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

APRIL 16TH, 2025

© 2025 Airia, LLC

# Company Background

airia

Enterprise AI platform to **accelerate and simplify AI adoption and operationalize** ongoing management

We are a **global organization** with employees across eleven countries and true follow-the-sun support

**Strong balance sheet** with substantial investments in R&D and a broad IP portfolio

Proven team with **extensive experience** building successful, trusted enterprise software companies

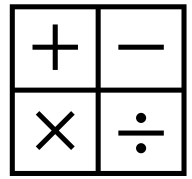
airwatch™ onetrust



© 2025 Airia, LLC

How do I get value?

# Change the Equation



- Investments don’t have to break the bank
- Returns can be immediate and impactful
- AI Orchestration layer is game-changing
- Training and adoption can accelerate organically
- Not moving fast is riskier than moving fast

airia

© 2025 Airia, LLC

How do I manage: Security, Risk, Data, Trust?

# What just happened?

🎉 DeepSeek-R1 is now live and open source, rivaling OpenAI's Model o1. Available on web, app, and API. Click for details.

deepseek

## Into the unknown

### Start Now

Free access to DeepSeek-V3.

Experience the intelligent model.

### Get DeepSeek App

Chat on the go with DeepSeek-V3

Your free all-in-one AI tool

# What Just Happened?

## DeepSeek Terms of Use

Last Update: January 20, 2025

No Indemnification | Confidential Data | Monitoring Interactions | Data Transfers

DeepSeek products and services are jointly owned and operated by Hangzhou DeepSeek Artificial Intelligence Co., Ltd., Beijing DeepSeek Artificial Intelligence Co., Ltd. and their affiliates (hereinafter referred to as **"DeepSeek"** or **"we"**). Before using the Services, please make sure to carefully read and understand this "DeepSeek Terms of Use" (hereinafter referred to as "these Terms") as well as other related terms, policies, or guidelines of this platform. When you use a specific function of the Services, there may be separate terms, related business rules, etc. ("Specific Terms") for that specific function. In the event of any conflict between these Terms and the Specific Terms, the provisions of the Specific Terms shall prevail. **All the aforementioned terms and rules form an integral part of these Terms (collectively referred to as "All Terms"), and have the same legal effect as the main text of these Terms.**

Among them, the **DeepSeek Open Platform Terms of Service** is specifically applicable to your use of the Application Programming Interface (API) or other developer tools and open platform services provided by this platform.

For detailed rules on how we collect, protect, and use personal information, please carefully read the DeepSeek Privacy Policy.

We especially remind you to carefully read (minors under the age of 18 shall read with their legal guardian) and fully understand all the terms before using the Services. When you agree to these Terms through online page clicks, checking boxes, or by actually using our services, it means you and we have reached an agreement on All Terms, you have accepted All Terms and their applicable conditions, and agree to be bound by All Terms. If you disagree with any part of these Terms, or cannot accurately understand our interpretation of any term, please click disagree or stop using our services.

### 7.Disclaimer of Warranties, Limitations of Liability, and Indemnity

7.1 NOTHING IN THESE TERMS SHALL AFFECT ANY STATUTORY RIGHTS THAT YOU CANNOT CONTRACTUALLY AGREE TO ALTER OR WAIVE AND ARE LEGALLY ALWAYS ENTITLED TO AS A CONSUMER.

7.5 You agree to indemnify, defend, and hold us and our affiliates and licensors (if any) harmless against any liabilities, damages, and costs (including reasonable attorneys'fees) payable to a third party arising out of a breach by you or any user of your account of these Terms, your violation of all applicable laws and regulations or third party rights, your fraud or other illegal acts, or your intentional misconduct or gross negligence, to the extent permitted by the applicable law.

# Entirely New Security Threat Vectors

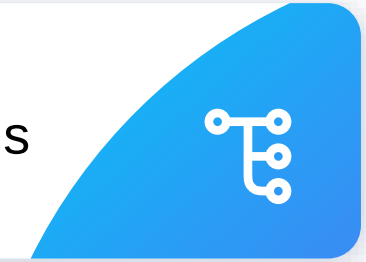
## New attack surfaces across the AI lifecycle

- Training data poisoning
- Model theft
- Untrusted inference infrastructure
- Data theft
- Uncertain model provenance
- Shadow AI
- Data leakage
- Model denial-of-service attacks
- Prompt injections
- Insecure tool calls

