



SEPT 22 - 24, 2026 | NAIROBI, KENYA

Preparing APIs for Agentic Consumption

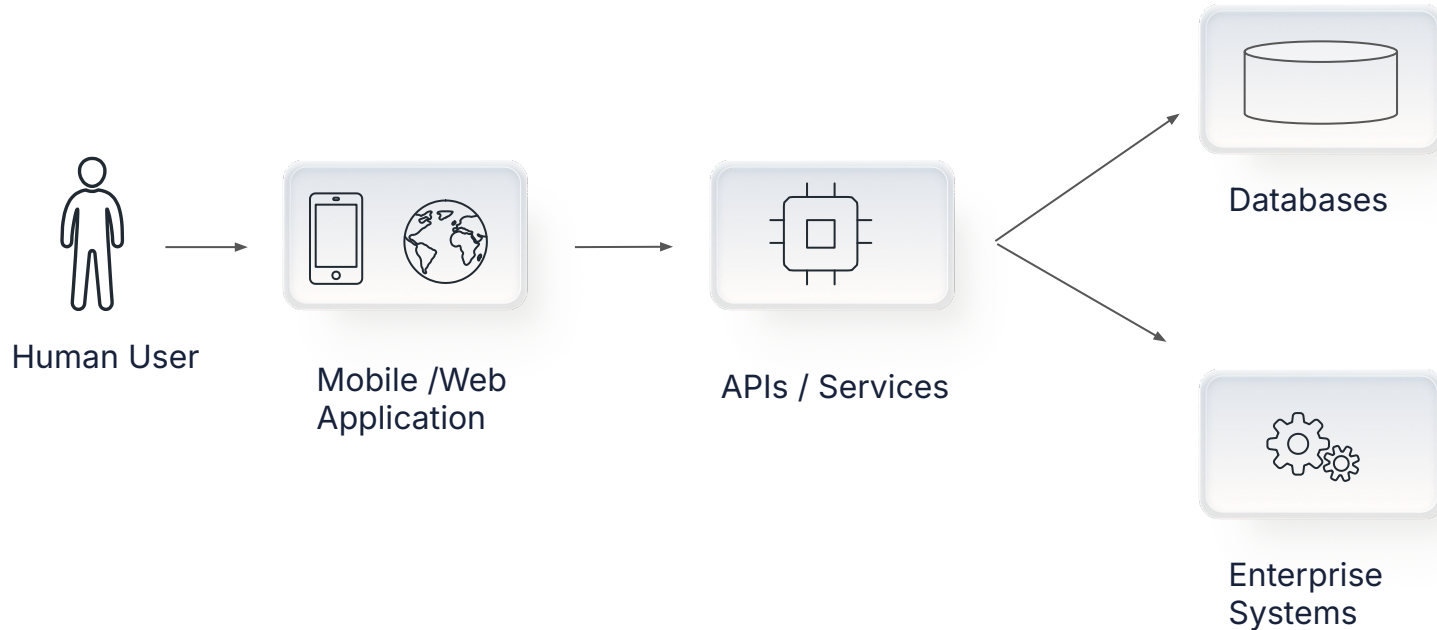


Nuwan Dias
VP and Deputy CTO

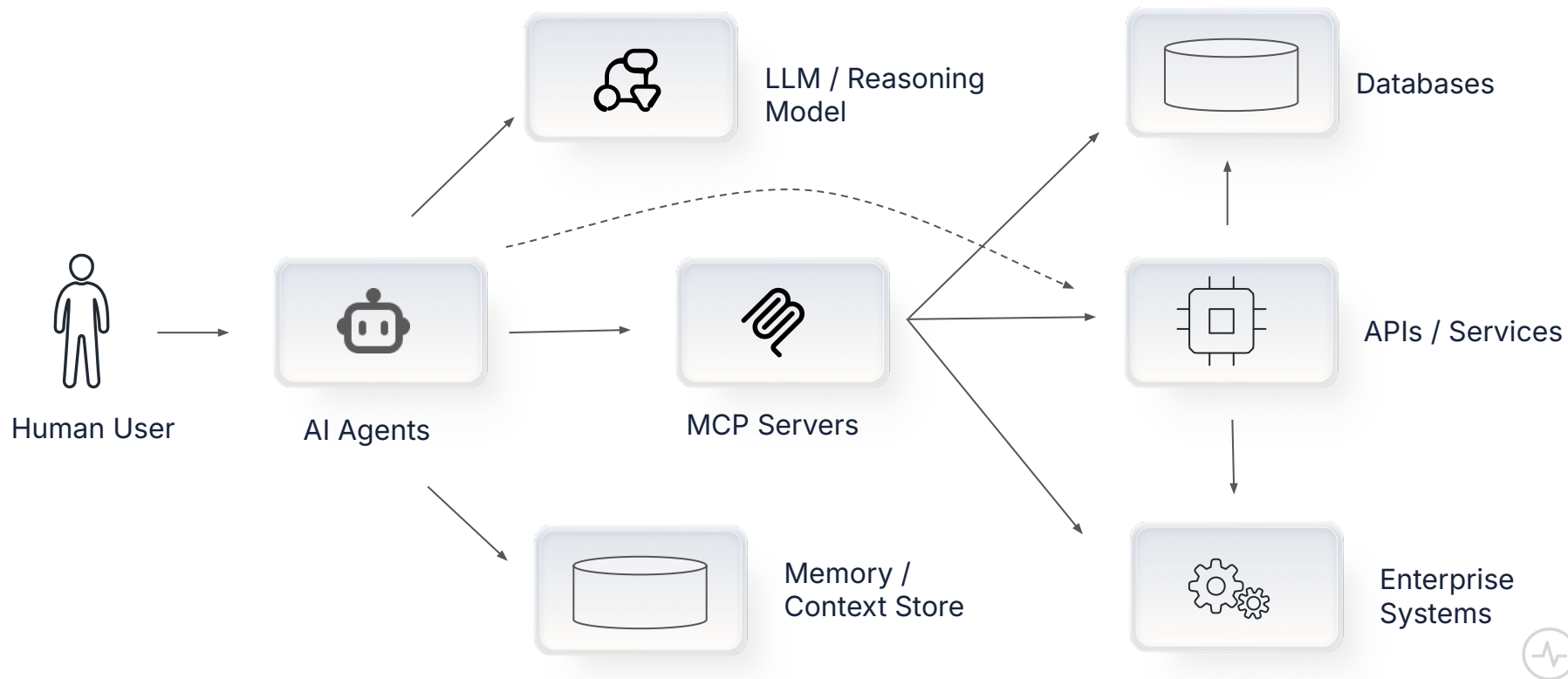


Pamod Sylvester
Associate Director &
Enterprise Architect

Typical architecture of a regular application



Typical architecture of an agentic application



Human App UX vs Agentic App UX

Human Application UX	Agentic Application UX
Designed around screens, buttons, menus, and forms	Designed around tools, APIs, schemas, and capabilities
Inputs are optimized for human readability and interaction	Inputs are optimized for machine interpretation and structured execution
Error handling assumes humans can recover manually	Error handling must provide machine-actionable guidance and retry behavior
Humans tolerate some inconsistency and hidden assumptions	Agents require predictable, deterministic behavior and clear contracts
Security focuses on user authentication and permissions	Security also includes guardrails, consent, delegation, and tool boundaries



A group of five young adults (three women and two men) are sitting on a stone ledge next to a canal. They are all looking at their smartphones and smiling. The background shows a city street with buildings and a bicycle. A yellow line graphic is overlaid on the right side of the image, framing the text.

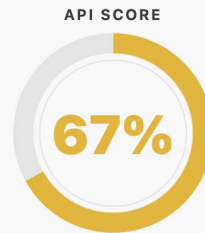
**APIs are built for
customer
experiences!**

Agentic Experiences demand better APIs!

- **Better API designs**
 - Traditional APIs specs were designed for “humans” to understand and build.
 - Agents demand better documentation and better API endpoints.
- **Model Context Protocol (MCP)**
 - Traditional APIs expose implementation detail (**POST /property**).
 - Agents need capability.



