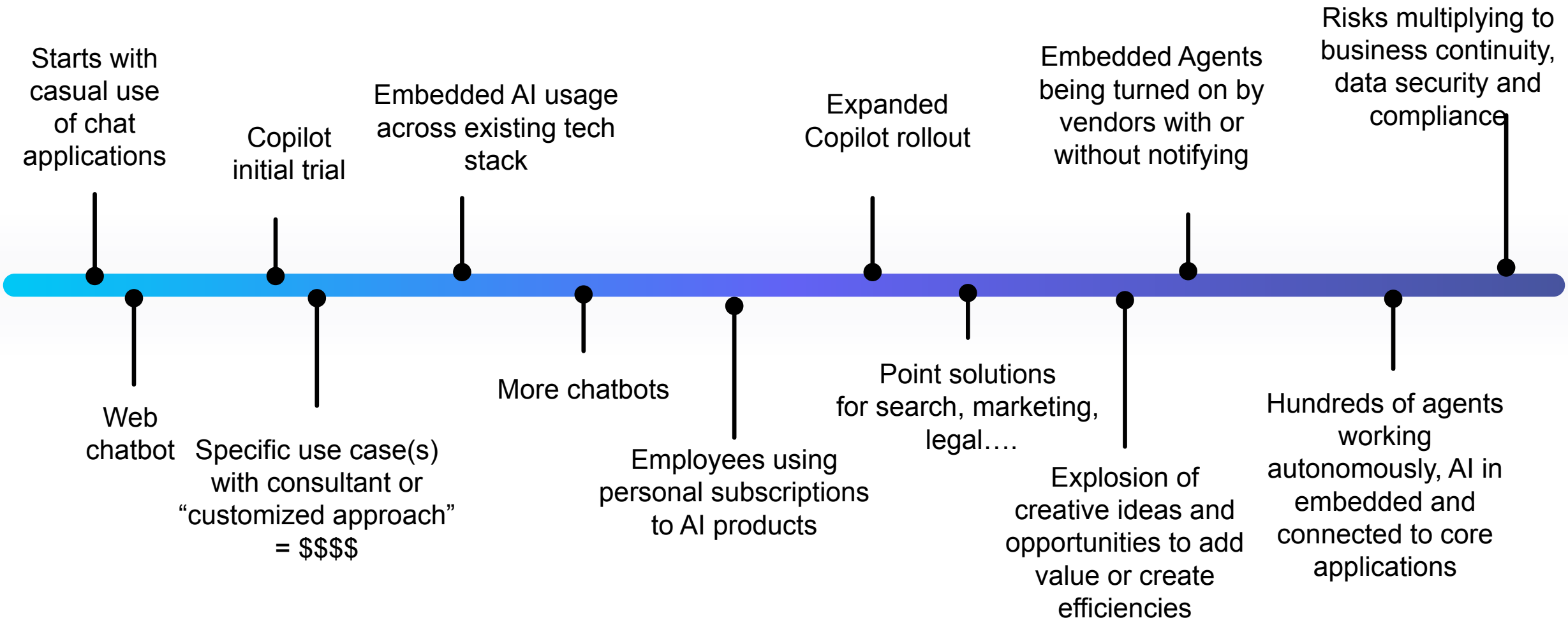
AI Sprawl is Happening Now
The Urgent and Growing Risks to Address