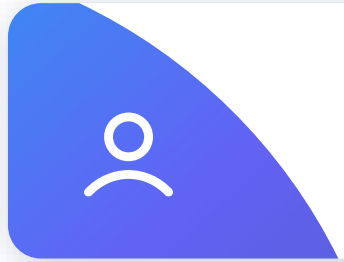

© 2025 Airia, LLC 

# AI Brand Risk

Biased Algorithms



Exposing PII



Low Quality Output

Significant questions about **how AI could impact public perception**

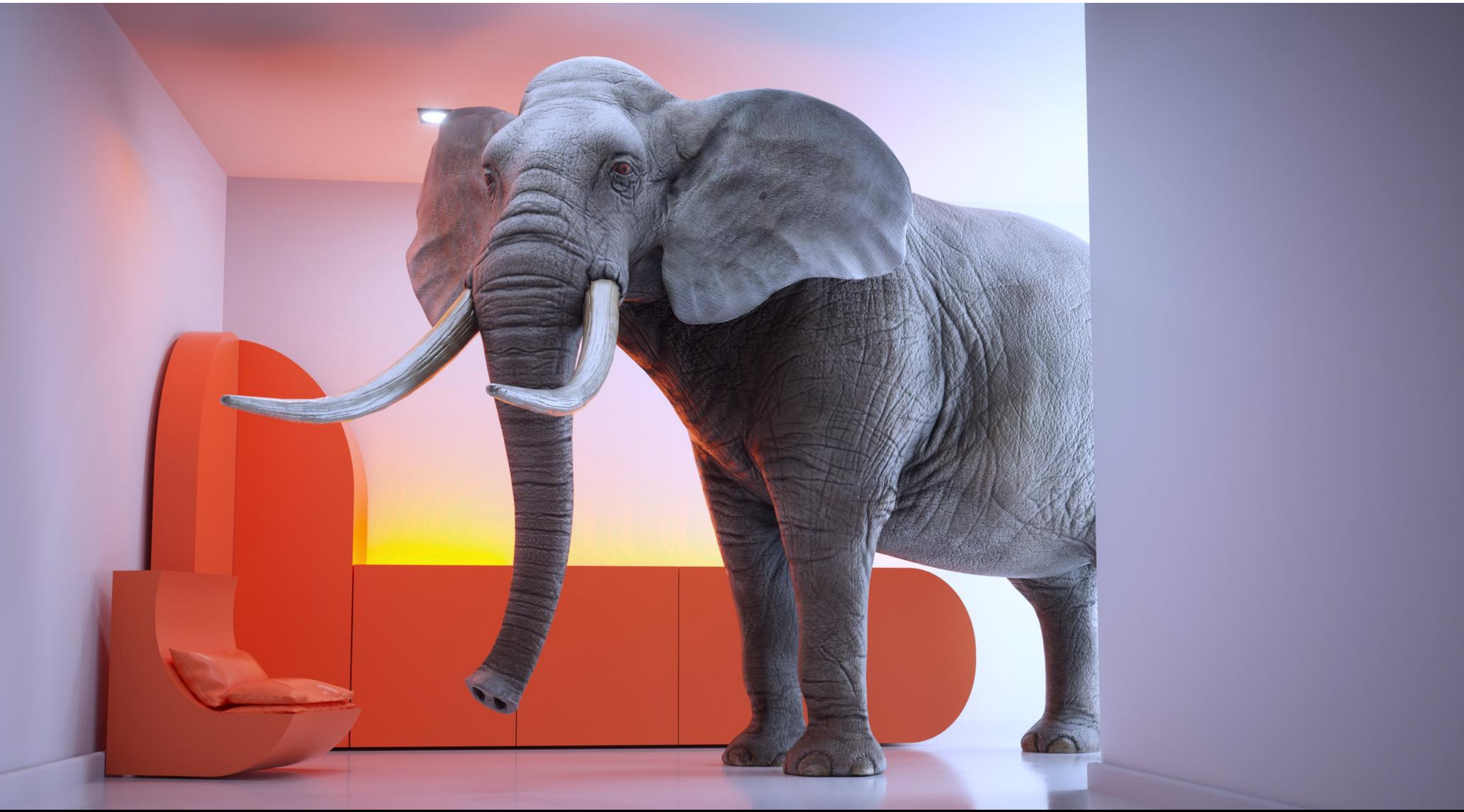
Insensitive Information

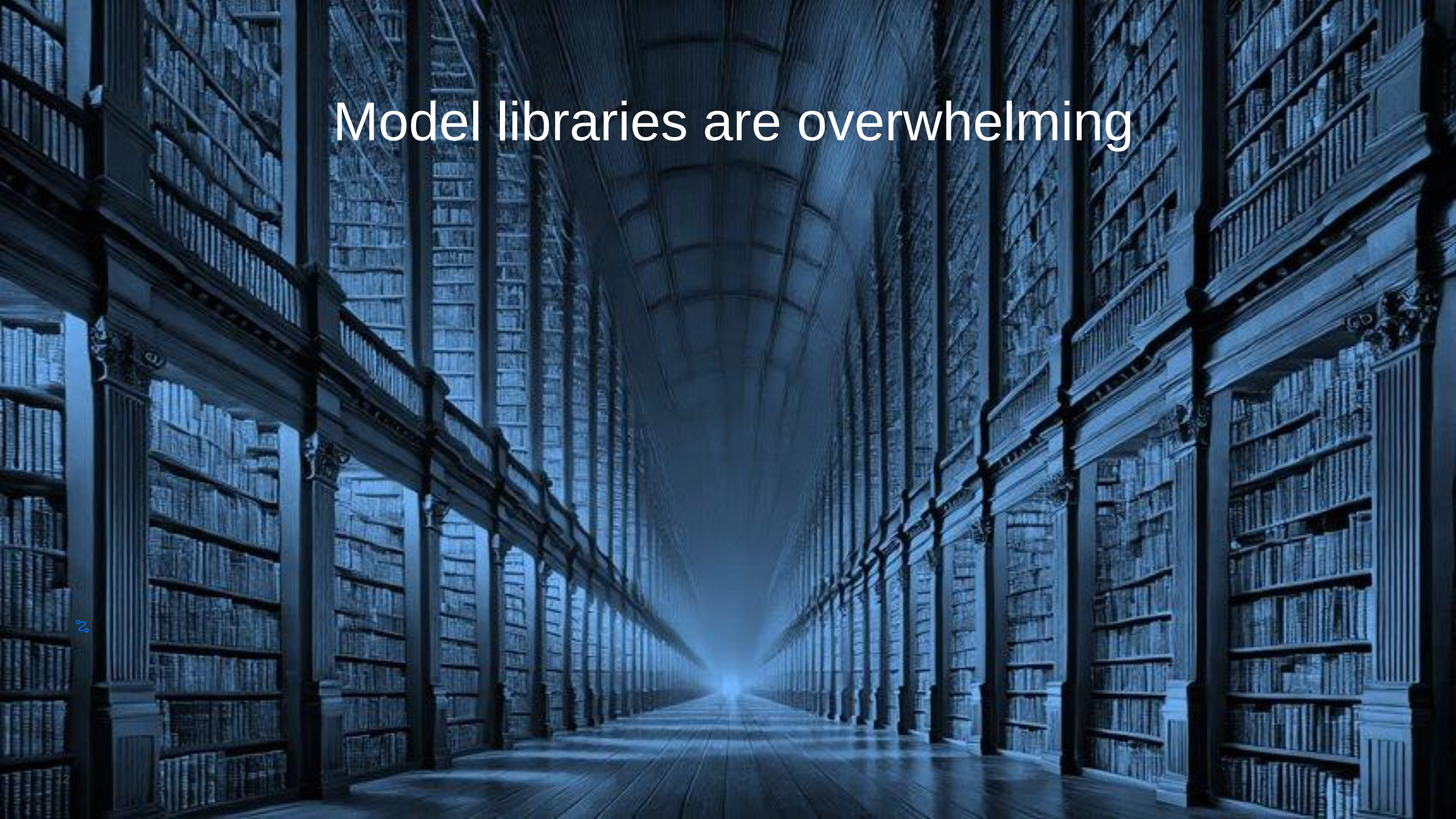
Misinformation in Training Data

Hallucinations



© 2025 Airia, LLC

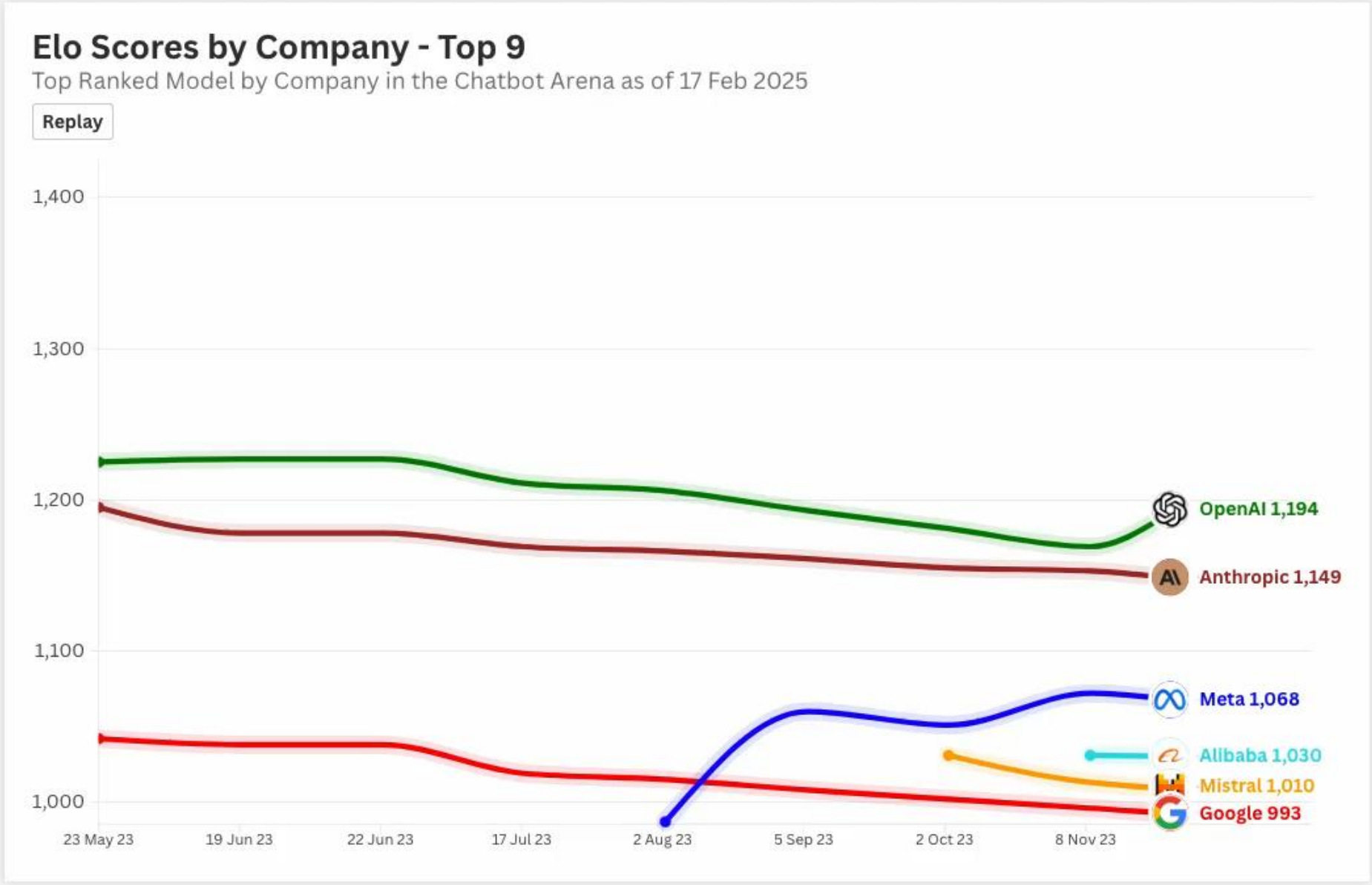



Model libraries are overwhelming

# Pace of Improvement is Accelerating

**Elo Scores by Top 9 Companies - 17 Feb 2025**

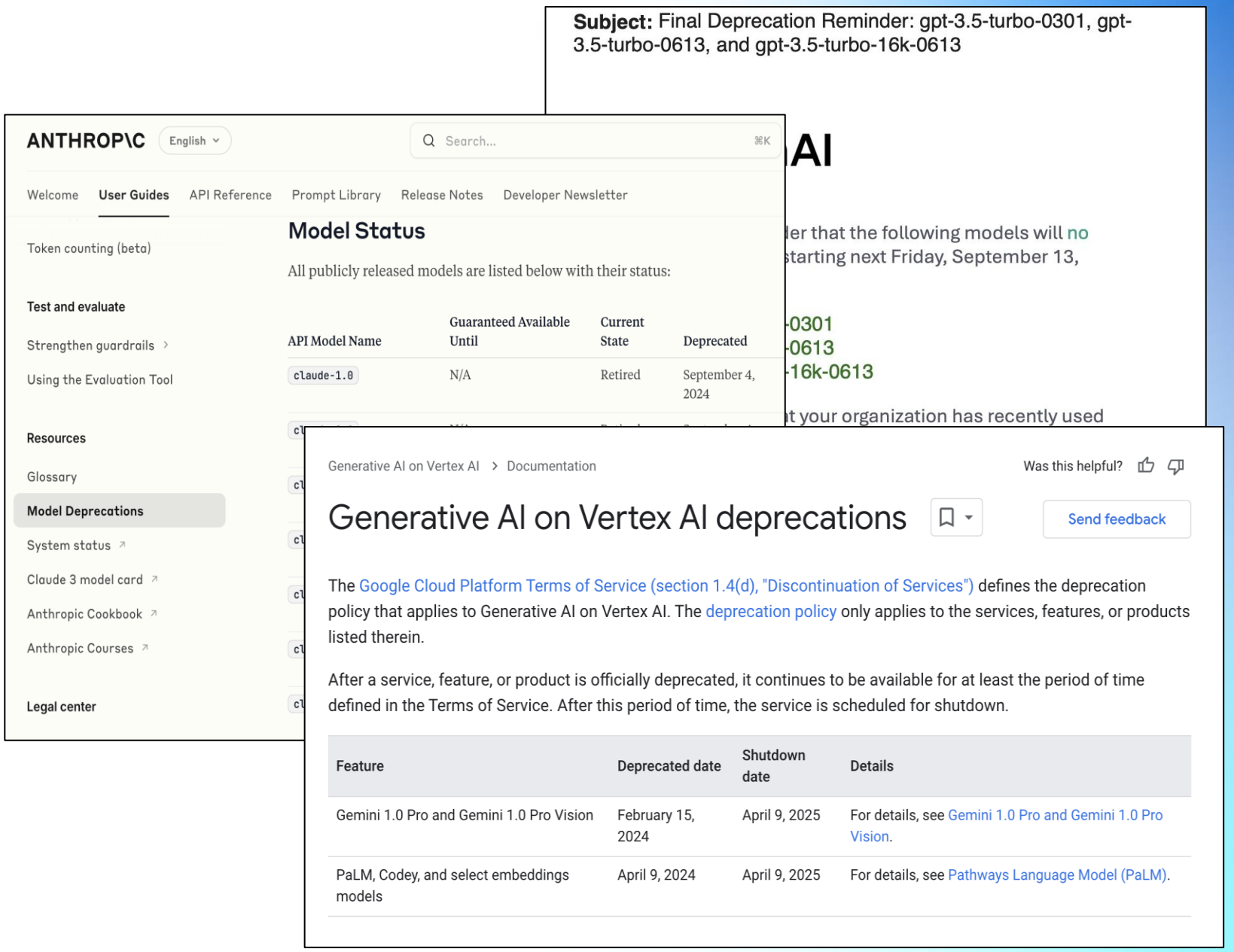
