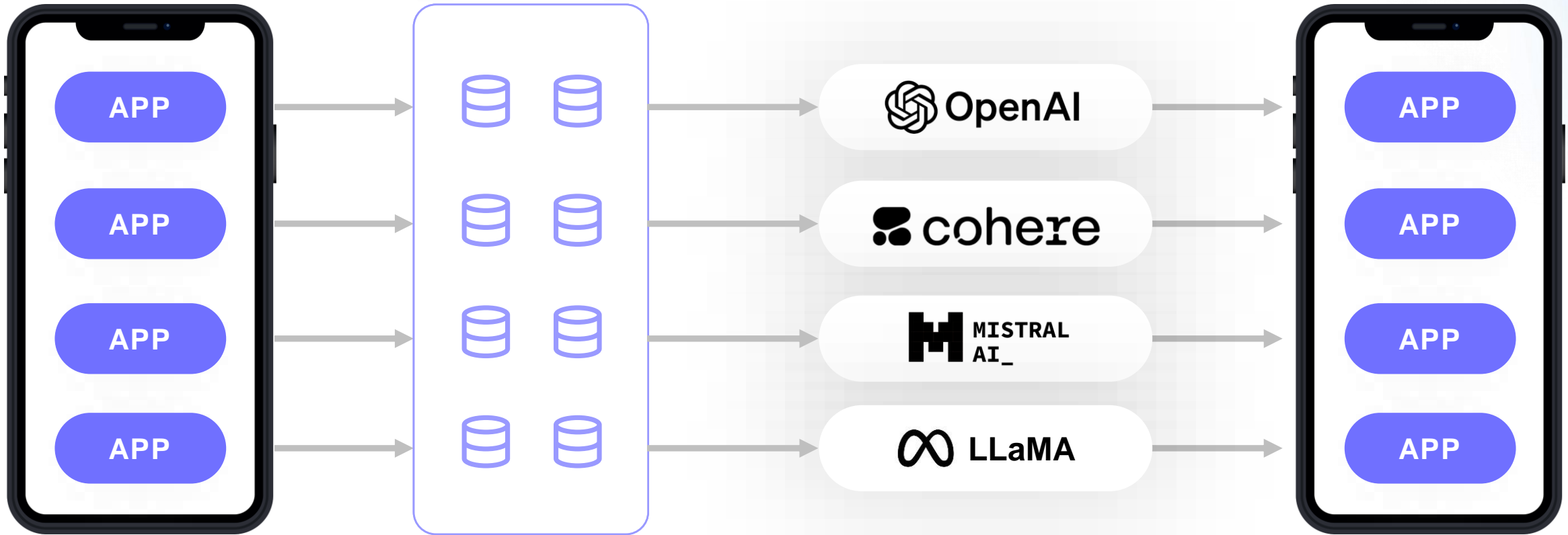


Across Multiple LLMs



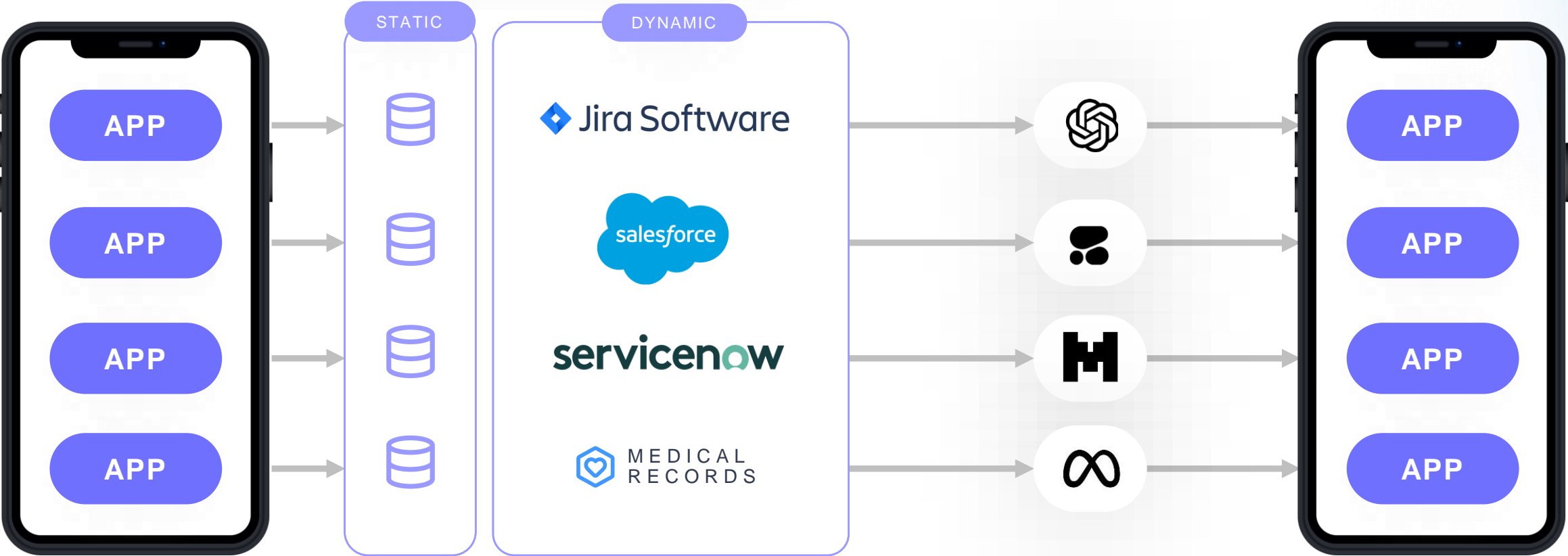