NITHISH RAJAN

HEAD OF SOLUTIONS

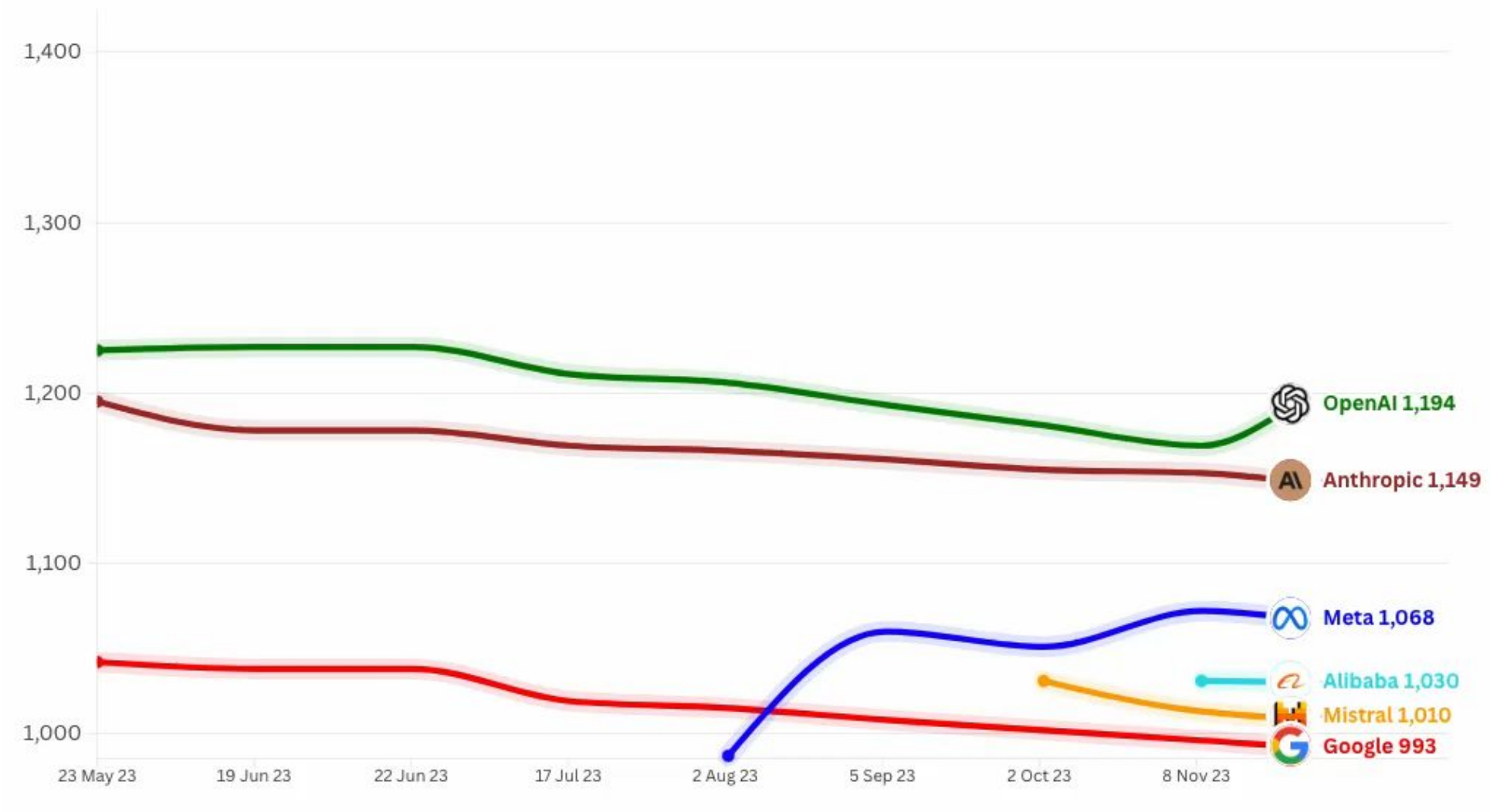
DECEMBER 9, 2025

Typical Enterprise AI Journey

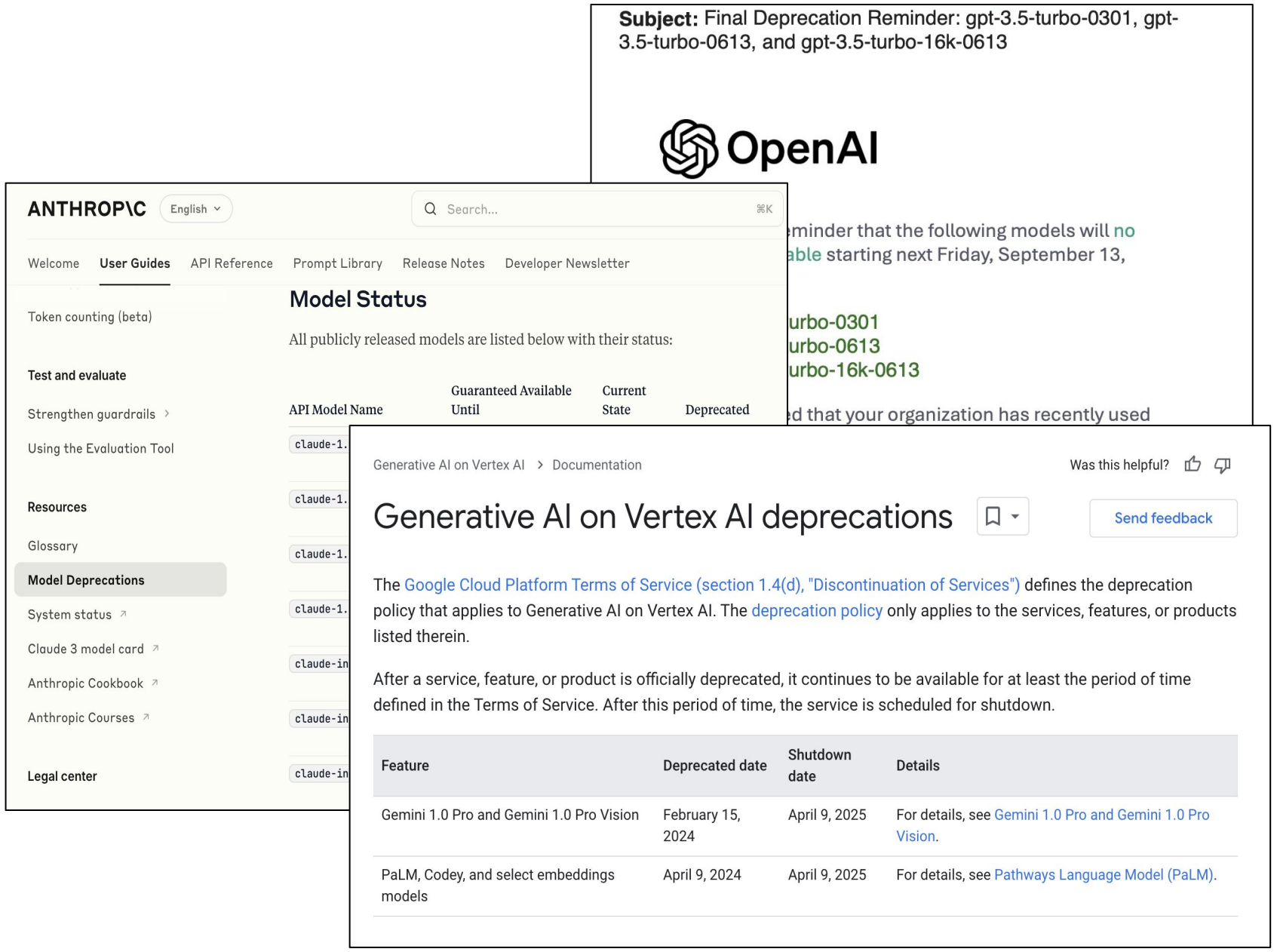


airia

AI proliferation will outpace your ability to manage, secure and govern it



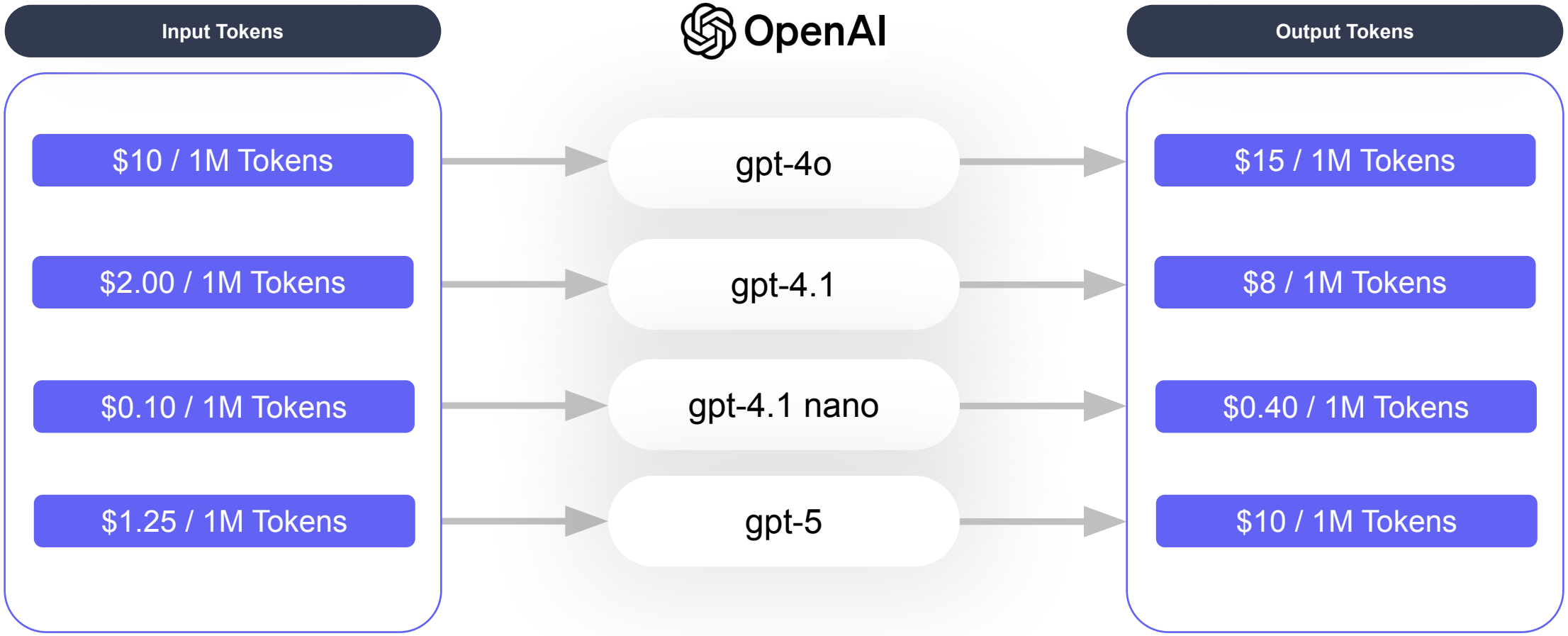
Rapid Deprecation of “Old” Models



airia

Cost Differences Becoming Significant

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




Business Continuity

AI Dependence Creates New Risks

Mashable

ChatGPT, Sora down: OpenAI confirms partial outage

Tech > Tech news

CHAT'S OFF ChatGPT DOWN as users report mysterious outage that stops bot from responding

Owners OpenAI has launched an investigation into the problem

Jamie Harris, Assistant Technology and Science Editor
Published: 8:47, 3 Sep 2025 | **Updated**: 11:00, 3 Sep 2025

Tom's Guide

ChatGPT is down — live updates on massive OpenAI outage

10 minutes ago

TechRadar

ChatGPT is down - here's everything we know about the outage

ChatGPT is experiencing a major outage as users across the internet report problems with OpenAI's chatbot. Techradar is covering the

LIVE 5 minutes ago

Is Claude AI Down? Users Report 'Unexpected Capacity Constraint' Error

Authored by: Aradhana Brahma | Updated Feb 24, 2025, 04:16 IST


Model Risk

replit

Can you trust the model?

DeepSeek Terms of Use

Last Update: January 20, 2025

No Indemnification

Confidential Data

Monitoring Interactions

Data Transfers

Dear users, welcome to DeepSeek!

D wned and ope telligence Co., Ltd., eir affiliates (k" 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.