By Peter Gostev on 14 Feb 2025




TEMPLATE CREDITS

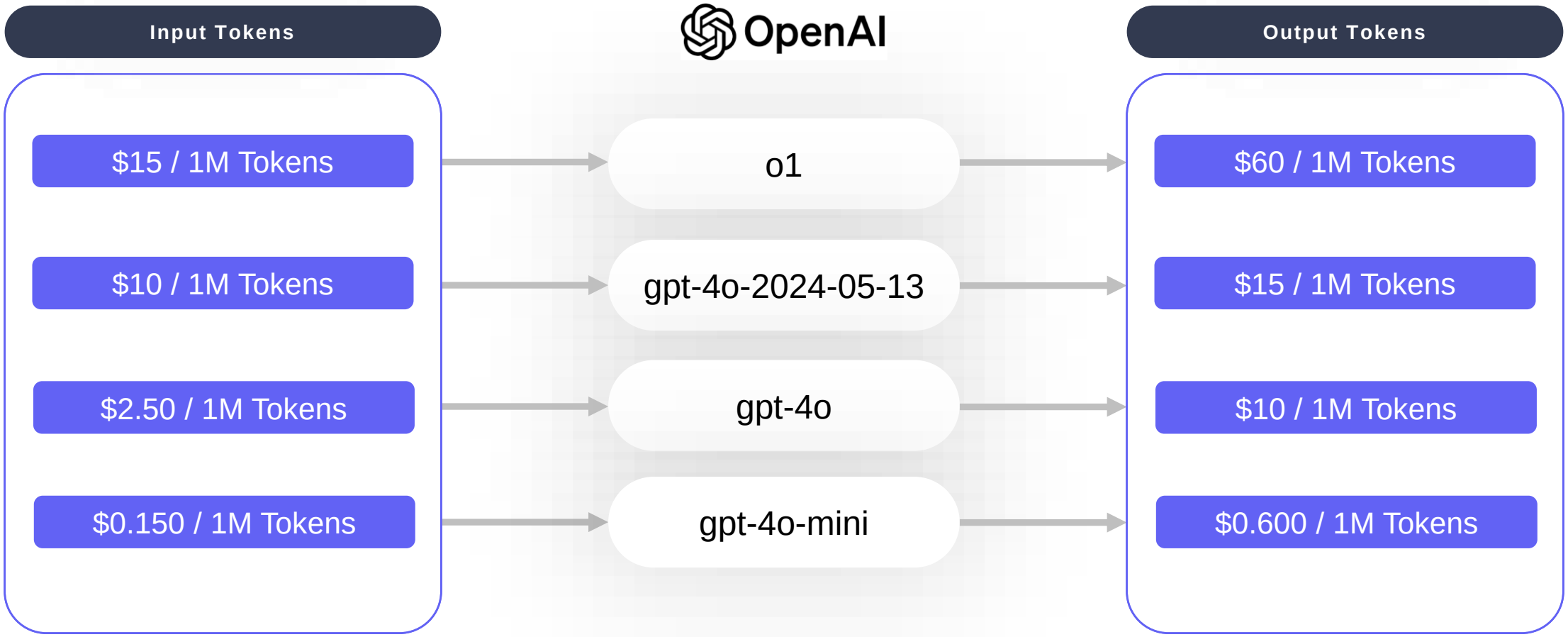
Line chart race by **Flourish teams**

# Rapid Deprecation of “Old” Models



# Significant Cost Differences

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





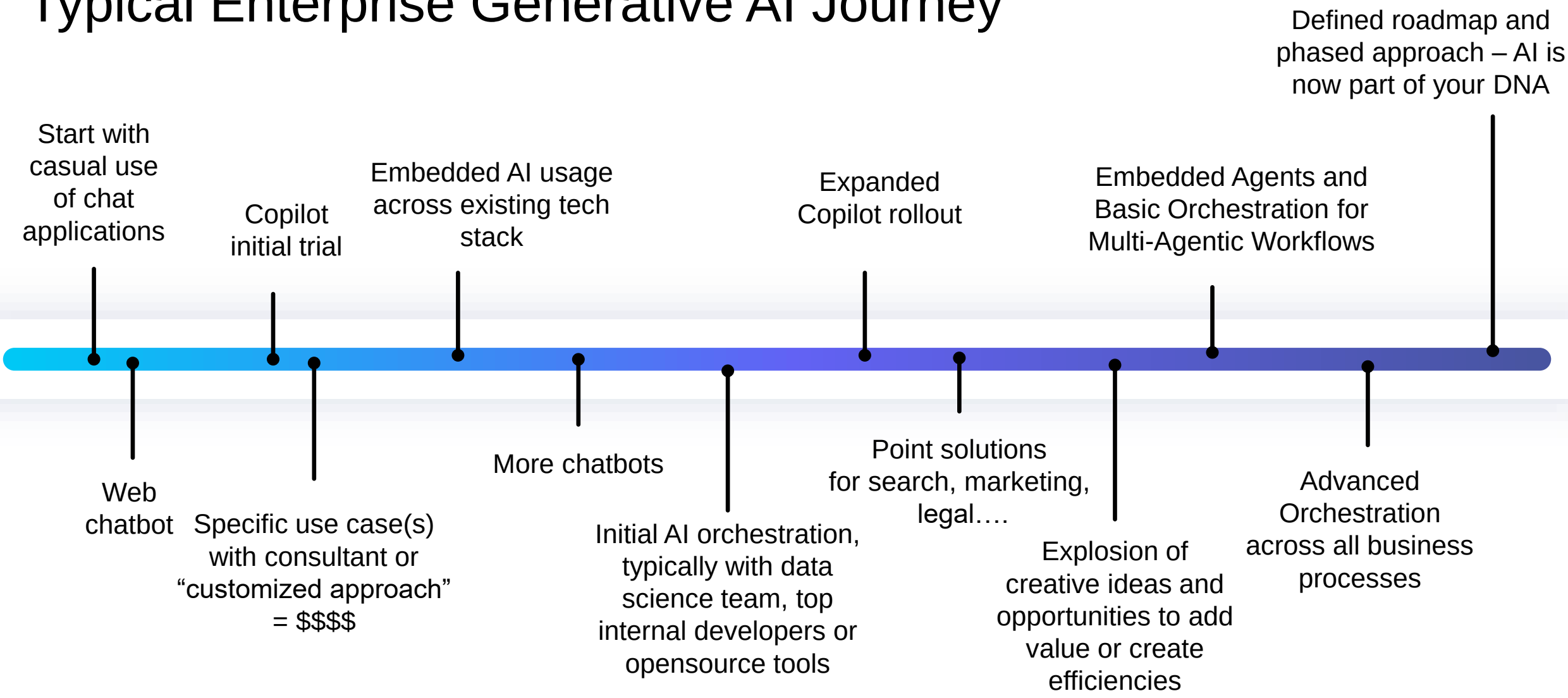
© 2025 Airia, LLC

# AI Speed Bumps to Realize Higher Value & ROI

- Implementation / Data Integration
- Cost
- Regulatory and Governance Challenges
- Security
- Legal and IP
- Brand and Reputational Risk