Combined with Company Information

ADDITIONAL DATA SOURCES

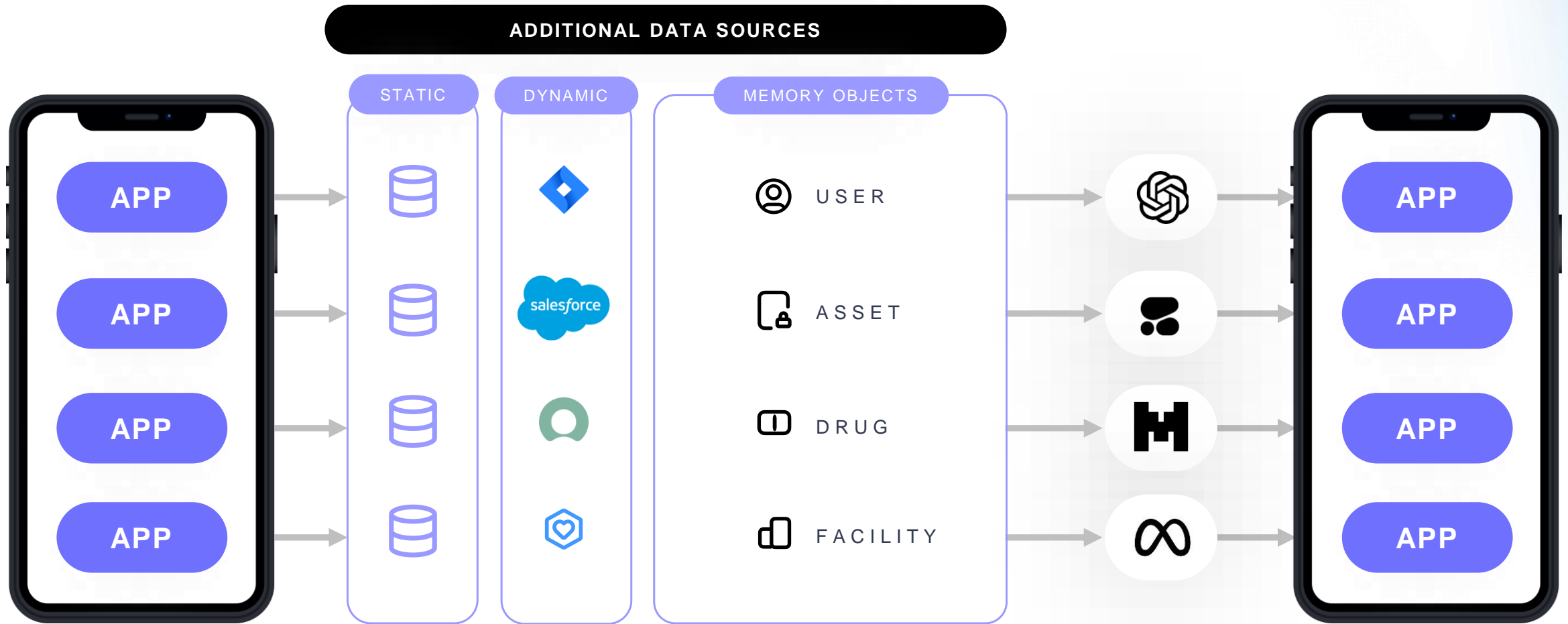


Transactional Data