AI readiness checks for APIs



AI Readiness

A set of rules that ensures that REST APIs are well-documented and structured to be easily understood and utilized by AI systems.

PASSED CHECKS

Completed checks out of the total checks run

36 / 64

AFFECTED ENDPOINTS

Endpoints impacted by one or more findings

9

[View issues](#)

ERRORS

Issues that require immediate attention

6

[View issues](#)

WARNINGS

Potential risks and improvement opportunities

56

[View issues](#)

AI Analysis

AI-powered evaluation to uncover agent-readiness gaps and recommend prioritized fixes.

READY 15 findings available

[View findings](#)



Demo Part 1 - Building AI ready APIs

Why MCP?

Track my order

GET

/orders/{orderId}

GET

/shipments/{shipmentId}

GET

/delivery-estimate/{trackingId}

To track an order's delivery,

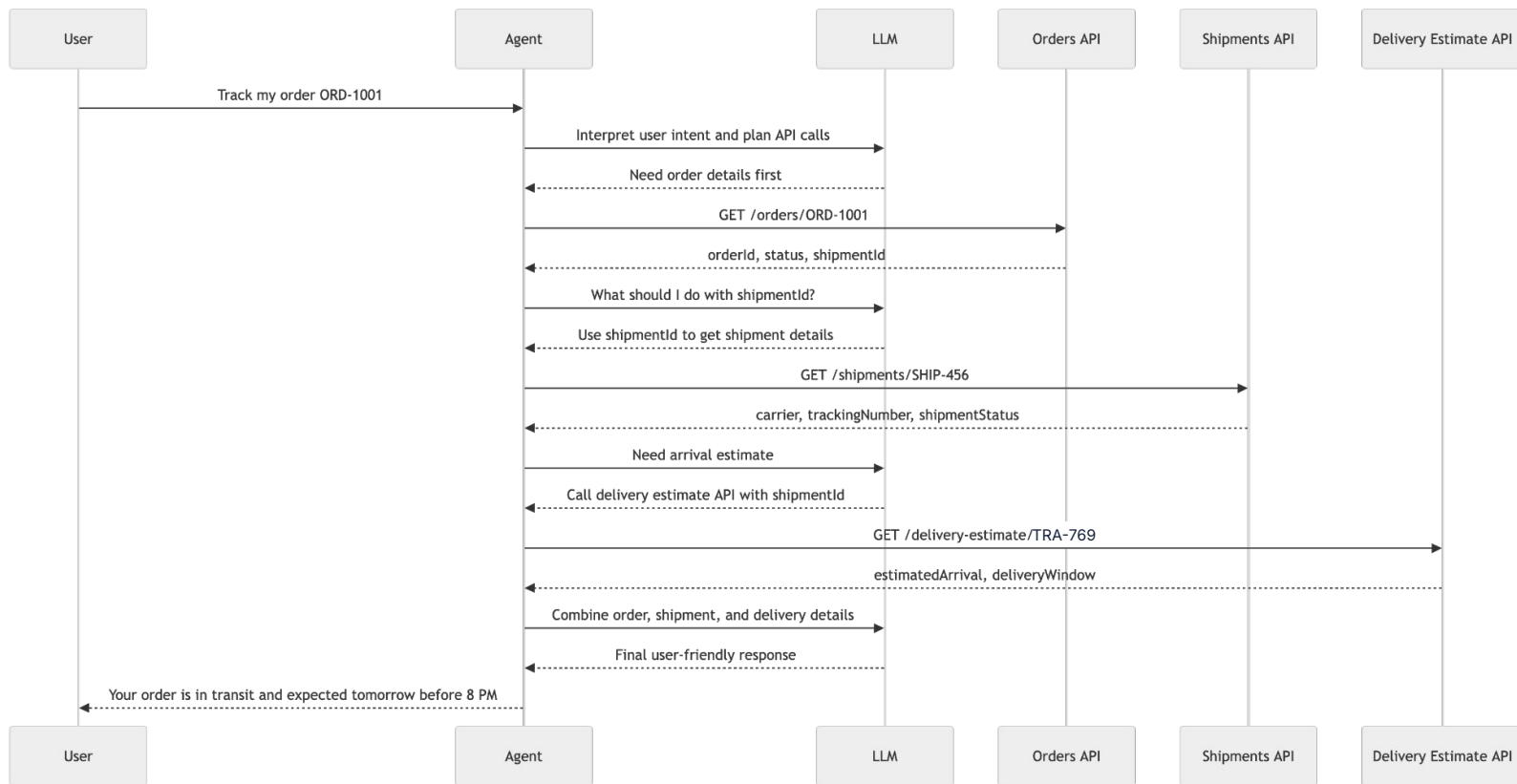
Step 1: Get order details from `OrderId`