Data Poisoning & Prompt Security

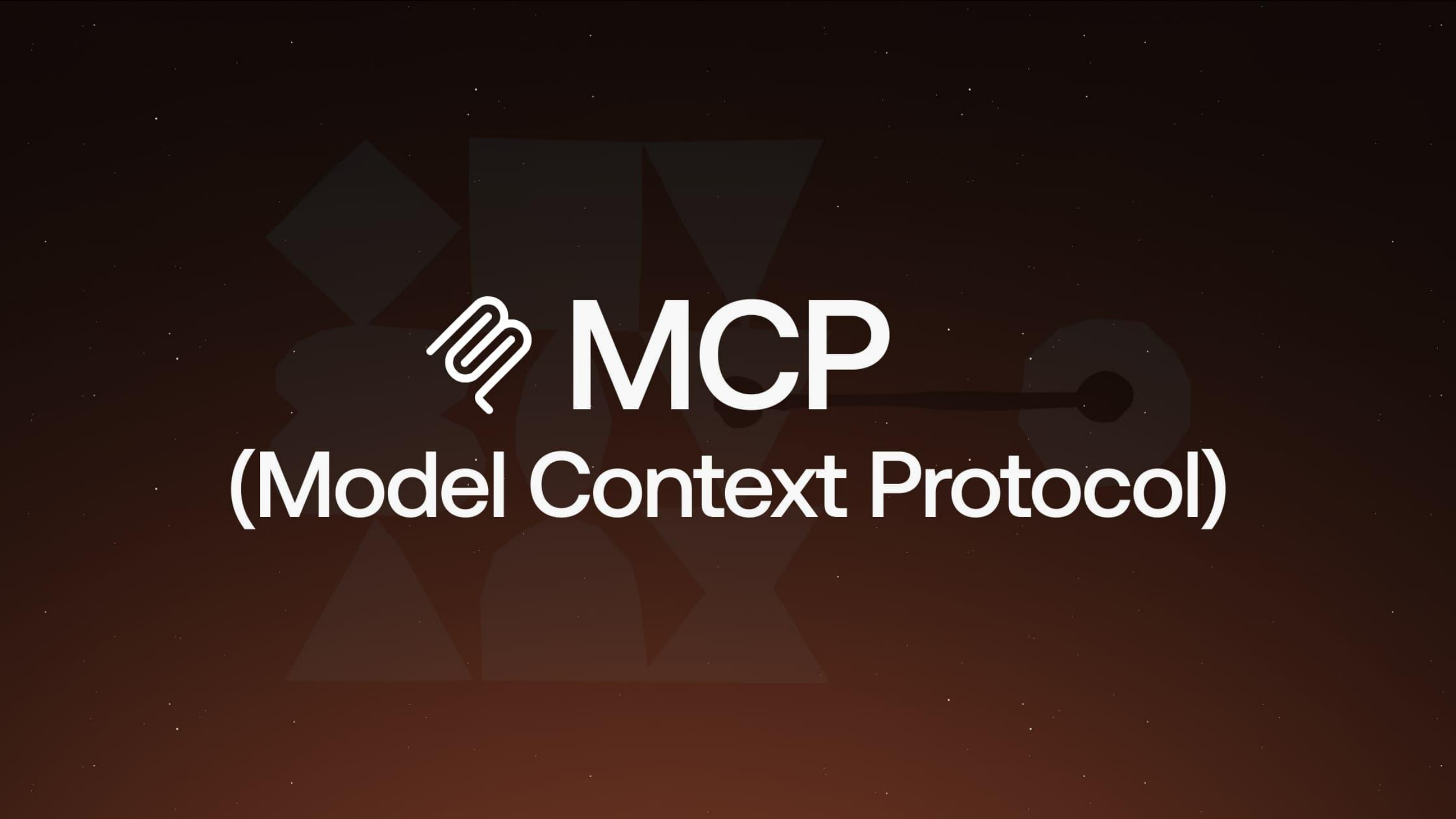
Lenovo's Customer Service AI Chatbot Got Tricked Into Revealing Sensitive Information. Here's How.

A single 400-character prompt exposed an almighty flaw in Lenovo's AI assistant

Published: August 20, 2025

CONTACT CENTER & OMNICHANNEL | CUSTOMER ANALYTICS & INTELLIGENCE | SECURITY, PRIVACY & COMPLIANCE | LATEST NEWS

New Security Concerns


MCP
(Model Context Protocol)

Model Context Protocol (MCP)

Open protocol for integration between LLMs and external data sources & tools.

What does it offer?

- Dynamic Context Enrichment
- Modular Toolchains
- Interoperability
- Cost Efficiency

Challenges

- Tool Poisoning & Rug Pulls
- Data Leakage
- Unauthorized Tool Execution
- Dependency Risks
- Insecure Communication

GBHackers News

Critical GitHub MCP Server Vulnerability Allows Unauthorized Access to Private Repositories

The Hacker News

Zero-Click AI Vulnerability Exposes Microsoft 365 Copilot Data Without User Interaction

CSO Online

Critical RCE flaw in Anthropic's MCP inspector exposes developer machines to remote attacks

A misconfigured default in the MCP inspector tool allows attackers to execute arbitrary commands via CSRF and legacy browser flaws,...

3 weeks ago

Agent Security

CISA Warns of Actively Exploited Langflow Remote Code Execution Vulnerability (CVE-2025-3248)

Posted by Diksha Ojha on May 6, 2025

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned users about a critical severity vulnerabi
tool designed for building agentic AI workflows. Successful exploitation of the vulnerability may allow
arbitrary system commands, leading to complete system compromise. CISA added the vulne

Langflow: CVE-2025-3248: Active Exploitation

Posted: 23rd May 2025 By: Insikt Group®

Vulnerabilit

A s
desc
unau
the un

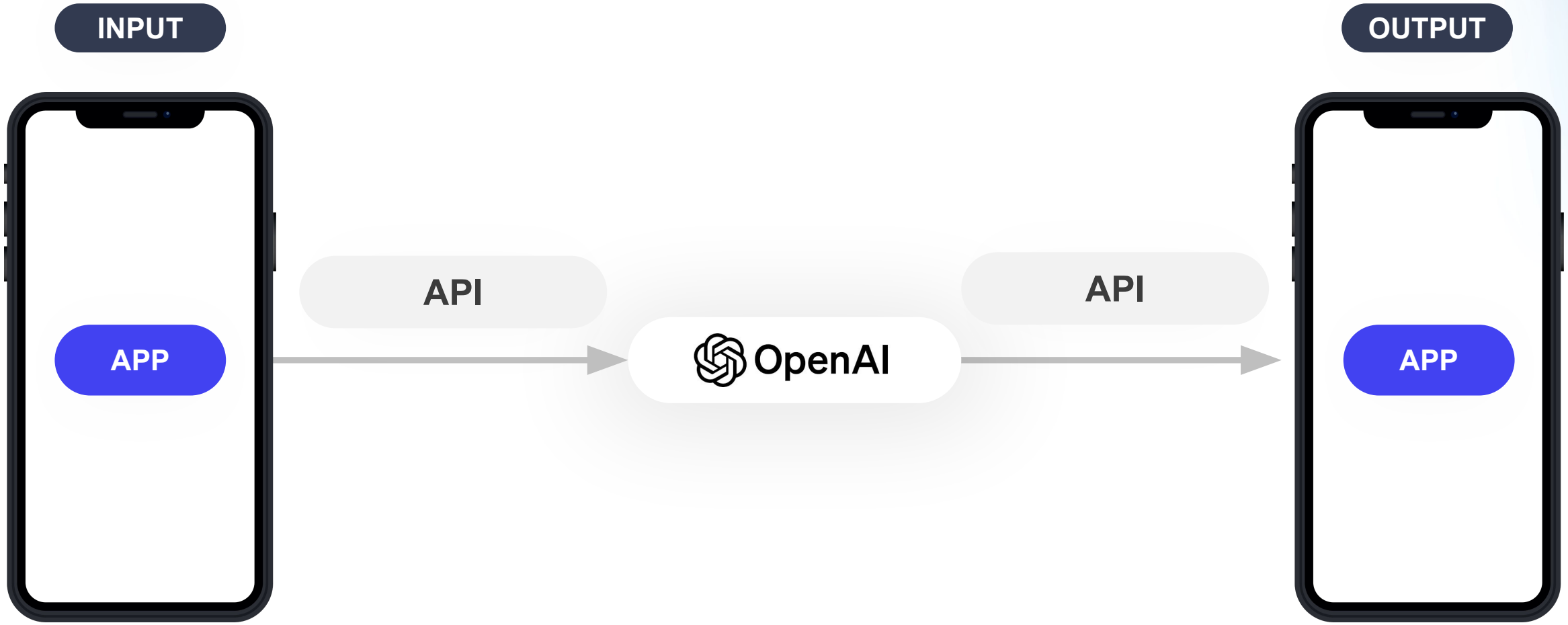
Vulnerabilities in Gen AI Could Prompt Data Leak