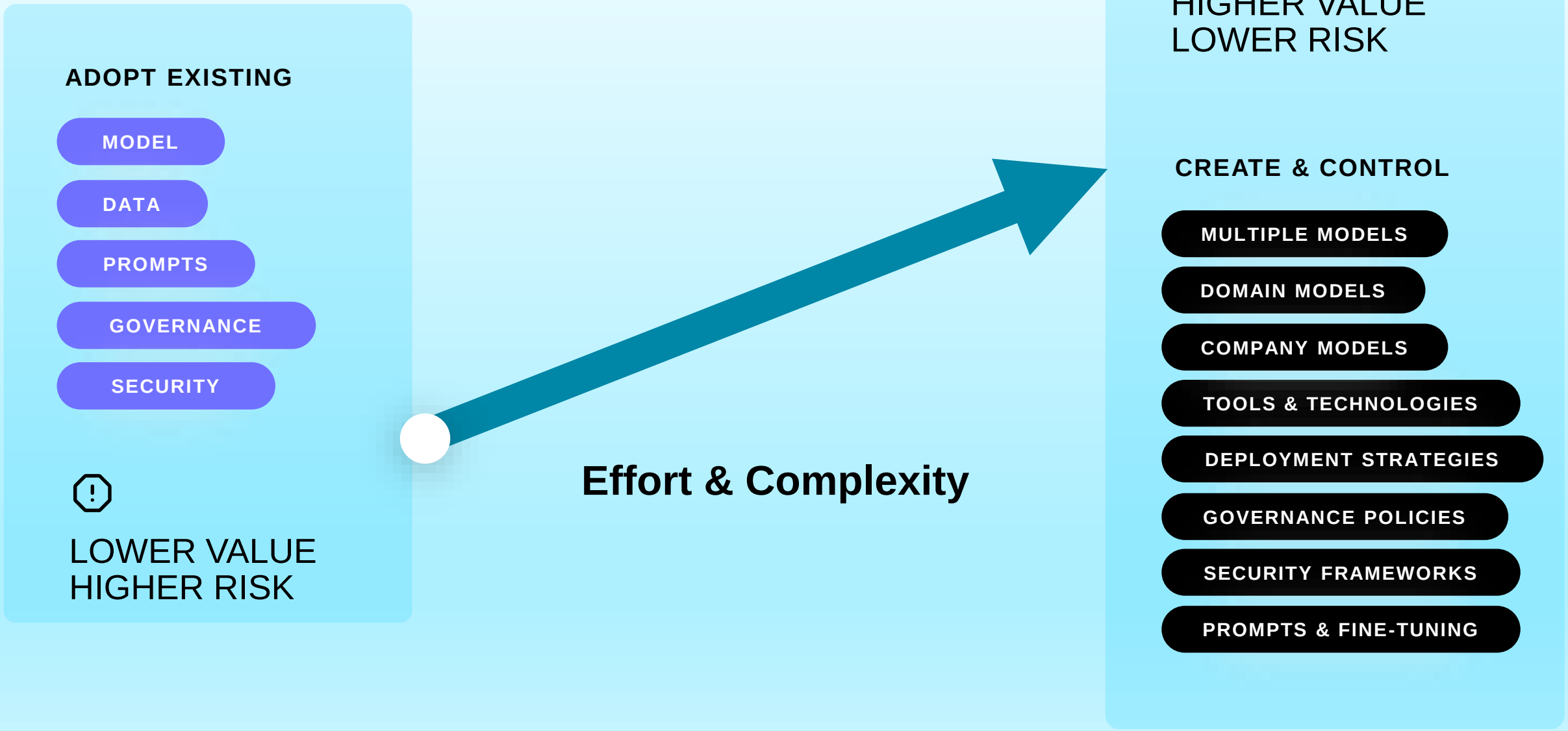
© 2025 Airia, LLC

# Typical Enterprise Generative AI Journey

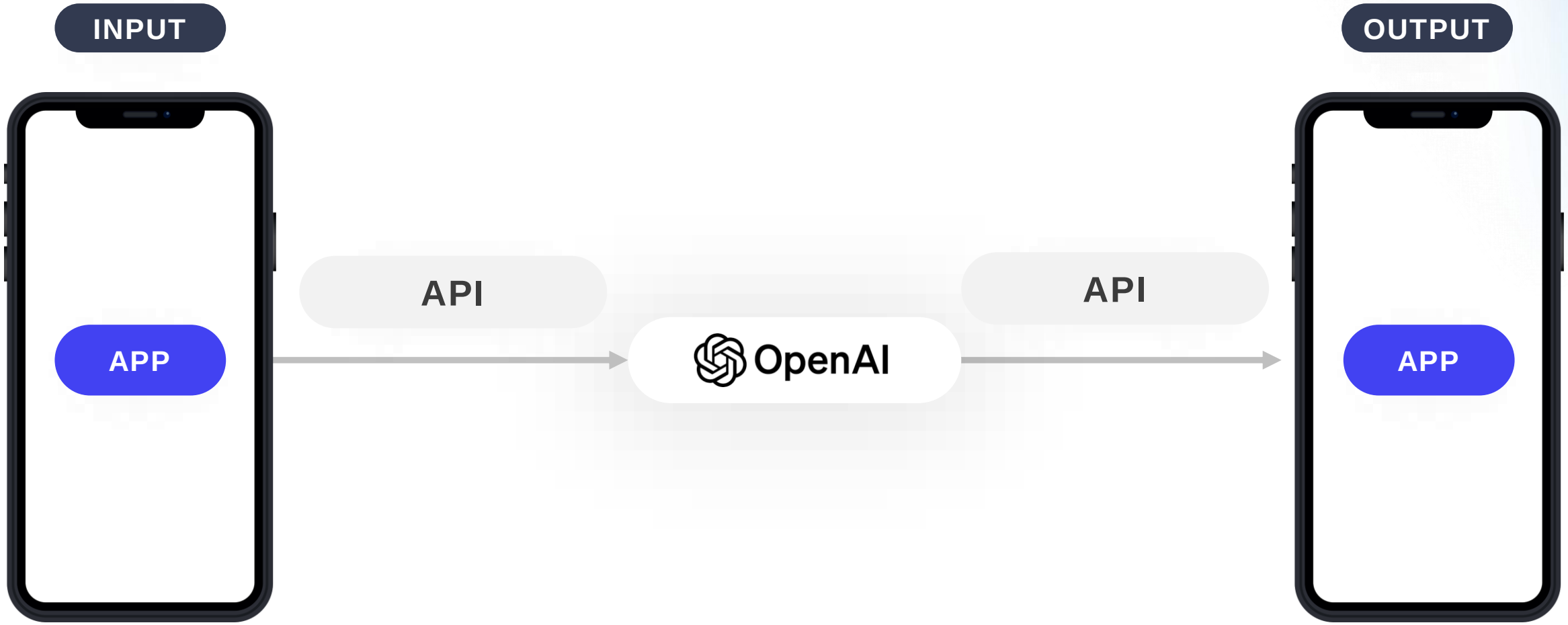



© 2025 Airia, LLC

# Building Agents to Create & Maximize AI Value



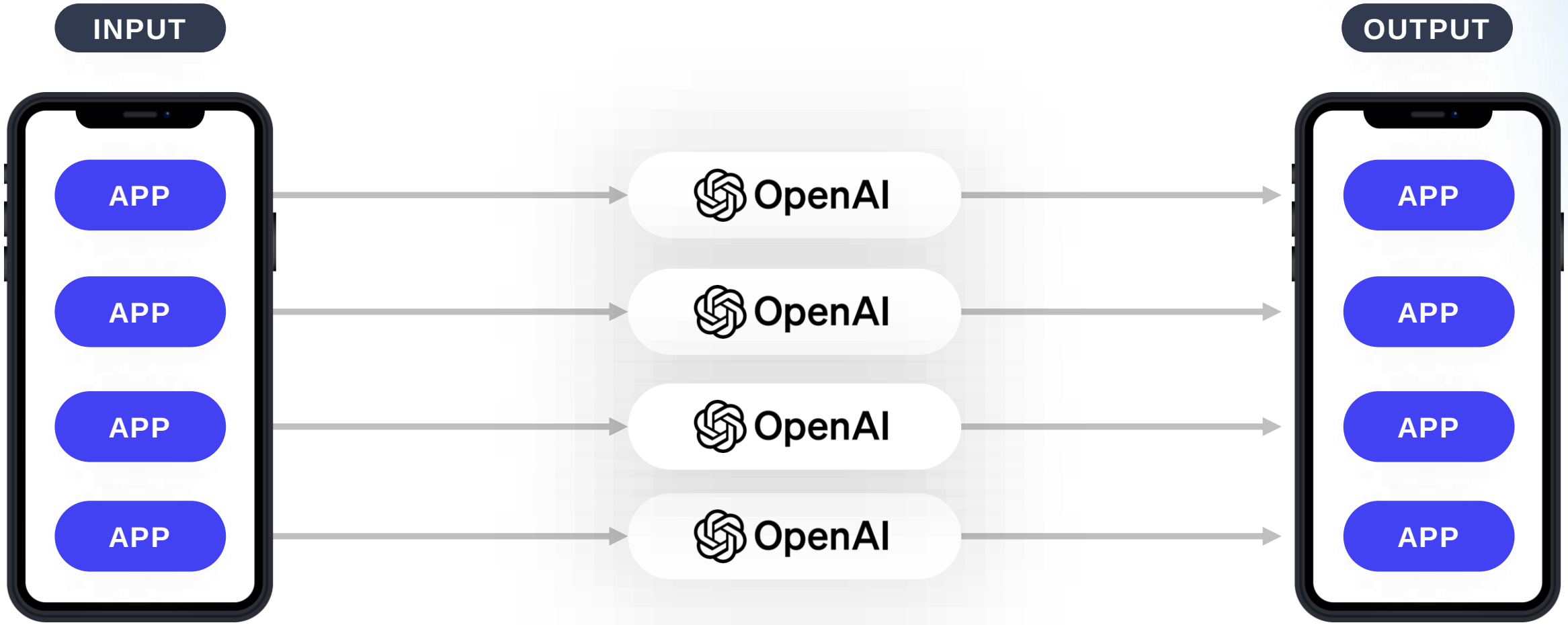
# A Common Starting Point





© 2025 Airia, LLC

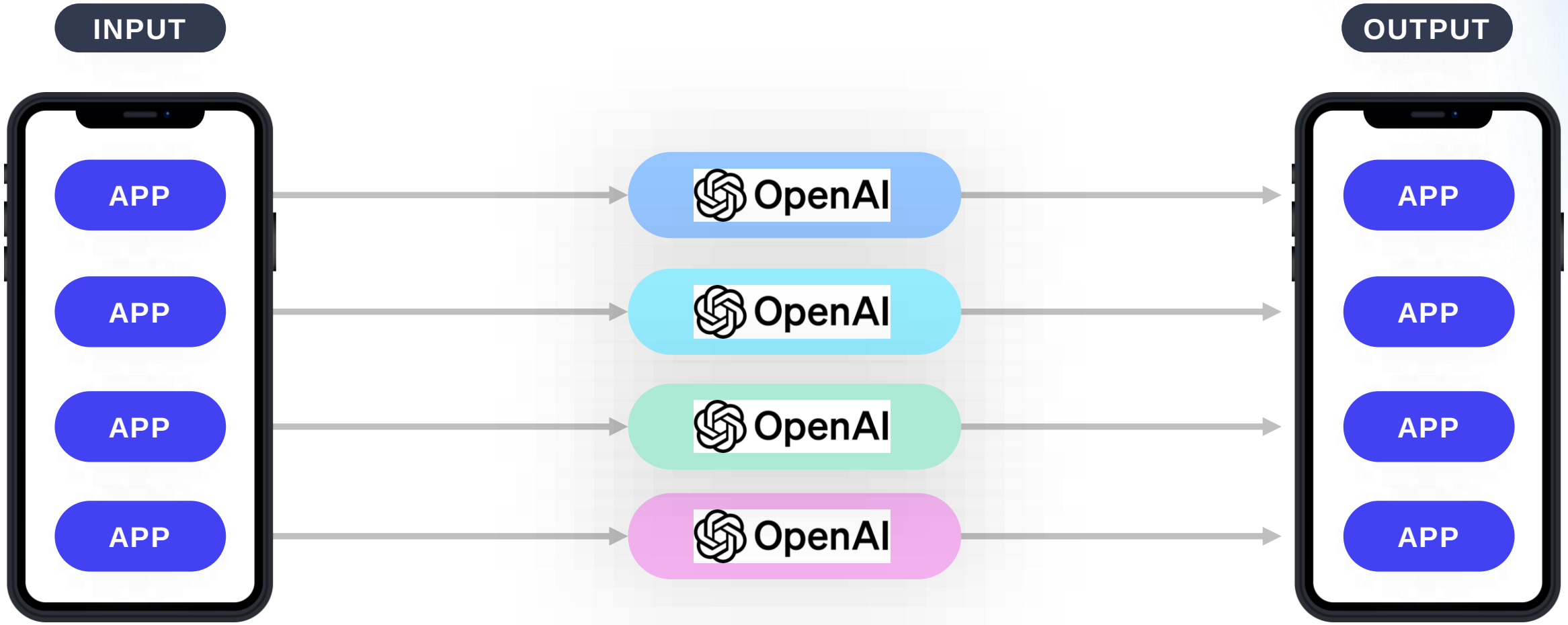