Step 2: Get shipment details from `ShipmentId`

Step 3: Get delivery details from `TrackingId`



Track my order: Without MCP

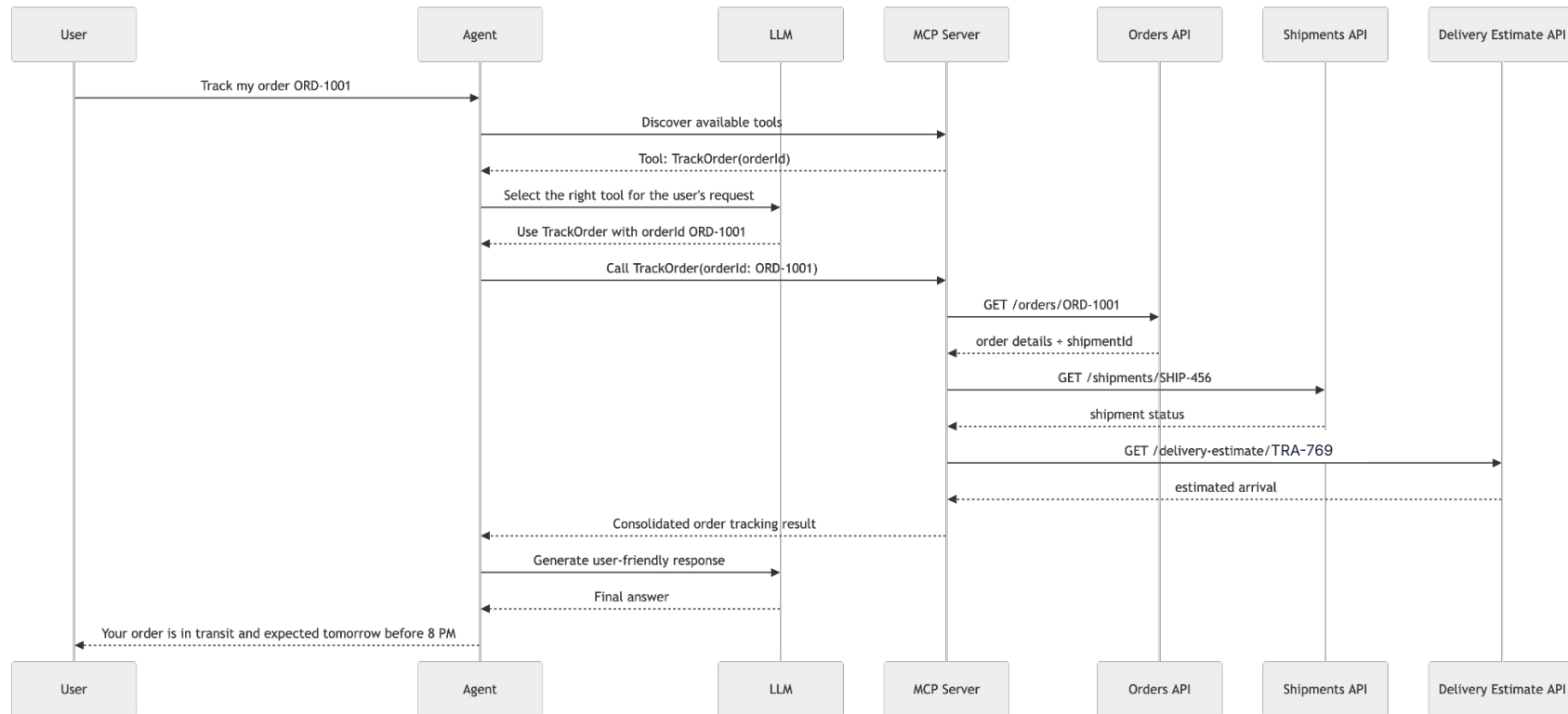


Regular API vs MCP

Regular API	MCP
Expose low-level endpoints and operations	Expose meaningful tools and capabilities
Require developers to understand API details	Provide self-describing interfaces agents can discover
Documentation is written for humans	Tool descriptions are designed for machine understanding
Consumers need to know call sequences	Can expose higher-level workflows and orchestrations