Open-Source Company Issues Patches After Being Alerted by

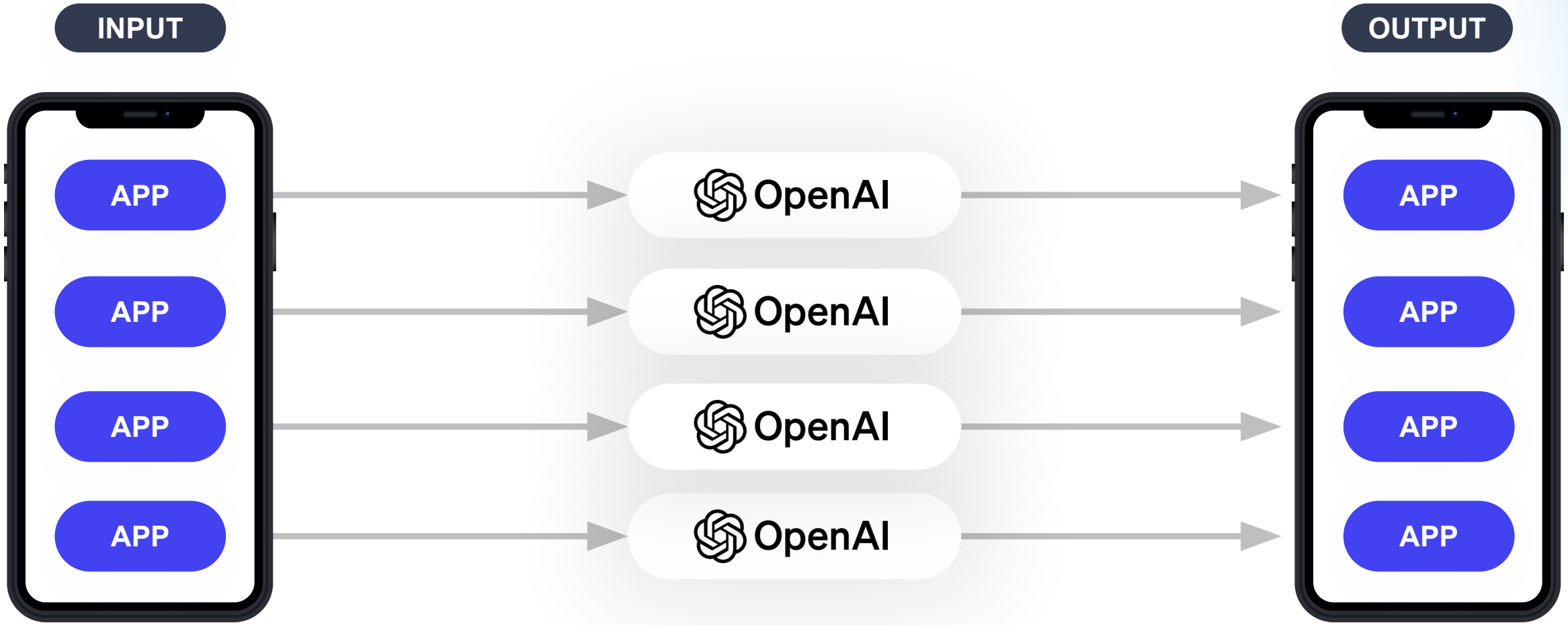
vulnerability to Langflow. In an article, the security researcher
nction without proper input sanitization. The function runs on an
oit this vulnerability by sending crafted payloads to specific API endpoints, leveraging