# Use Cases Expanded





© 2025 Airia, LLC

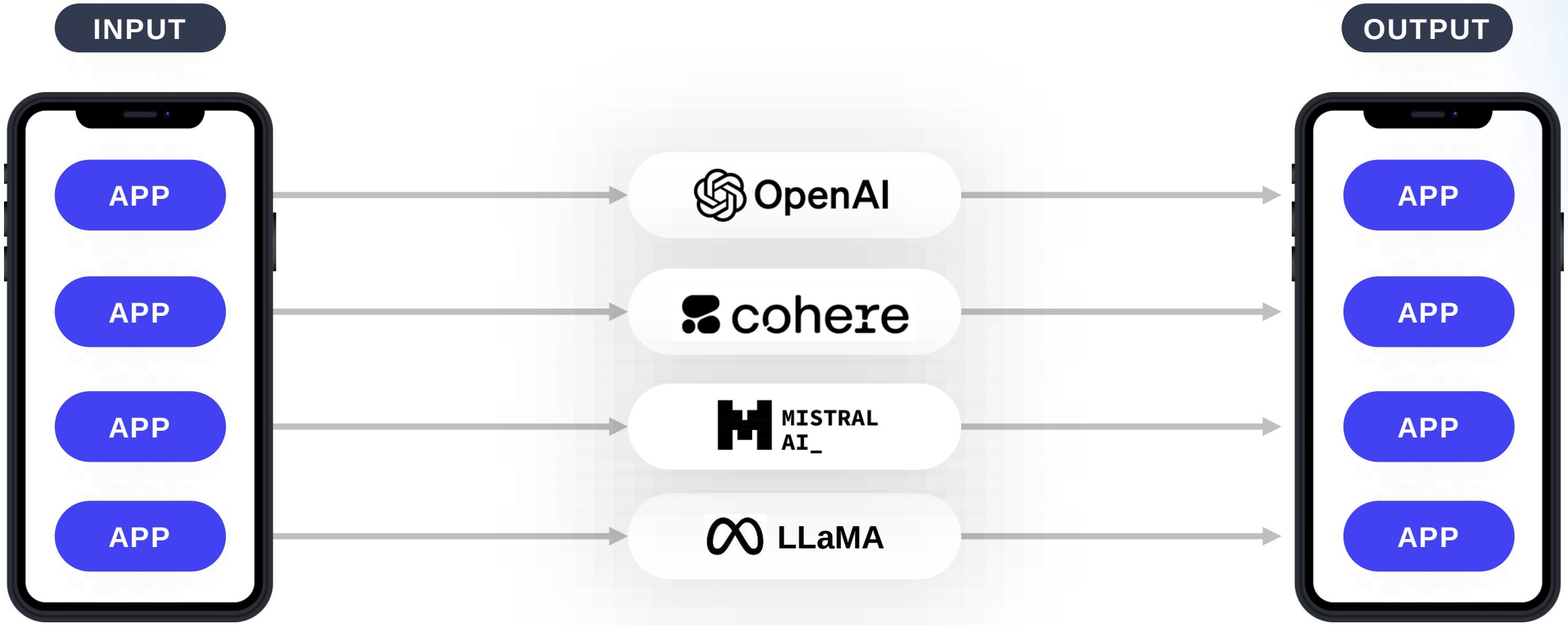
# Version Proliferation from LLMs





© 2025 Airia, LLC

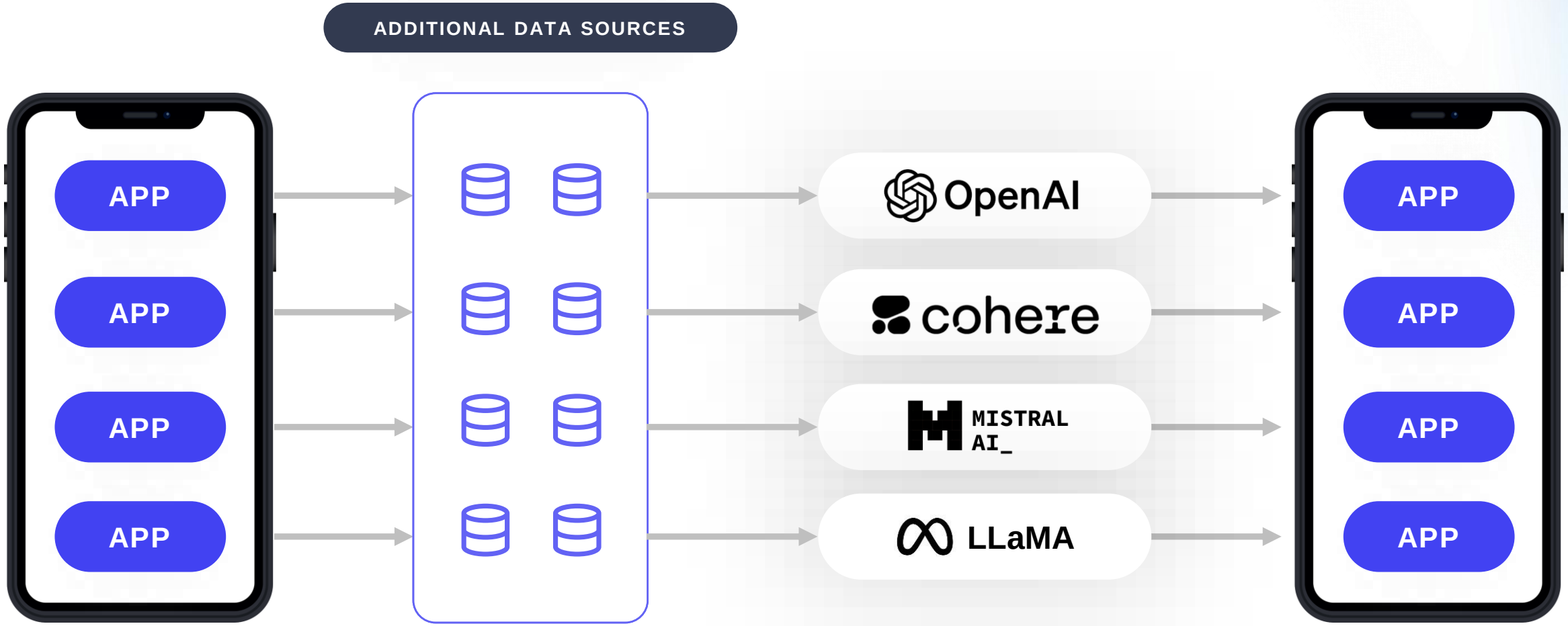
# Across Multiple LLMs





© 2025 Airia, LLC

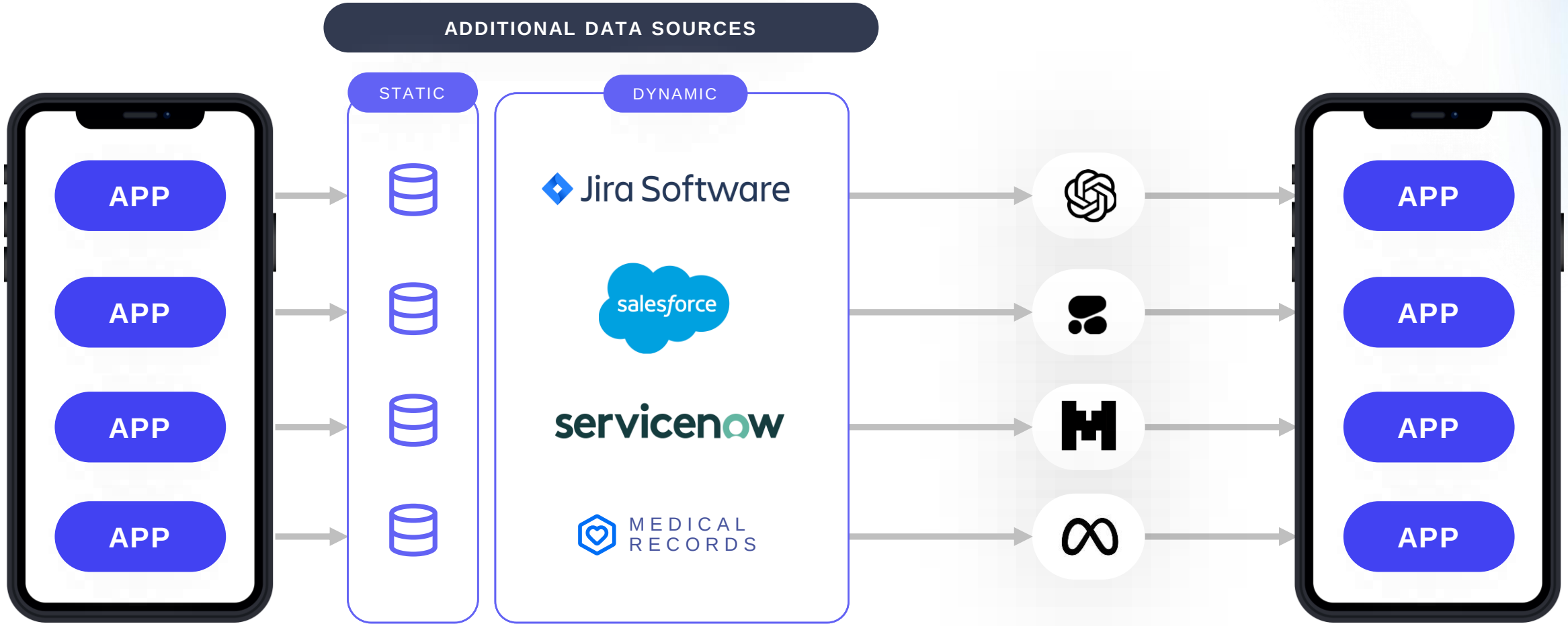
# Combined with Company Information





© 2025 Airia, LLC