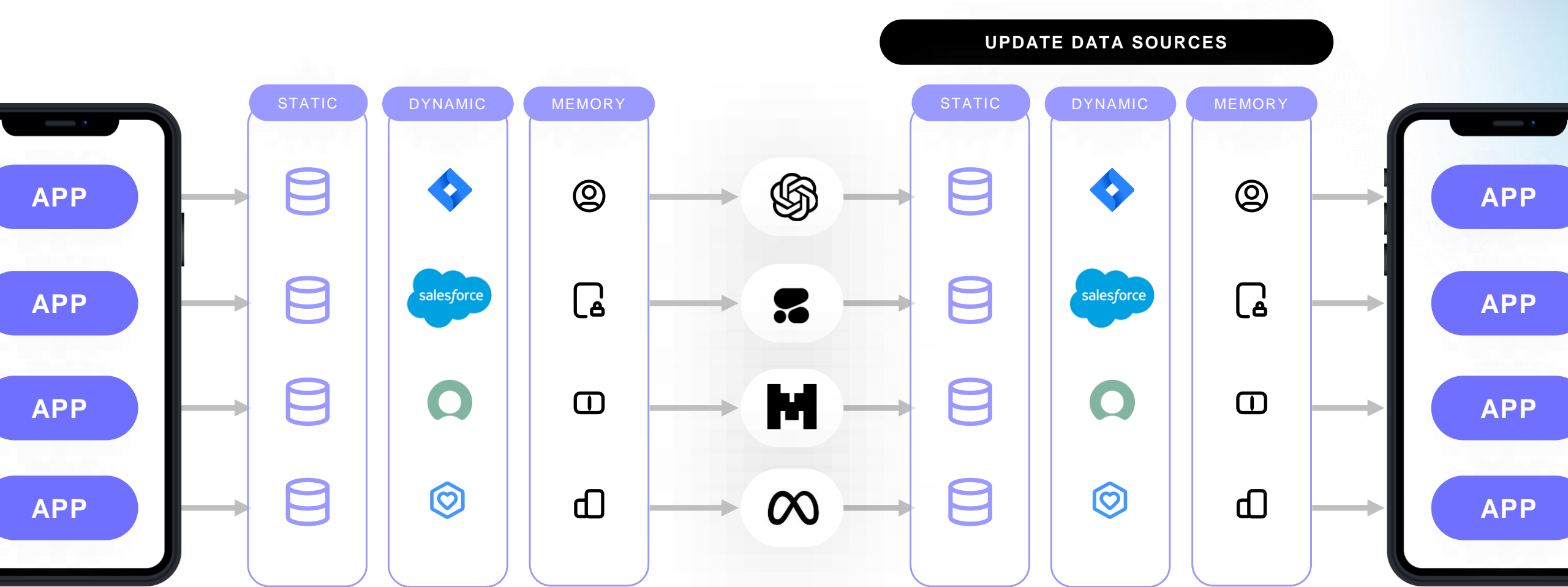
ADDITIONAL DATA SOURCES



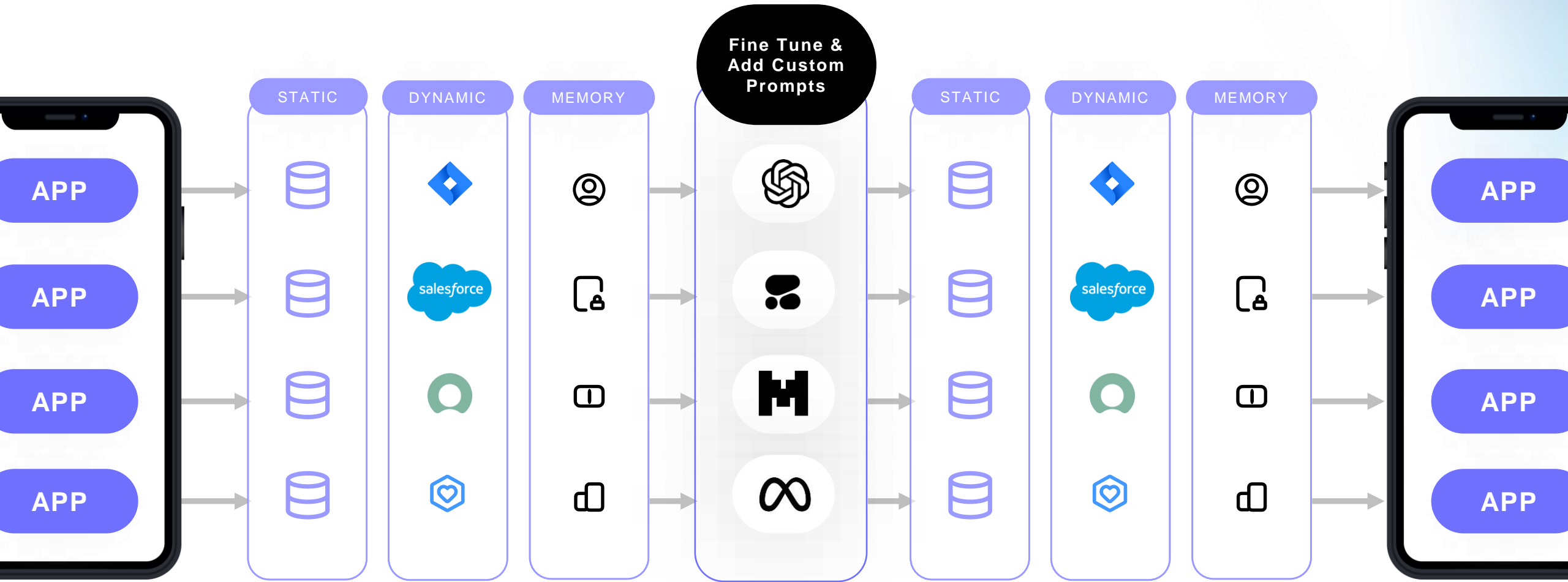