A2A protocol

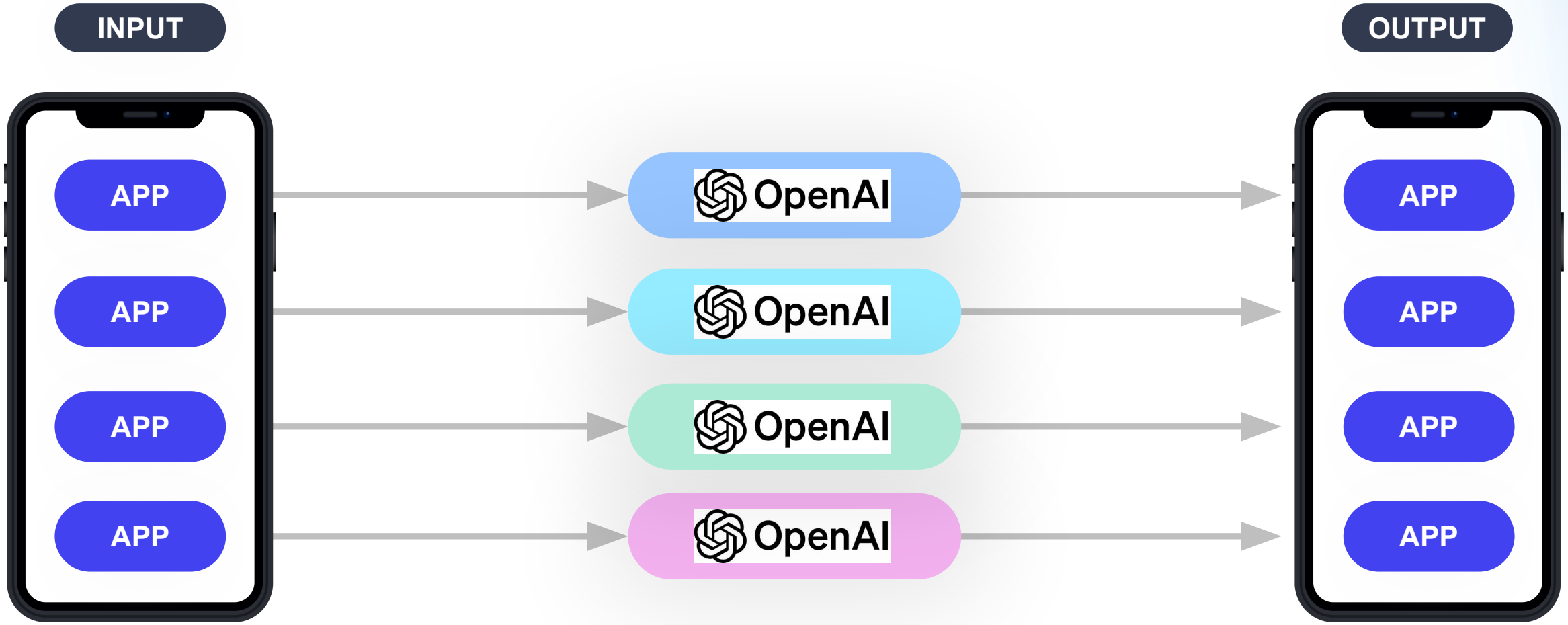
A Common Starting Point



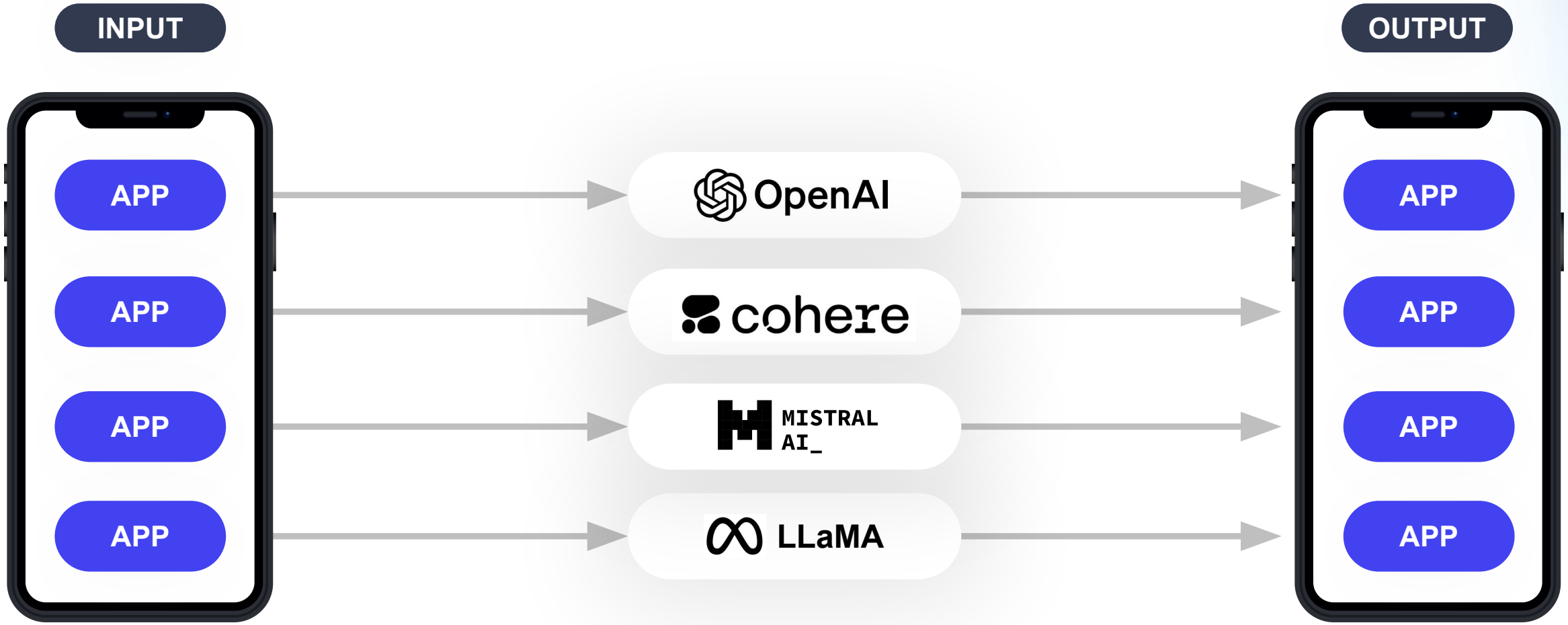
Use Cases Expanded



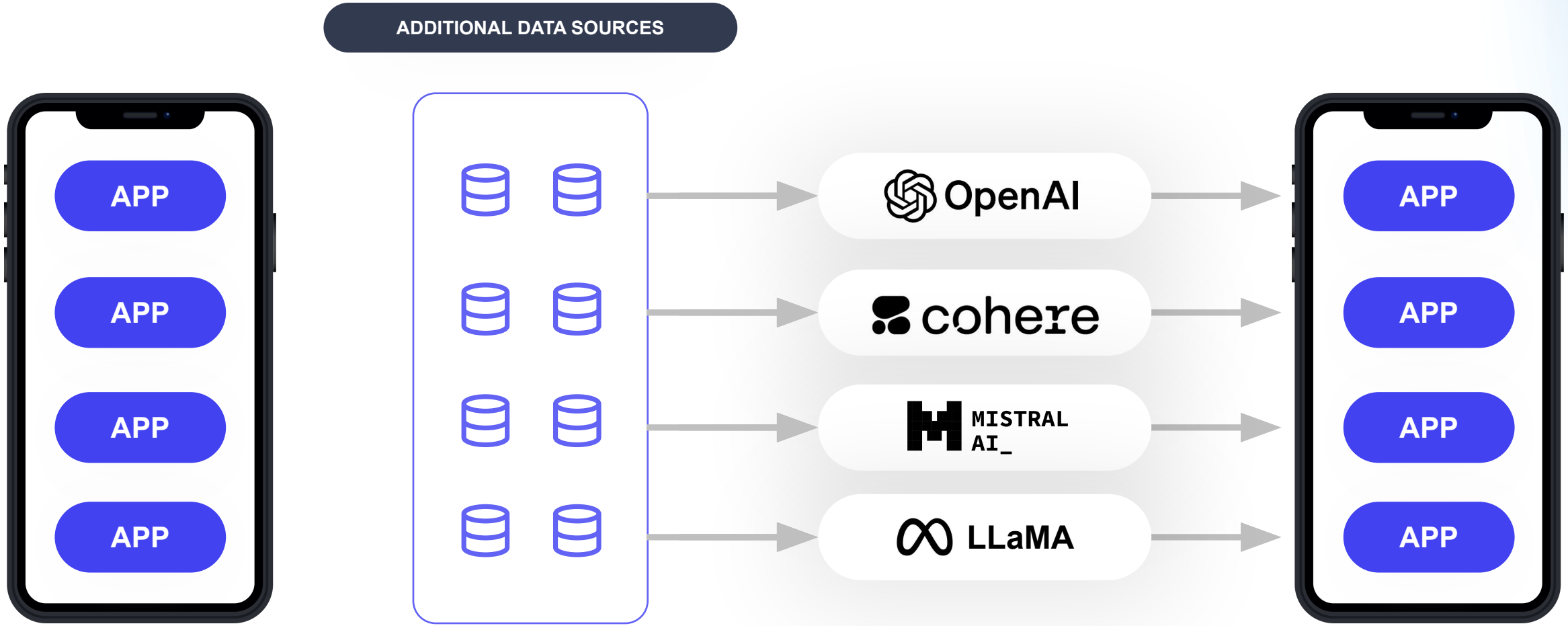
Version Proliferation from LLMs



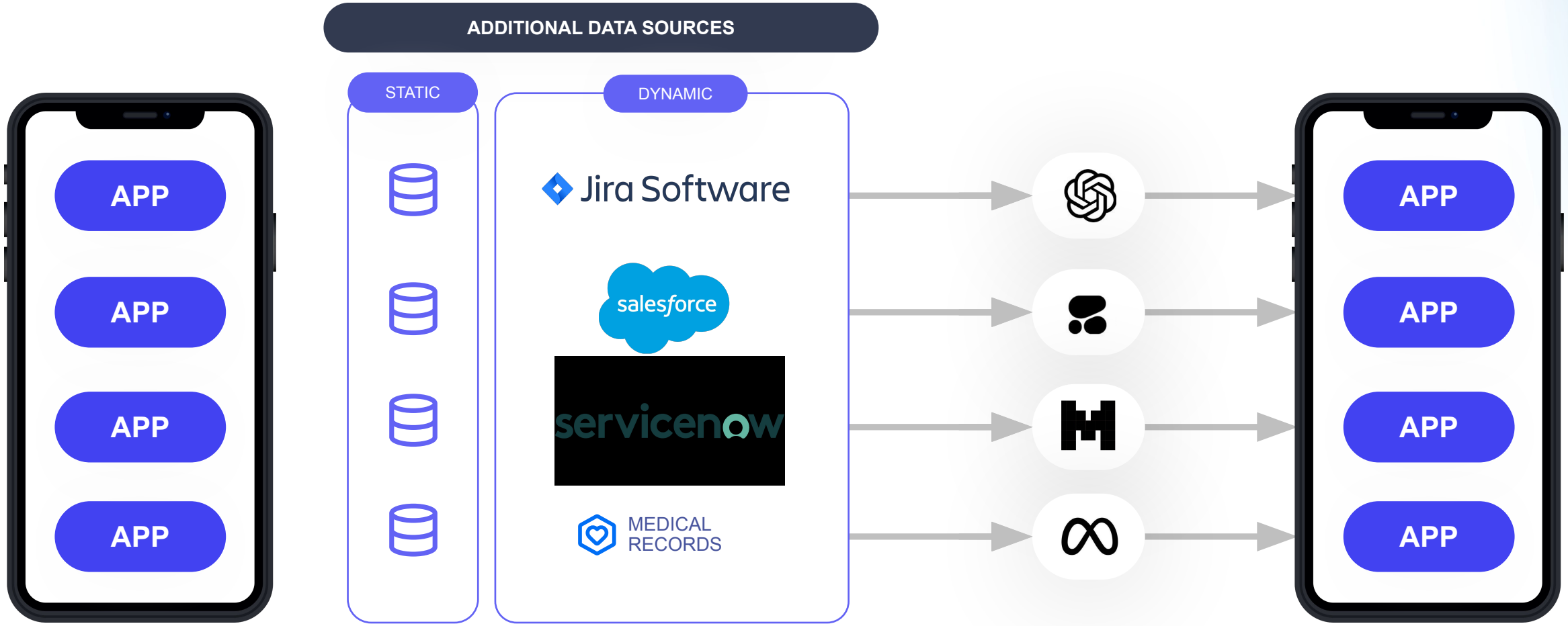
Across Multiple LLMs



Combined with Company Information

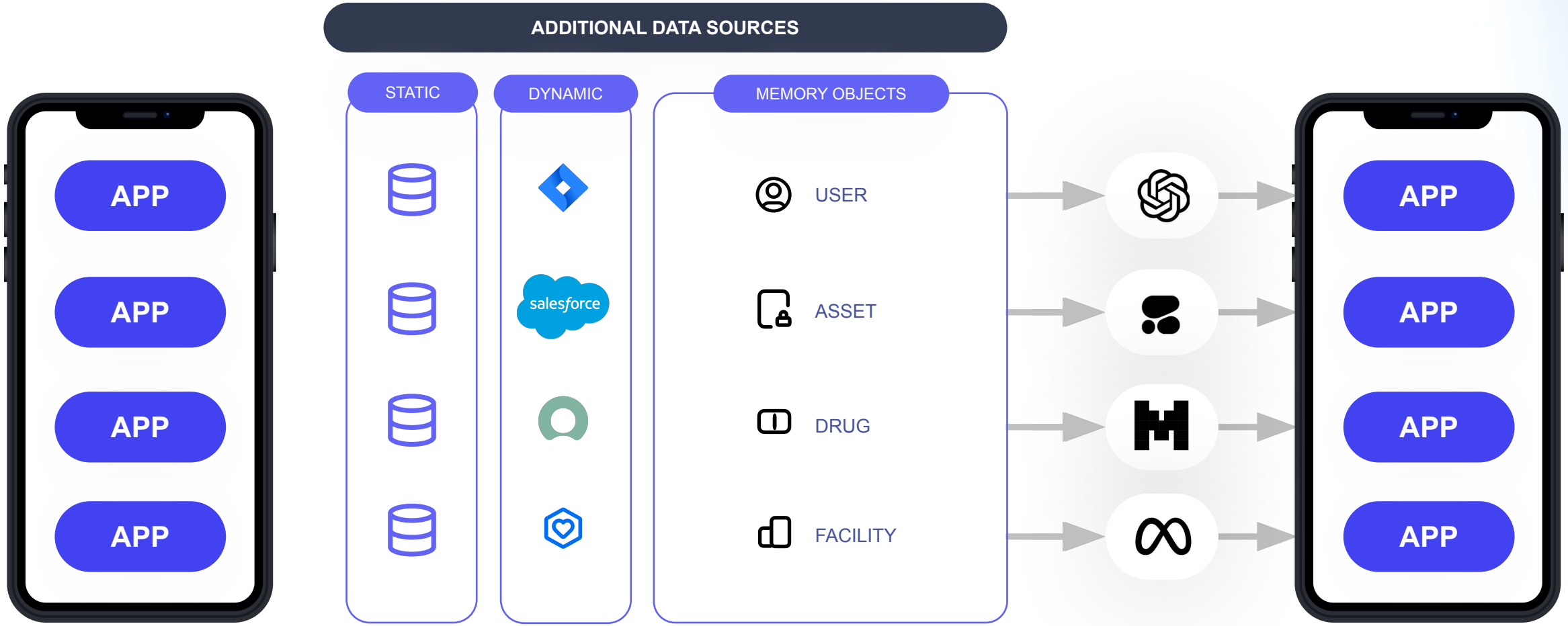


Transactional Data

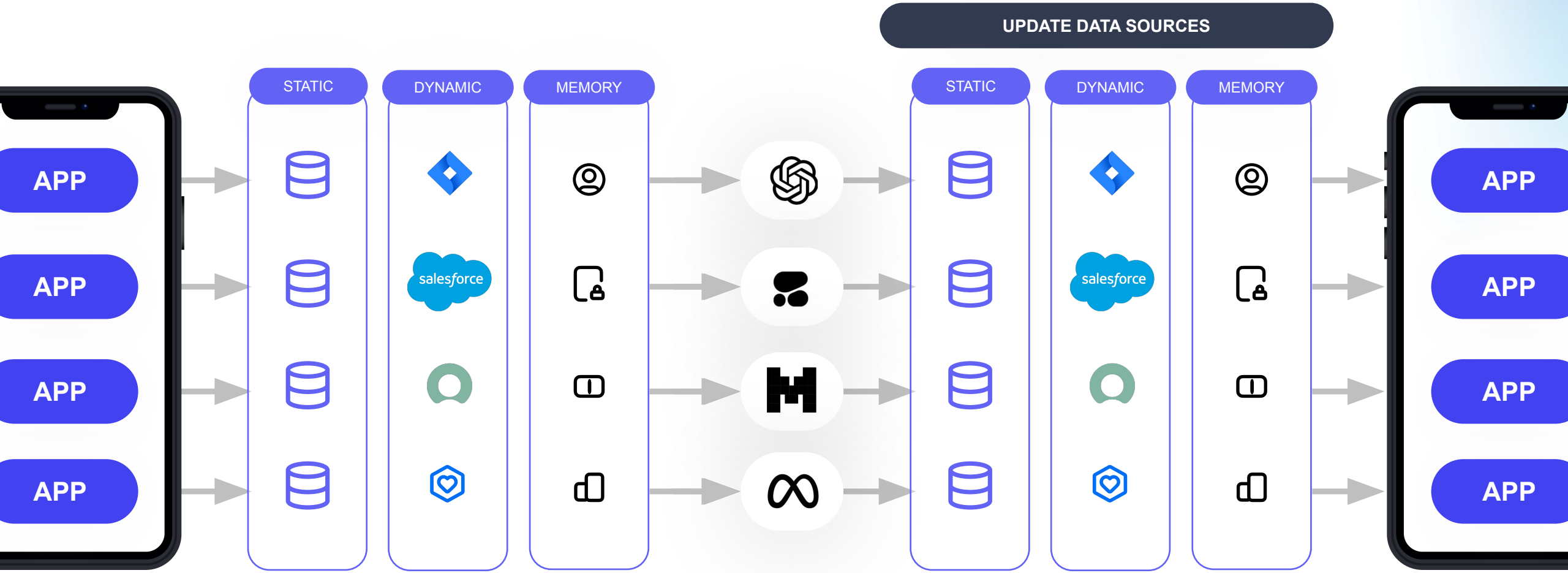


airia

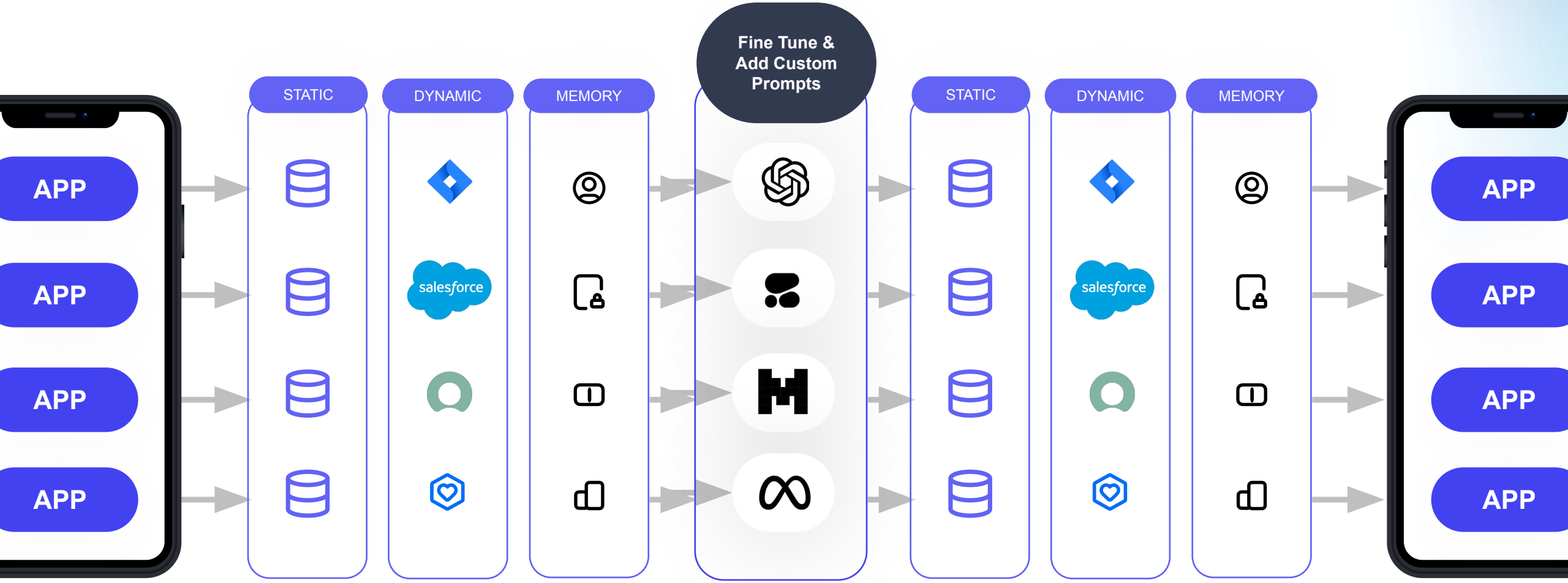
Plus Memory Objects



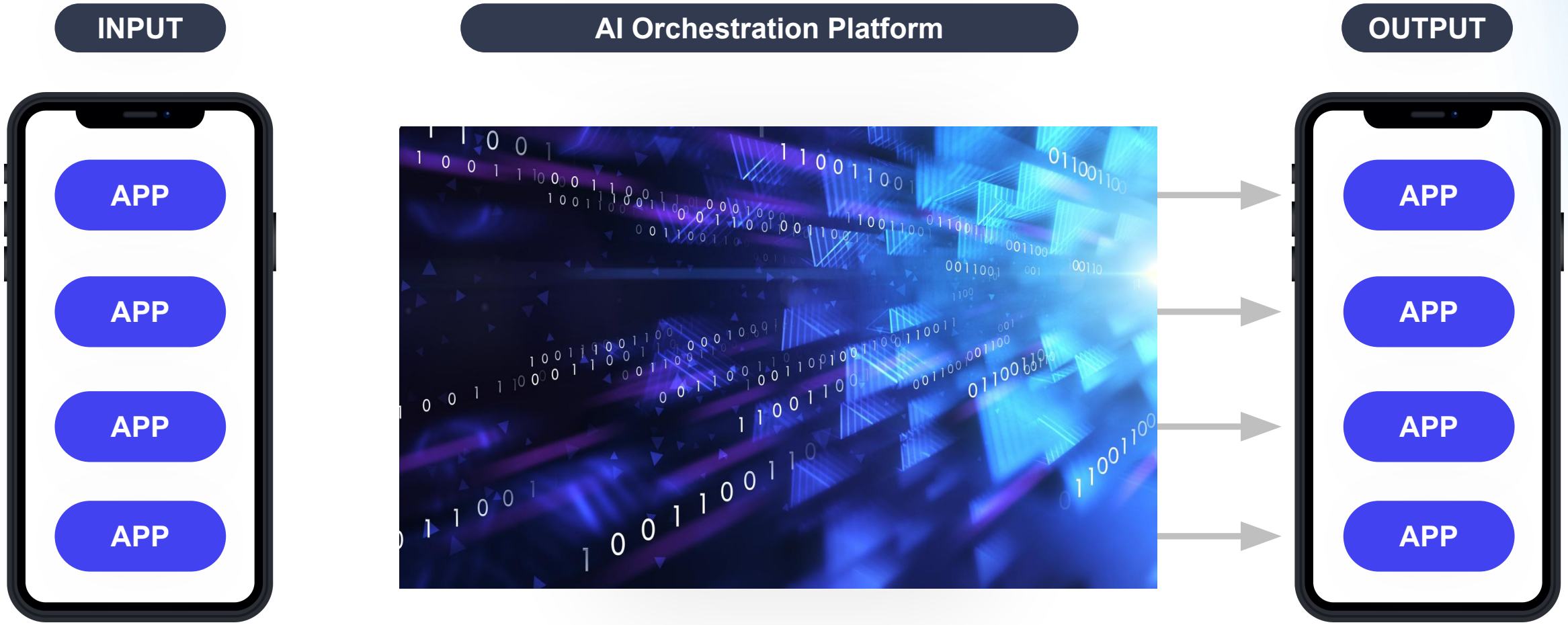
Write Updates to Data Sources



Prompts & Fine Tuning



The Need for AI Orchestration & Security



AI Management, Security & Governance

Increase agentic resilience & compliance without sacrificing employee innovation

AI Orchestration

Empower teams to rapidly design, test, and scale AI agents with reusable components without lengthy development cycles

- Agent Builder
- Prototyping Studio
- Data Integration
- Cost Optimization
- Enterprise Search
- Model Lifecycle Management

AI Security

Protect your AI ecosystem with embedded security controls and continuous monitoring to mitigate vulnerabilities and safeguard data.

- Security Posture Management
- Agent Red Teaming
- Agentic Security
- Data Security Controls
- Routing Engine
- Responsible AI Guardrails

AI Compliance

Drive trust and accountability with AI inventories designed to meet ISO 42001, EU AI Act, and the next wave of AI governance requirements.

- AI Inventory Management
- 3rd Party AI Risk Management
- Governance Operations
- Governance LLM-as-a-judge
- Human Oversight
- Audit & Observability

airia

AI Management, Security & Governance

Increase agentic resilience & compliance without sacrificing employee innovation

AI Orchestration

Empower teams to rapidly design, test, and scale AI agents with reusable components without lengthy development cycles

- Agent Builder
- Prototyping Studio
- Data Integration
- Cost Optimization
- Enterprise Search
- Model Lifecycle Management

AI Security

Protect your AI ecosystem with embedded security controls and continuous monitoring to mitigate vulnerabilities and safeguard data.

- Security Posture Management
- Agent Red Teaming
- Agentic Security