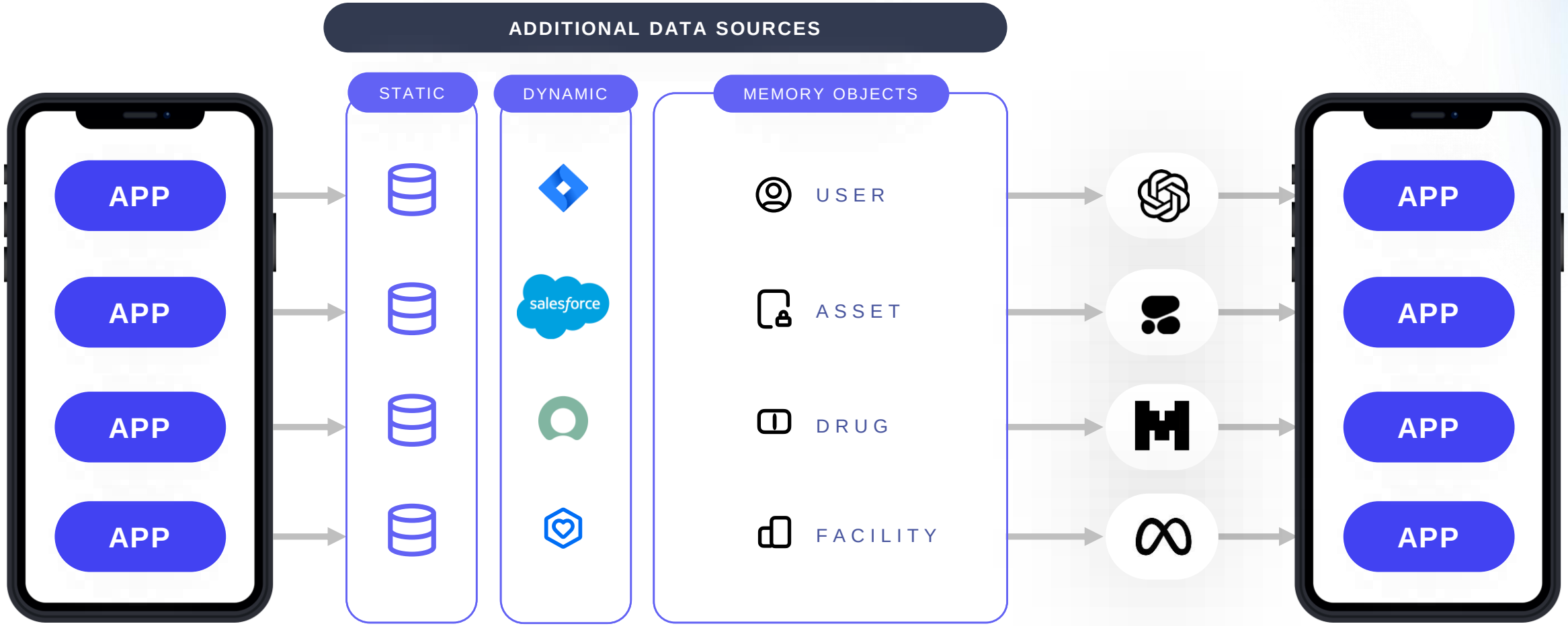
# Transactional Data





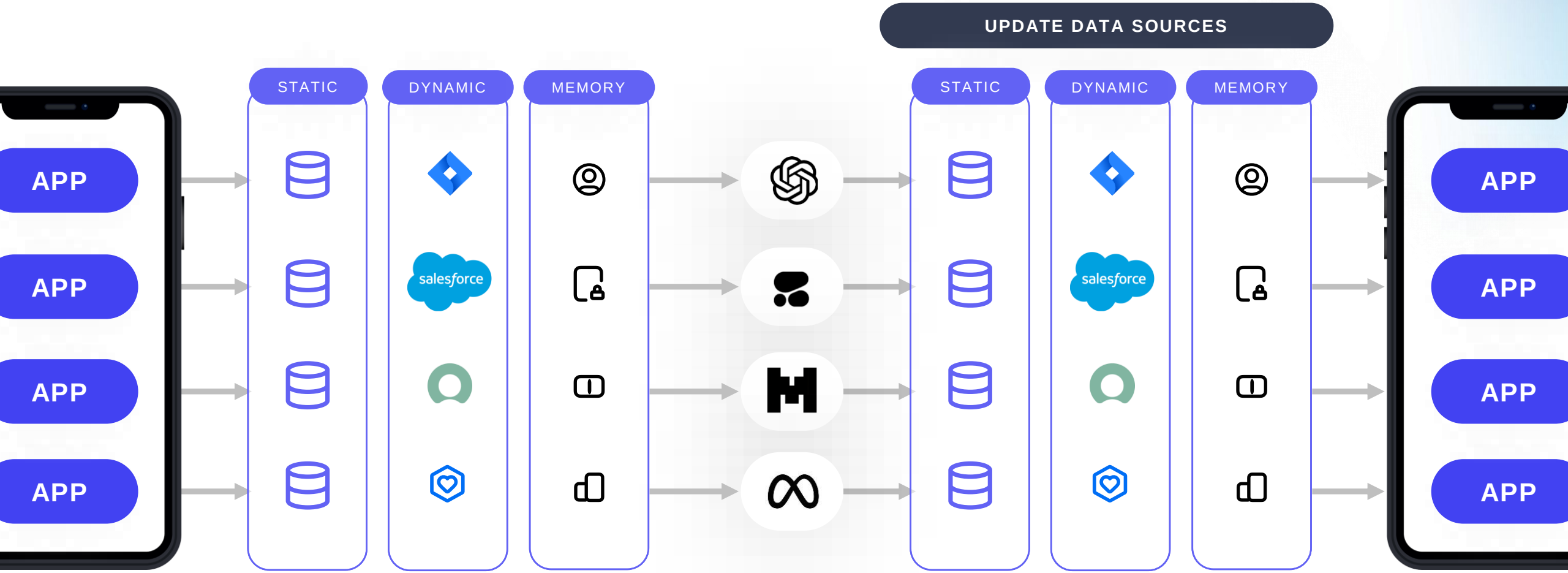
© 2025 Airia, LLC

# Plus Memory Objects





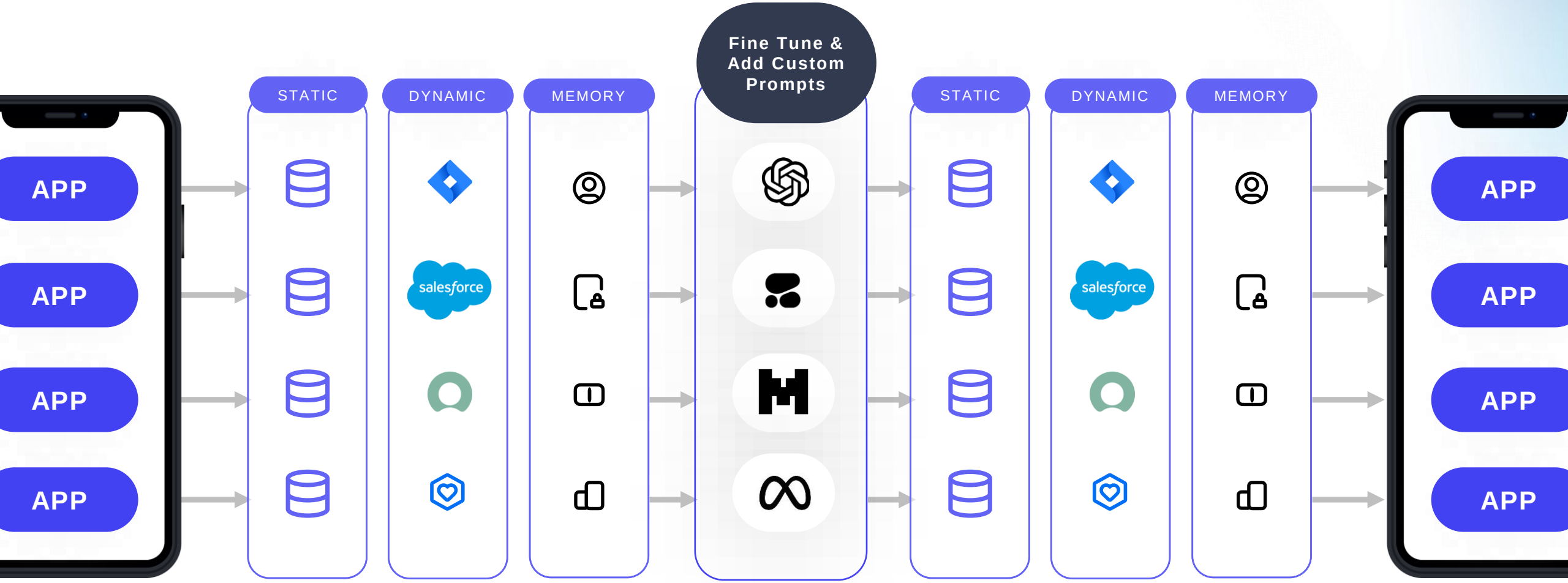
© 2025 Airia, LLC





© 2025 Airia, LLC

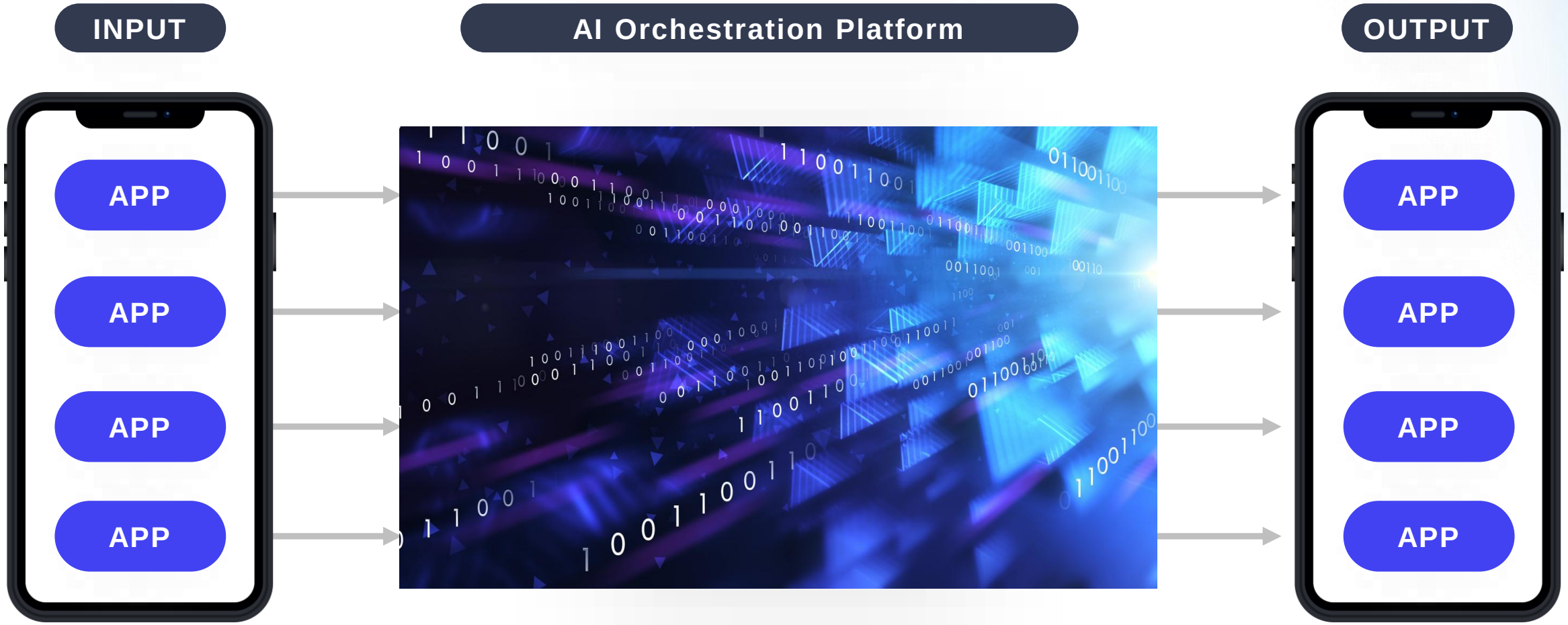
# Maximize Value with Prompts & Fine Tuning