Plus Memory Objects



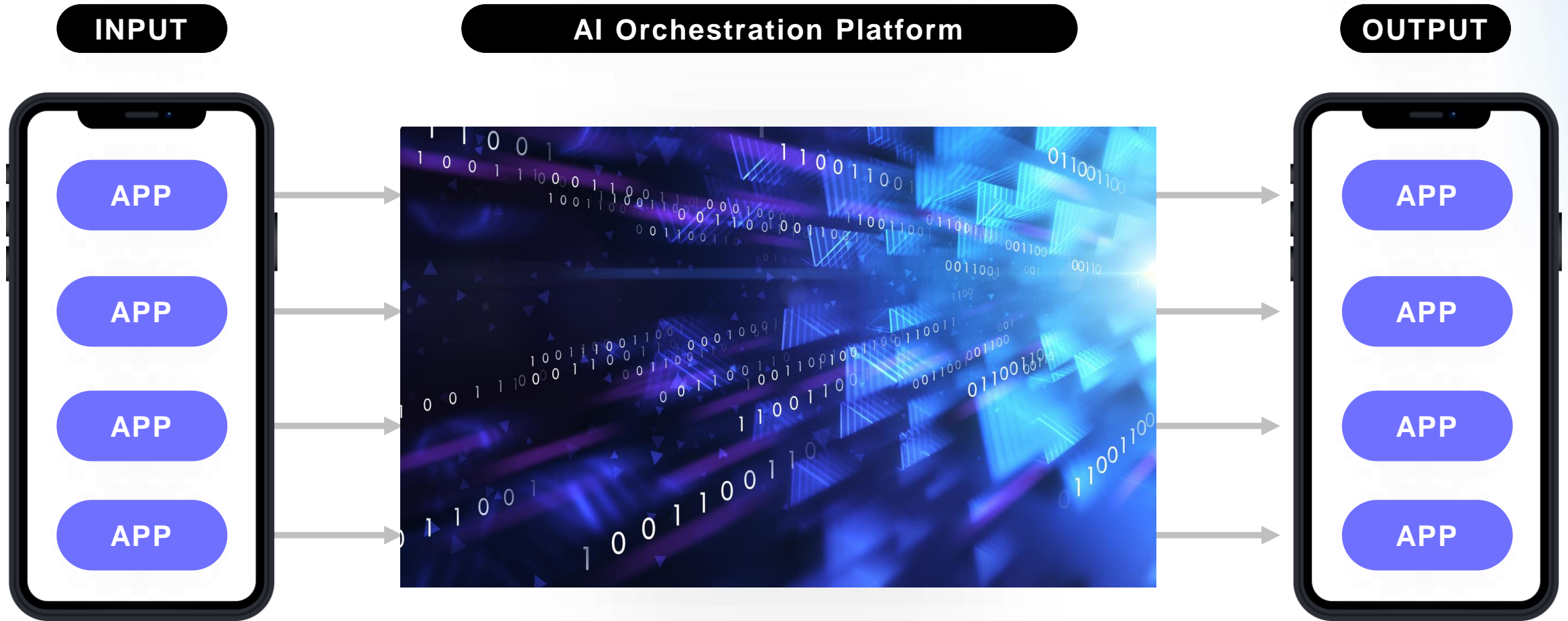
Write Updates to Data Sources



Maximize Value with Prompts & Fine Tuning









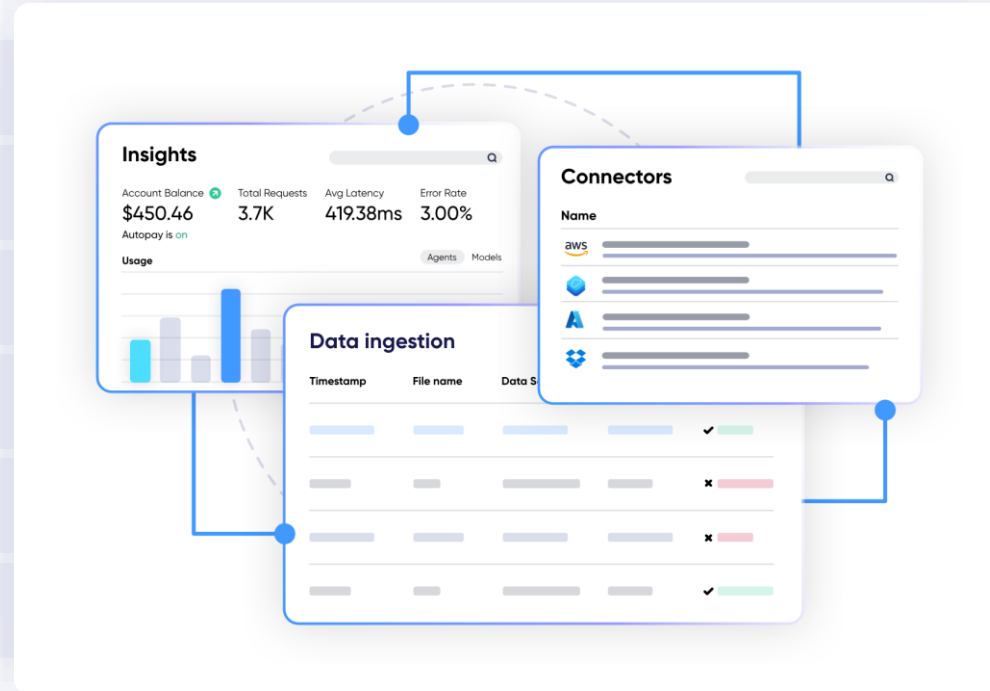
Abstract Operational Complexity for Success