- Data Security Controls
- Routing Engine
- Responsible AI Guardrails

AI Compliance

Drive trust and accountability with AI inventories designed to meet ISO 42001, EU AI Act, and the next wave of AI governance requirements.

- AI Inventory Management
- 3rd Party AI Risk Management
- Governance Operations
- Governance LLM-as-a-judge
- Human Oversight
- Audit & Observability

airia

AI Management, Security & Governance

Increase agentic resilience & compliance without sacrificing employee innovation

AI Orchestration

Empower teams to rapidly design, test, and scale AI agents with reusable components without lengthy development cycles

- Agent Builder
- Prototyping Studio
- Data Integration
- Cost Optimization
- Enterprise Search
- Model Lifecycle Management

AI Security

Protect your AI ecosystem with embedded security controls and continuous monitoring to mitigate vulnerabilities and safeguard data.

- Security Posture Management
- Agent Red Teaming
- Agentic Security
- Data Security Controls
- Routing Engine
- Responsible AI Guardrails

AI Compliance

Drive trust and accountability with AI inventories designed to meet ISO 42001, EU AI Act, and the next wave of AI governance requirements.

- AI Inventory Management
- 3rd Party AI Risk Management
- Governance Operations
- Governance LLM-as-a-judge
- Human Oversight
- Audit & Observability

airia

AI Management, Security & Governance

Increase agentic resilience & compliance without sacrificing employee innovation

AI Orchestration

Empower teams to rapidly design, test, and scale AI agents with reusable components without lengthy development cycles

- Agent Builder
- Prototyping Studio
- Data Integration
- Cost Optimization
- Enterprise Search
- Model Lifecycle Management

AI Security

Protect your AI ecosystem with embedded security controls and continuous monitoring to mitigate vulnerabilities and safeguard data.

- Security Posture Management
- Agent Red Teaming
- Agentic Security
- Data Security Controls
- Routing Engine
- Responsible AI Guardrails

AI Compliance

Drive trust and accountability with AI inventories designed to meet ISO 42001, EU AI Act, and the next wave of AI governance requirements.

- AI Inventory Management
- 3rd Party AI Risk Management