© 2025 Airia, LLC

# Abstract Operational Complexity for Success



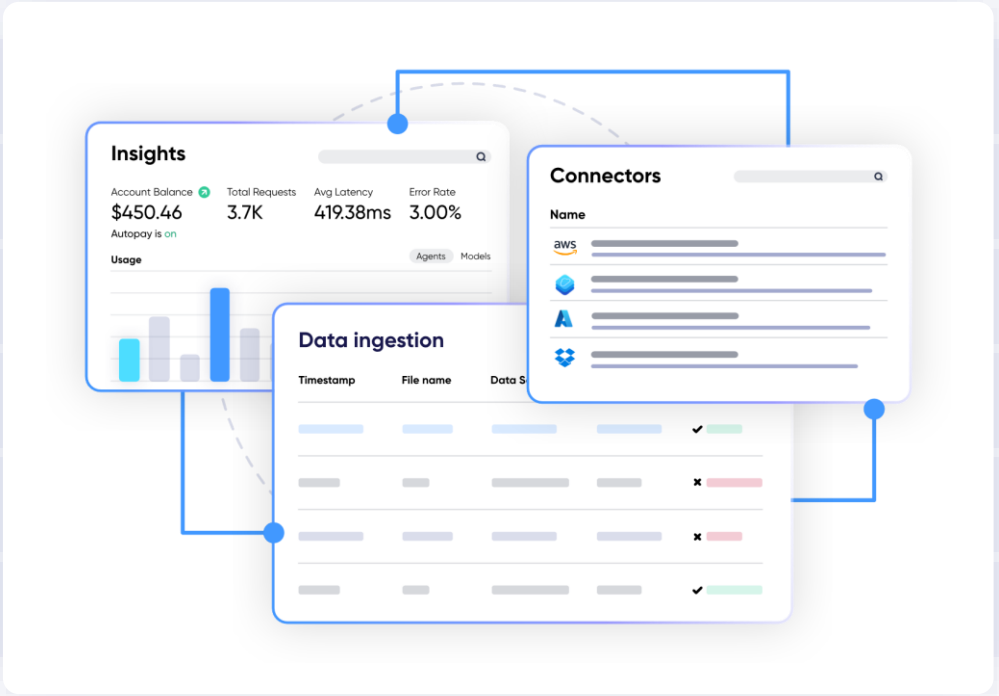


© 2025 Airia, LLC

# Enterprise AI Platform

## Accelerate and secure AI deployments with a comprehensive platform

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

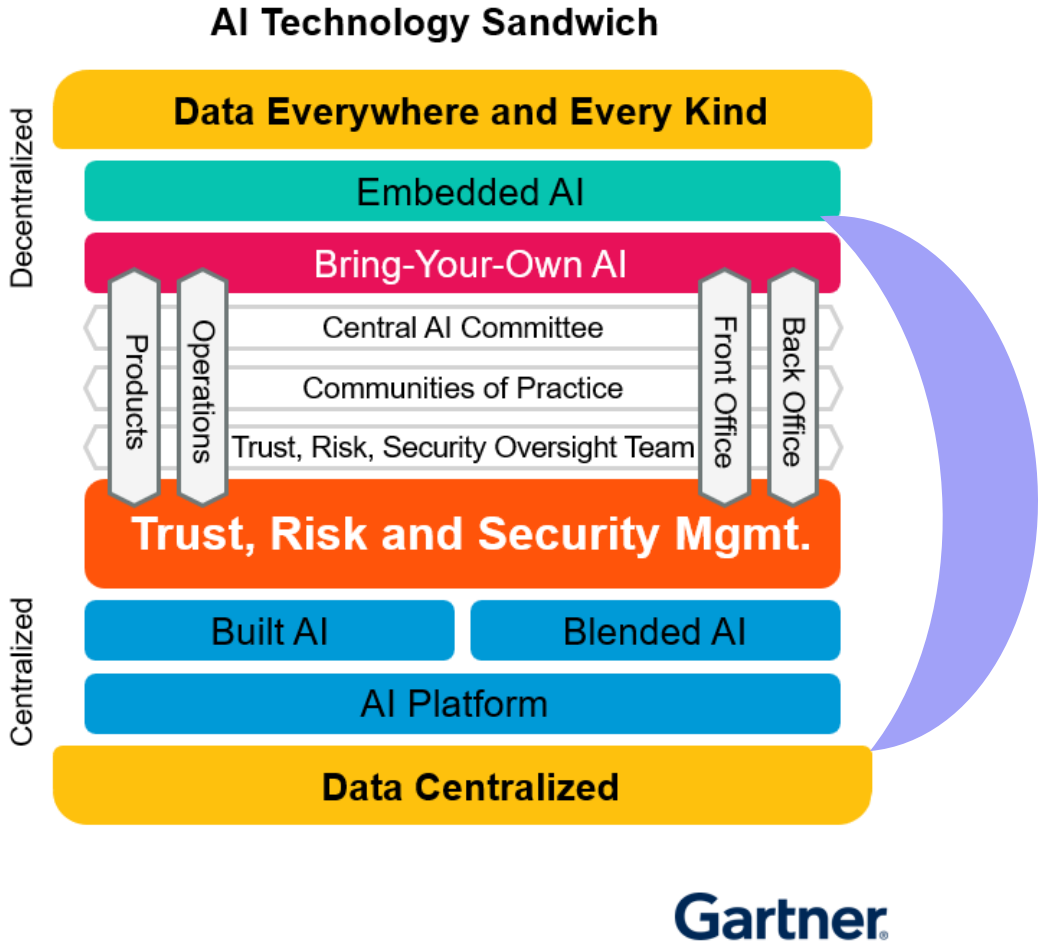



- Observability
- Orchestration
- Prototype & Testing
- Prompt Studio
- Prompt Management
- Security & Governance

**Data Integration** | **Enterprise Security** | **Responsible AI** | **Deployment Options**

airia

© 2025 Airia, LLC

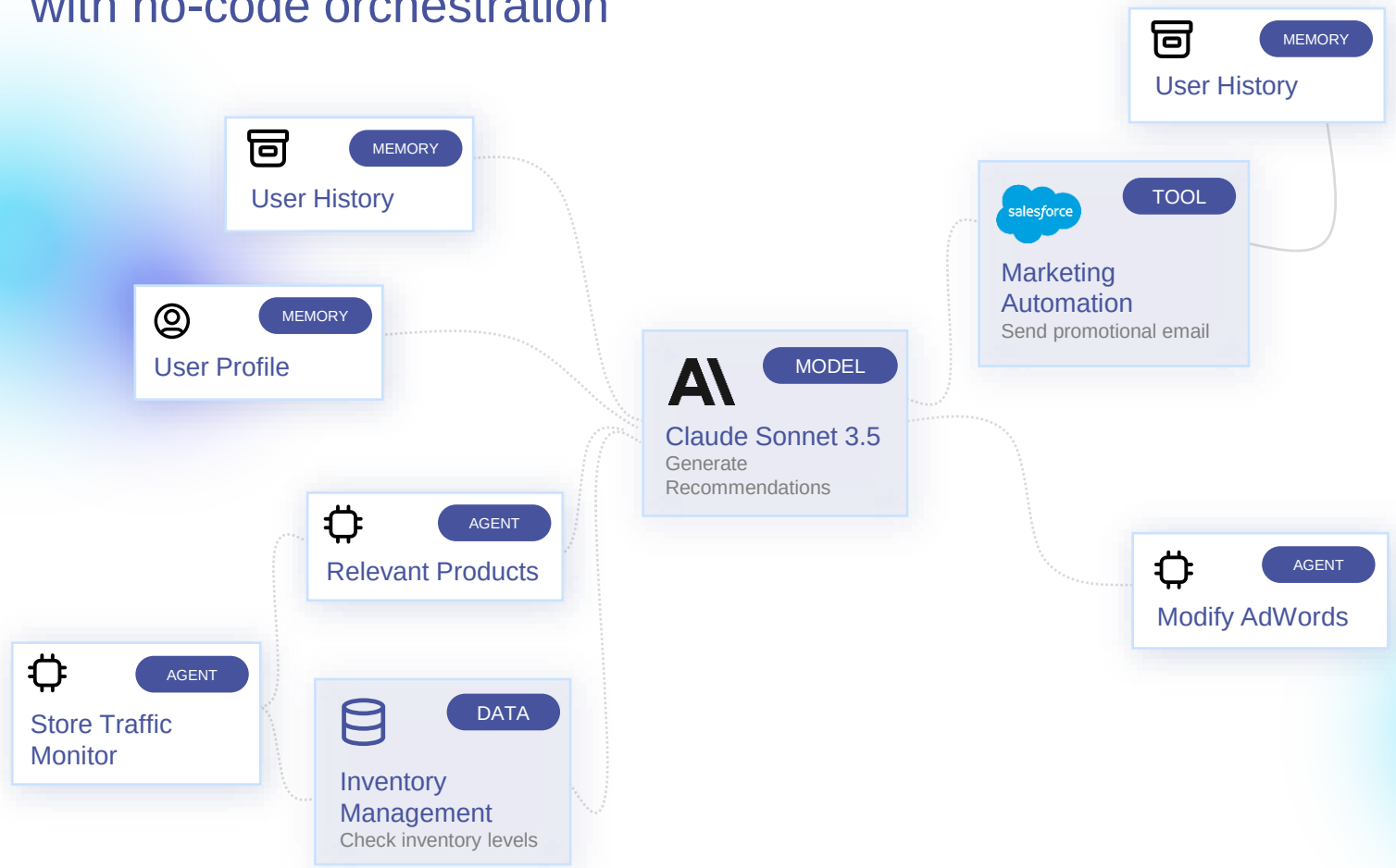


Gartner®, AI Technology Sandwich: A Conceptual Framework for Executing AI, 21 October 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

airia

# AI Agent Orchestration

## Seamlessly build and deploy AI Agents with no-code orchestration




### Seamless Orchestration

- Choose from leading AI models
- Build in drag-and-drop interface
- Combine models, data, apps & actions
- Retrieve and update dynamic data across 1000+ enterprise apps

### Build Agentic Workflows

- Manage the sequence and timing of various stages of AI Agents
- Built truly agentic workflows by teaming Agents to solve problems or generate content on their won

### Gain Performance Insights

- Monitor performance of AI models
- Manage model costs and utilization
- Monitor API call performance
- Maintain detailed audit logs

airia

© 2024 Airia, LLC 

# New Agent Libraries & Communities for **Enterprises**

## Human Resources

- Talent Acquisition
- Employee HR Assistant
- HR Communications
- Compensation and Benefits

## Sales

- Sales Forecasting
- Customer Churn Prediction
- Lead Scoring
- Sales Training Assistant

## Marketing

- Marketing Copywriter
- SEO Recommendations
- Product Recommendations
- Customer Segmentation

## Finance

- Invoice Processing
- Corporate Policy Updates
- Fraud Detection
- Spend Analysis

## Legal

- Contract Document Search
- Compare & Redline
- Summarize Contracts
- Patent Drafting

## Engineering

- Code Review
- Documentation Creation
- Automated Testing
- Feature Prioritization

## IT Security

- RFI Respondent
- Security Questionnaire
- Privacy Questionnaires
- Policy Search

## Customer Service

- Sentiment Analysis
- Support Chat Assistant
- SOW Creation
- Knowledgebase Articles


© 2025 Airia, LLC

# Build Agents in Minutes

© 2025 Airia, LLC 

# Assistants

Select an assistant to chat and engage with your files in real-time.
Ask questions, get insights, and interact with your docs.

Search assistants...