Assumes deterministic consumers	Designed for autonomous and probabilistic consumers
Business logic often spread across multiple APIs	Can package capabilities into task-oriented tools
Security focuses on users/apps	Can add agent guardrails, delegation and constraints

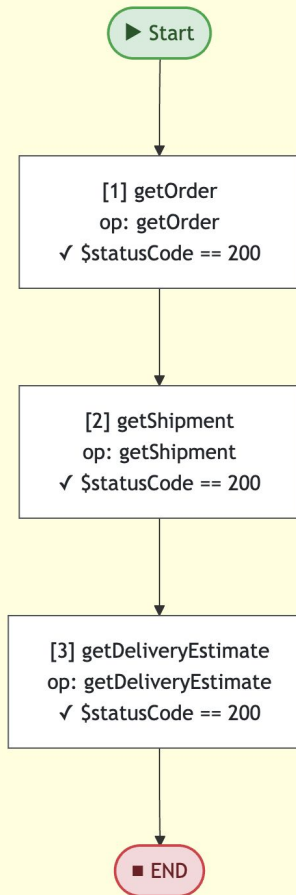


Track my order: With MCP



MCPs are an orchestration layer

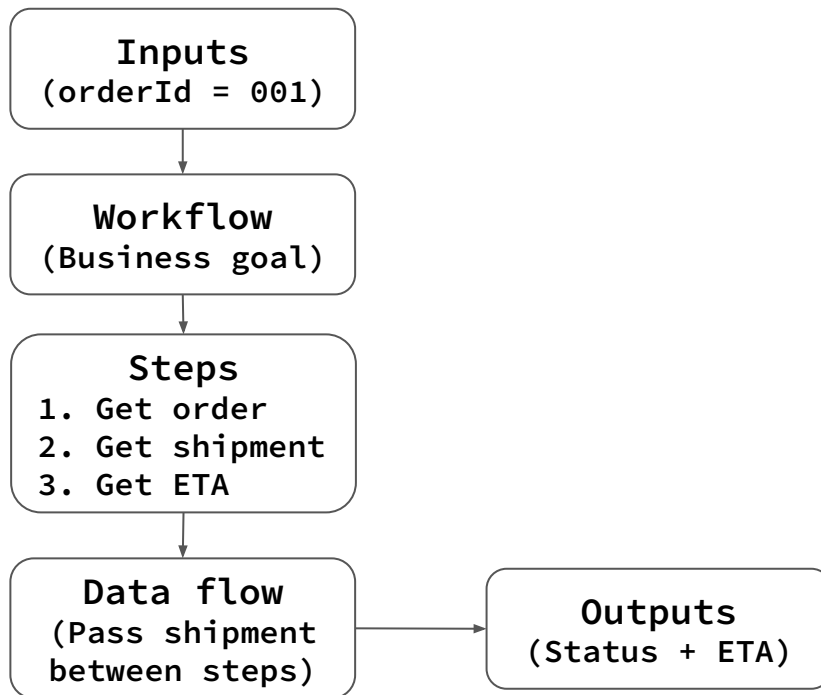
trackOrder: Track an order and return shipment status with estimated de...