- Governance Operations
- Governance LLM-as-a-judge
- Human Oversight
- Audit & Observability

airia

AI Security & Governance

Reduce attack surfaces across the AI lifecycle

Data collection → Model training → Deployment → Run

Development & Deployment | **Runtime**

Model Security

- Run models trained on proprietary data in your own infrastructure or trusted providers
- Prevent model Denial of Service attacks by rate limiting requests
- Deploy models from an Enterprise Model Library with established model provenance

Supply Chain

- Limit use to approved models
- Limit use to approved model providers
- Switch Model and provider without code changes
- Scan and sanitize model responses to close backdoors in compromised models

Shadow AI

- Observability into AI usage from corporate devices
- Just-in-time Acceptable AI Use Policy popup
- Prevent file upload to known consumer AI clients on corporate devices

Data Security

- Detect and block prompt injections
- Prevent PII, PCI, and PHI data leakage
- Prevent sensitive company data leakage
- Prevent secrets leakage
- Response sanitization
- Utilize Activre Security Testing

Identify & Secure: AI Security Posture Management (AI-SPM)

Agent & AI Usage Discovery

- Detect shadow AI usage across the organization
- Monitor sanctioned AI usage
- Generate a compliance ready AI-Bill of Materials

Security Posture Management

- Auto-configure agents to route through AI Gateway
- Comprehensive observability and monitoring
- Enable Runtime security Guardrails

Use Case: Sanctioned Agent building

A financial services organization allows developers to build agents on N8n with a preapproved list of Models. Airia automatically detects agents configured with LLM nodes and routes them through the AI Gateway to enforce runtime security guardrails for prompt filtering and DLP to prevent sensitive data exposure.

AI Gateway

Gain observability & apply guardrails to

Observability for AI and Agents built on any agentic framework

Centralize oversight for AI applications across your enterprise by funneling all AI application traffic through the Airia AI Gateway. Configure Airia to retain user prompt and model response data for regulatory compliance needs.