Enterprise AI Platform

Accelerate and secure AI deployments with a comprehensive platform

-  **AI Gateway**
-  **Cost Optimization**
-  **Developer Studio**
-  **Intelligent Routing**
-  **Model Lifecycle**
-  **Model Guardrails**



- Observability** 
- Orchestration** 
- Prototype & Testing** 
- Prompt Studio** 
- Prompt Management** 
- Security & Governance** 

Data Integration

Enterprise Security

Responsible AI

Deployment Options

Your company data has always been one of your most valuable assets.

Now, it's not just your data,

it's your **AI**

[Data Integration
Models
Prompts
Tuning
Policies
Governance]

Now, it's not just your data,

it's your **AI strategy & platform**

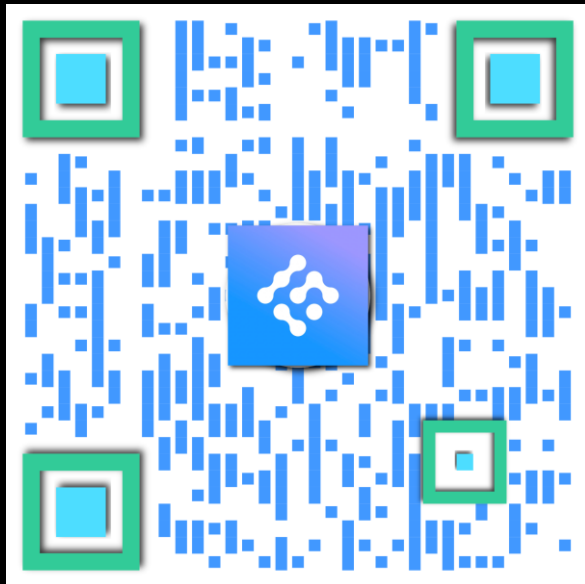
own AI. How do I avoid vendor lock in. What are AI Agents. What is computer vision? What is AGI/Artificial General Intelligence? What is the singularity? How smart is AI? How will AI affect our capital and operating expenditures? What is Jailbreaking an LLM? What is accelerated computing? How can an AI be made better? Why should I care about AI? What is parallelization? What is a

H100? Does OpenAI use my questions to train other models (or LLMs)? What is a private model? How do I use a private model? Is it safe to give an LLM my contracts and info? Can an LLM write documents for me? What causes a model to hallucinate? How do I trust answers from LLMs aren't hallucinations? Should I train a model for my company? How

**how can
airia help me
with AI?_>**

long does it take to train a model on my data? How do I give an LLM sensitive information from my company? Can AI be secure? What is the future of AI in my field? How can I use AI in my work? How reliable are AI models? What are the potential risks of error or bias? What happens when AI gets it wrong? How does AI

Request a copy of today's presentation



Visit our booth for a live demo | #B12