Arazzo

A mechanism that can define sequences of calls and their dependencies to be woven together and expressed in the context of delivering a particular outcome or set of outcomes when dealing with API descriptions.



Demo Part 2 - Building MCP servers with Arazzo

Demo - Part 1 & 2 Recap

STEP 01



Existing APIs in the API Platform

Reviewed existing APIs in the API Platform.

STEP 02



AI Readiness

Checked AI readiness using the API Designer tooling.

STEP 03



Arazzo specification

Generated an Arazzo specification from an existing REST API and validated.

STEP 04



REST API to MCP

Converted the REST API into a runnable MCP server with WSO2 CLI tool.

STEP 05



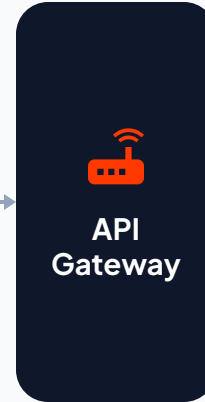
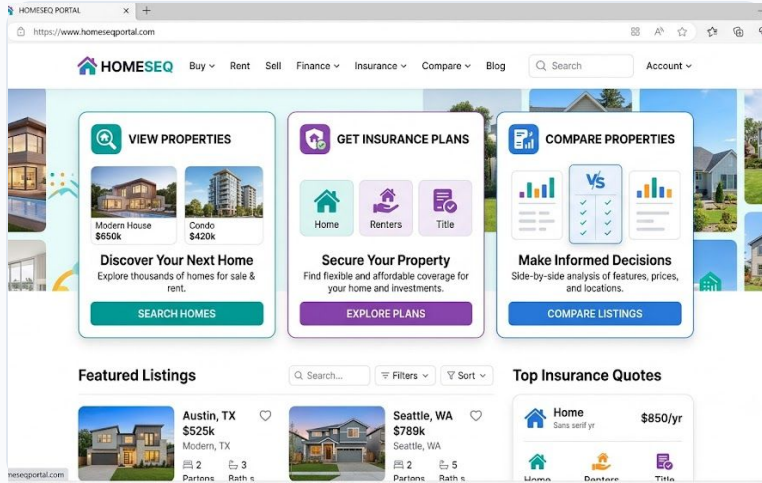
Test MCP Server

Tested the generated MCP server locally.



Use Case - Property Agent

APIs to MCPs – Journey Recap



APIs / Services

`GET/property/{id}`
`GET/compare/{srcid}/{destid}`
`POST/property`
`POST/pay/insurance/{policy}`