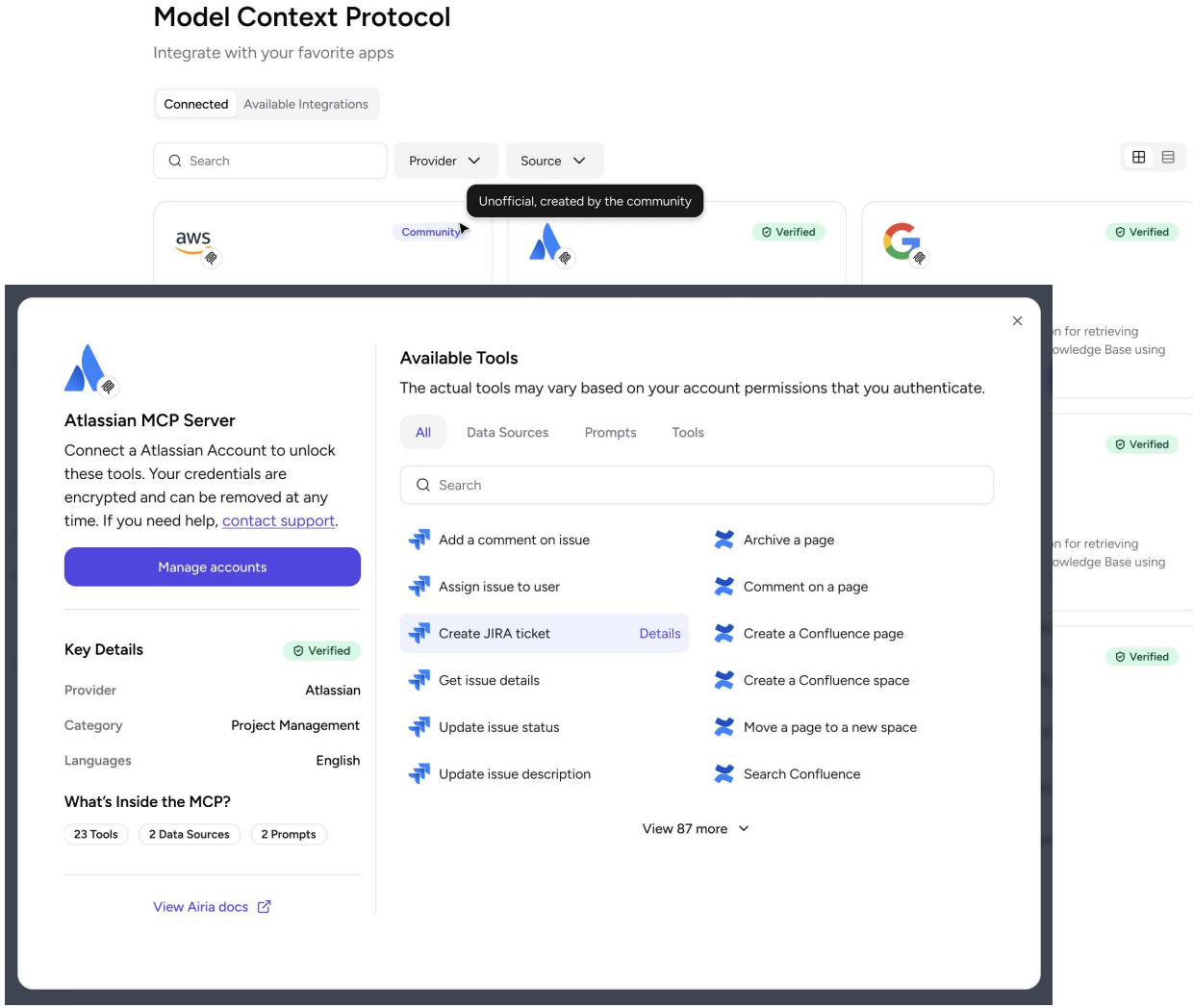
Security for non-Airia built agents

Enforce Airia Guardrails on all AI applications and safeguard your AI estate just as you would for Airia built agents.

Build Secure Integrations with MCP servers

Model Context Protocol

- Select from a curated list of popular MCP servers
- Integrate with remote MCP servers
- Securely deploy STDIO MCP servers to ephemeral sandboxes to ensure
  - Zero retention
  - Secure credential handling
  - Tool level authorization
  - Change management controls for Tools



Embrace & Manage the A2A Protocol

Agent interoperability standard introduced in April 2025

- Build complex, cross-platform automation by discovering, importing and chaining any A2A-compliant agent.
- Retain AI agent execution details complete with request and response details and apply guardrails.

Test & Validate: AI Red Teaming

Automated AI Red Teaming & Security Testing

- Automated Attack simulation to test agents against curated adversarial prompt datasets.
- Adversarial Attack Library
- Goal oriented red teaming / Dynamic adversarial prompt generation
- Actionable and auditable risk findings

Use Case: AI vulnerability identification

A large manufacturer is building agents in house and adopting AI agents from Salesforce. Airia can connect to their existing AI products and environments to run custom or scheduled tests

RED TEAM

AIRIA SECURITY

airia

Stay Current By Using the Best Models

Model re-routing based on

Any trigger → **Any reason** → **Any model**

Risk Score

Source

Application / User agent

Destination model

Data location

Data Security Policies

Request Complexity

Model and Provider Availability

Preference

Cost
Quality

Performance

Inference Latency
Availability

Data Governance Policies

Data Leakage Protection
Privacy

OpenAI

ANTHROP\C

airia

Enterprise AI Platform

Accelerate and secure AI deployments with a comprehensive platform

Rapid Agent Prototyping

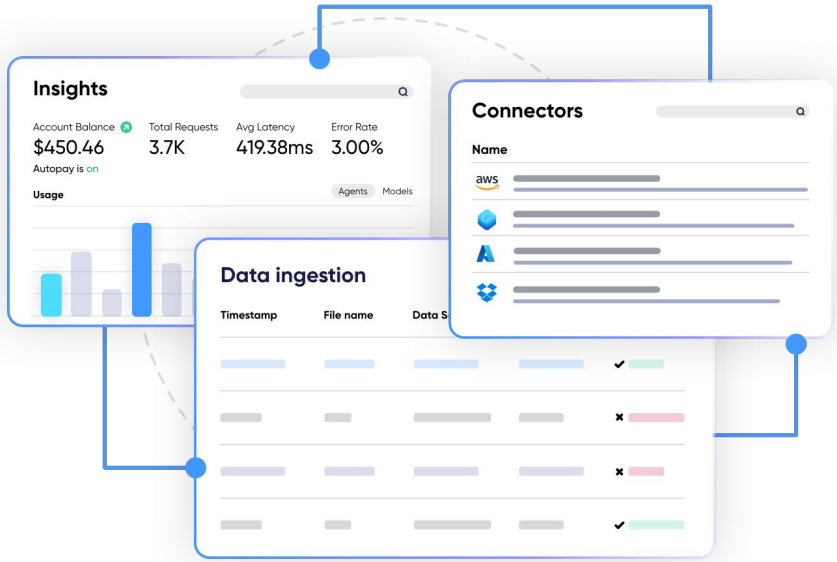
Accelerate time-to-value and reduce technical barriers to AI adoption.

No-Code Builder | Pre-Built Libraries | Prototype Studio

Data Integration Architecture

Seamlessly connect to existing enterprise systems to maximize investments.

Enterprise Apps | Data Sources | Model Agnostic



Intelligent AI Operations

Optimize AI performance, manage costs and scale your AI deployment.

Cost Optimization | Routing Engine | Model Lifecycle

AI Security & Governance

Ensure enterprise-grade security, compliance, and responsible AI usage.

DLP Controls | Audit & Observability | Responsible AI

CONNECTOR MARKETPLACE | **MULTI-CHANNEL DELIVERY** | **SECURE BY DESIGN** | **FLEXIBLE HOSTING OPTIONS**

airia

Airia Agent Library for **Enterprises**

Growing list of 2,700+ pre-configured AI agents

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

Flexible Deployment Options

Support for multiple hosting models to fit your operational, security, and compliance requirements.

Shared Cloud

Fast deployment, zero operational overhead

Deploy in a secure, multi-tenant environment on shared infrastructure.

Dedicated Cloud

Secure cloud deployment with added support

Deploy in your own dedicated environment, fully managed by Airia.

Private Cloud

Maintain network control on existing infrastructure

Deploy in your existing Azure or AWS cloud for more control and security.

On-Premises

Companies needing full management and control

Self-host in your data center for complete control and ongoing management.

Choose the right hosting

- Time to Value: Fast deployment or controlled enterprise rollout
- Security Posture: Multi-tenancy or full deployment isolation
- Compliance Needs: Regulatory requirements and data residency
- IT Resources: Airia managed or in-house DevOps teams
- Control & Cost: Cost-efficiency or infrastructure ownership

Thank You

Interest in learning more?
Visit us at **C82**

For a copy of my slides:
NithishRajan@airia.com