Request Assistant

All | Recommended | Favorites

Category: All Categories

### An Engineering Search
General
An Agent That Will Search Across Jira And Confluence For Tickets Or Articles On The Requested Topic

### Annie your Analyst Assistant
Sales Ops | Analyst Relations
An Agent To Help You Understand What The Analyst Reports Are Saying

### Ask Airia
Everyone
An Agent To Use Via Chat Or Slack To Ask Questions

### Charlotte the Chef
AI Friends
Cook Up Some Conversation With Charlotte The Chef!

### Chat
Chat | Everyone
A ChatGPT Chat Agent, With Memory Objects Enabled

### Chat with Afraz Jaffri
Analyst Relations
This Is An Agent That Will Let You Chat With Afraz Jaffri

### Chat with Akanksha Bansal
Analyst Relations
This Is An Agent That Will Let You Chat With Akanksha Bansal

### Chat with Alastair Woolcock
Analyst Relations
This Is An Agent That Will Let You Chat With Alastair Woolcock

### Chat with Alys Woodward
General
This Is An Agent That Will Let You Chat With Alys Woodward

### Chat with Annette Zimmermann
Analyst Relations
This Is An Agent That Will Let You Chat With Annette Zimmermann

### Chat with Anthony Mullen
Analyst Relations
This Is An Agent That Will Let You Chat With Anthony Mullen

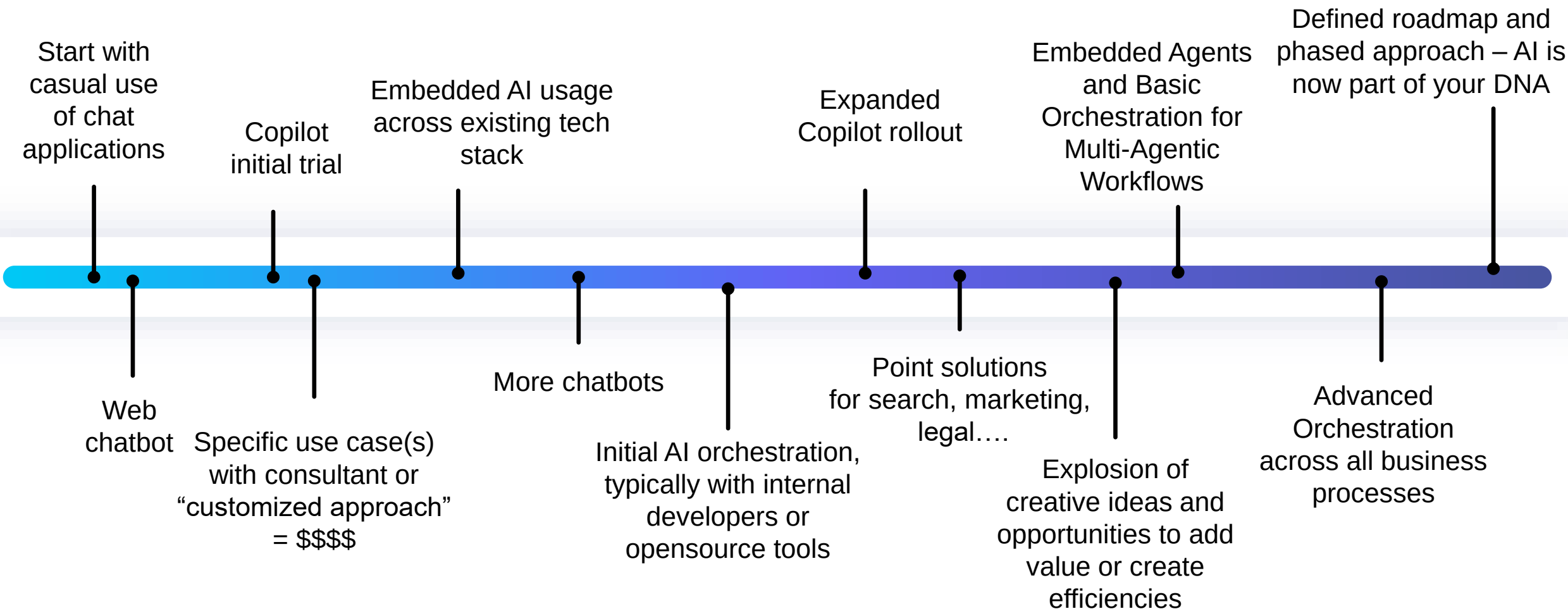
### Chat with Arun Batchu
Analyst Relations
This Is An Agent That Will Let You Chat With Arun Batchu

### Chat with Arun Chandrasekaran
Analyst Relations
This Is An Agent That Will Let You Chat With Arun Chandrasekaran

### Chat with Aura Popa
Analyst Relations
This Is An Agent That Will Let You Chat With Aura Popa

### Chat with Avivah Litan
Analyst Relations
This Is An Agent That Will Let You Chat With Avivah Litan

# Typical Enterprise AI Journey

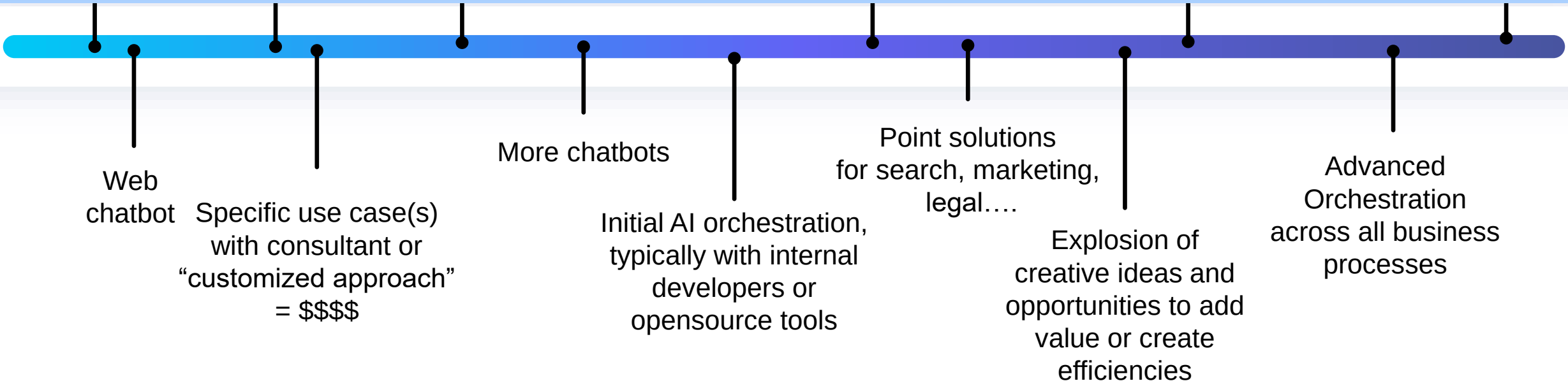



airia

© 2025 Airia, LLC

# Future Agentic Landscape – Agents are the new APIs

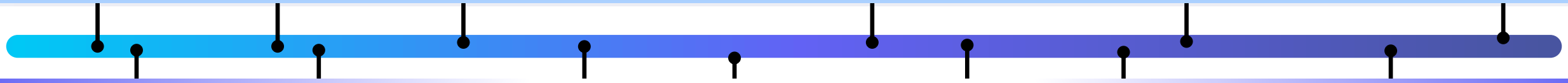
## Existing Tech Stack – AI Enabled & Mature




© 2025 Airia, LLC

# Future Agentic Landscape – Agents are the new APIs

## Existing Tech Stack – AI Enabled & Mature



## Consolidated New AI Tech Stack
## Rationalized Investments for Use Case, Security and Orchestration Apps

© 2025 Airia, LLC

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


© 2025 Airia, LLC 

Now, it’s not just your data.

**It’s your AI**

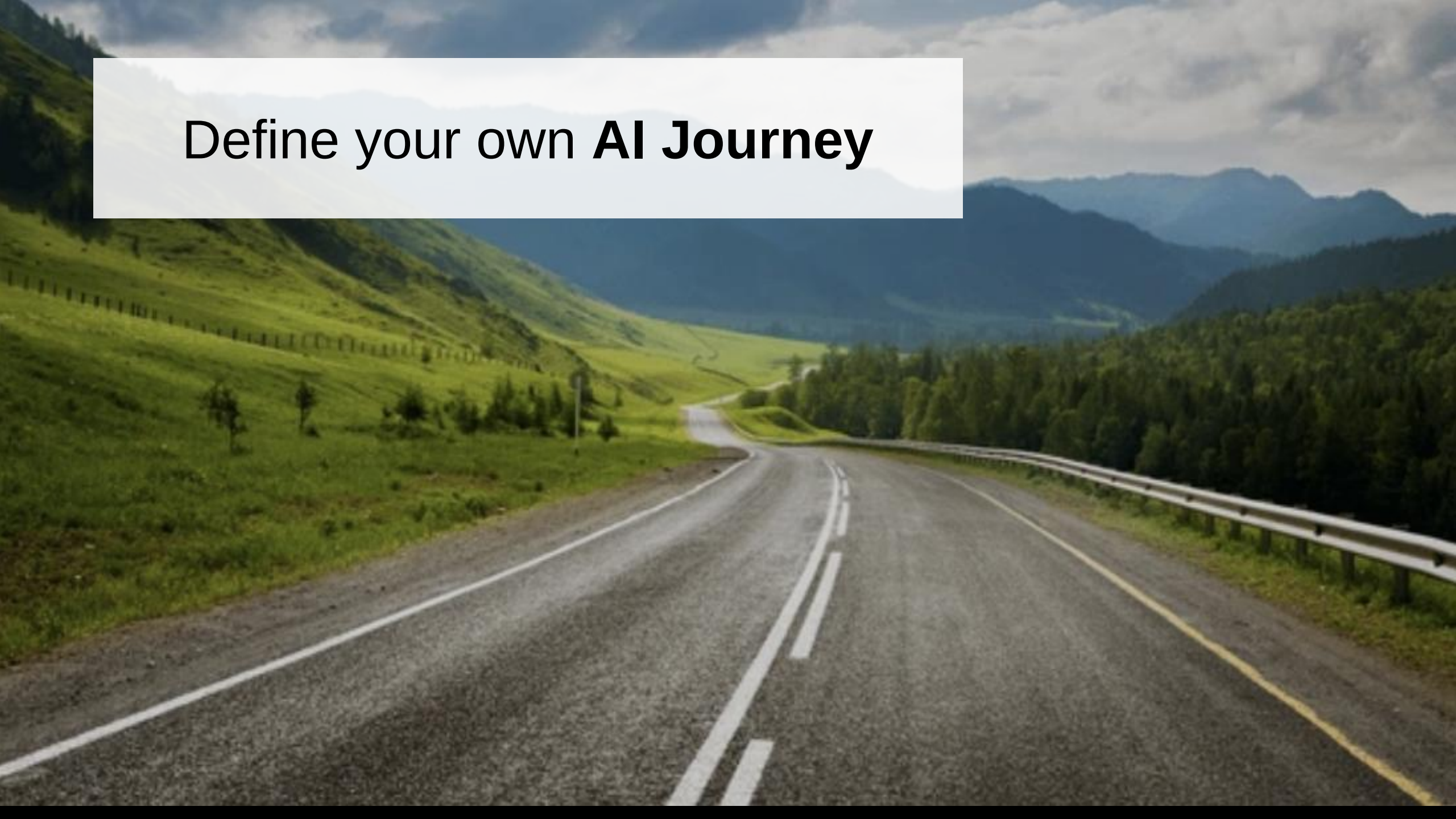
© 2025 Airia, LLC 

Now, it’s not just your data.

**It’s your AI { Strategy & Platform }**



© 2025 Airia, LLC 


Define your own **AI Journey**

# Contact Airia

© 2025 Airia, LLC 