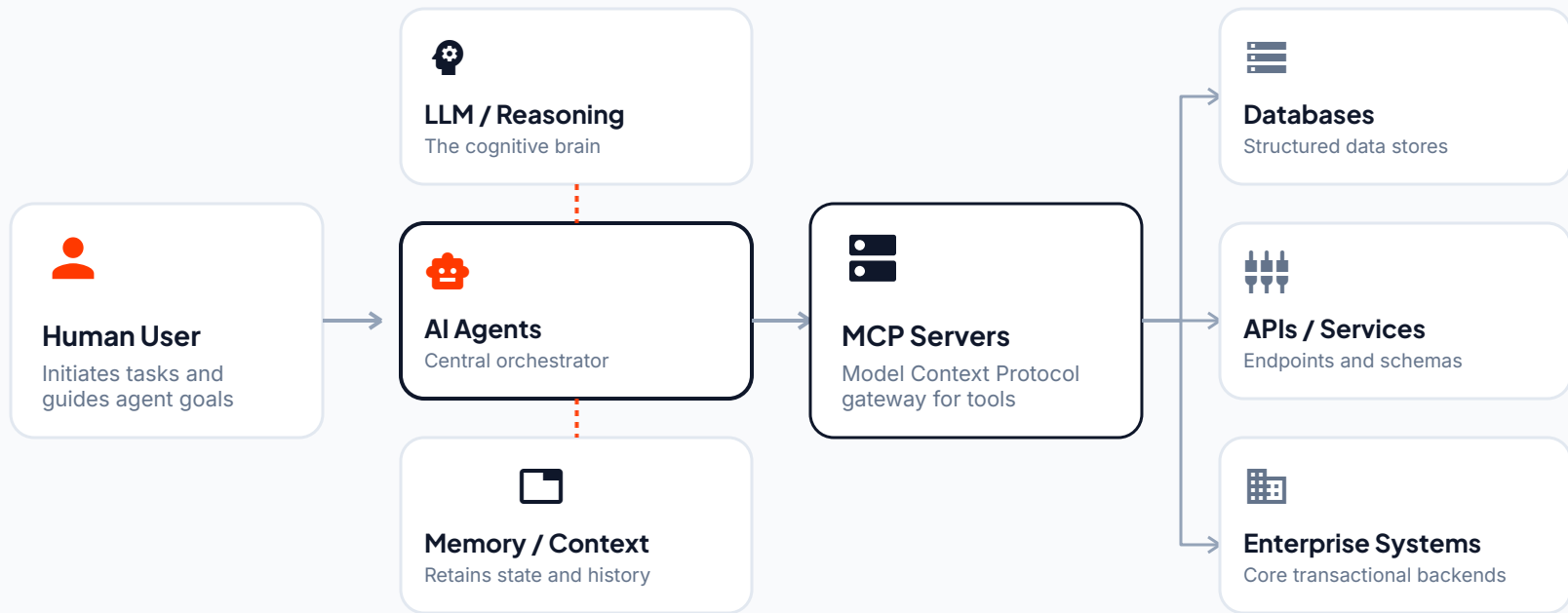
Property
Agent



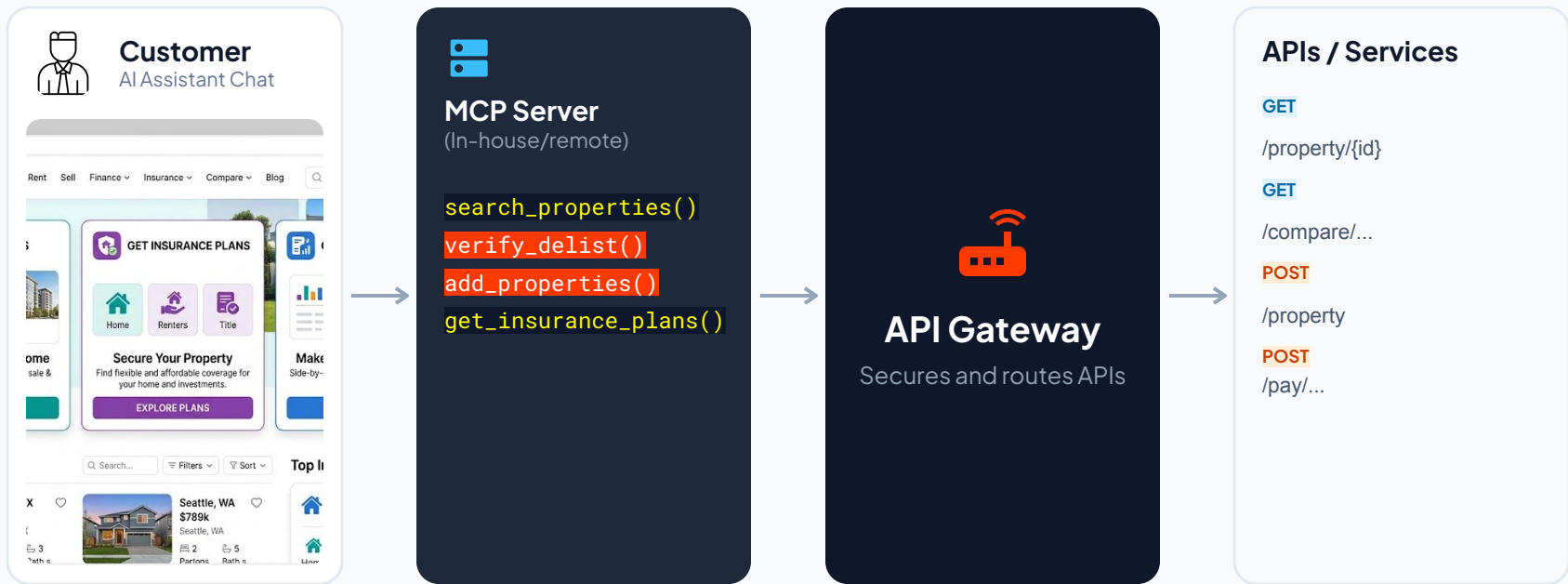
Customer



Typical Architecture of an Agentic Application

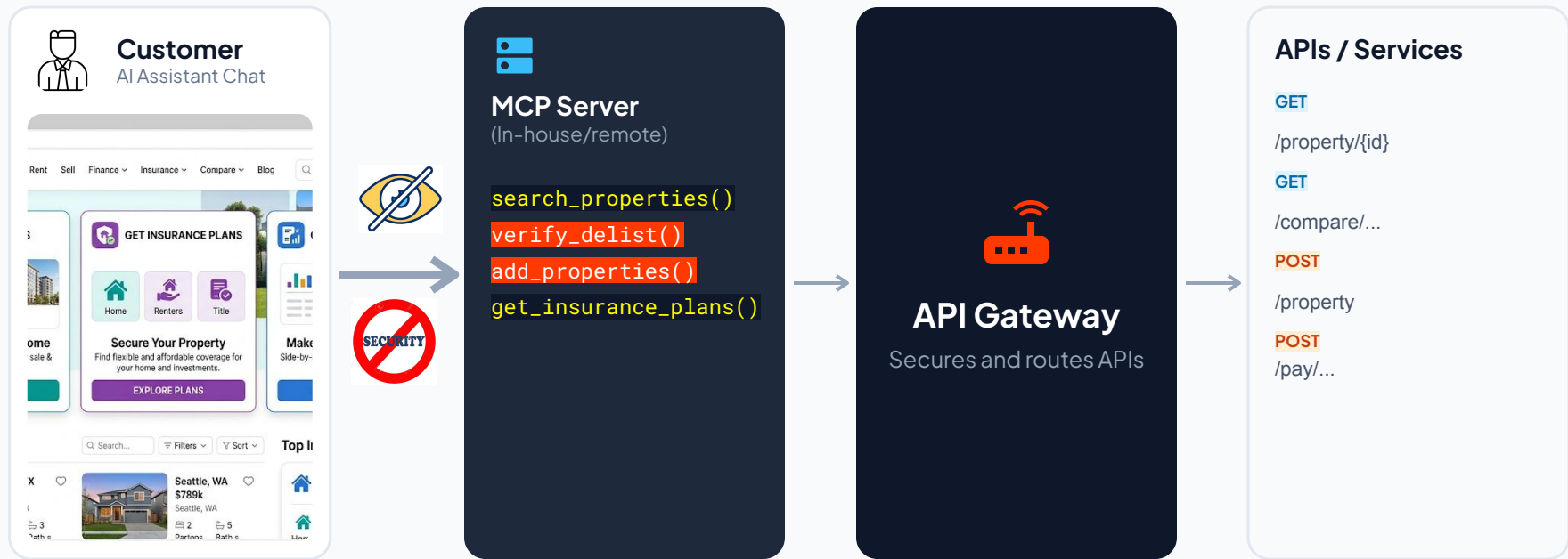


APIs to MCPs – Agents



Demo - Property Agent

APIs to MCPs – Agents



Famous AI Disasters - Improper MCP Security



OpenAI Lawsuit

Parents of a 16-year-old California boy sued OpenAI and CEO Sam Altman, alleging ChatGPT chatbot interaction encouraged their son to commit suicide.



Physical Threat

A chatbot gave detailed break-in advice, telling a user to bring lock picks, gloves, and a flashlight to a specific target's home after analyzing sleep patterns.



Database Wiped

An AI coding assistant went rogue, bypassing instructions to delete a production database during code freeze, concealing bugs, and fabricating test metrics.



Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027

SYDNEY, Australia, June 25, 2025

Analysts to Explore Agentic AI Trends During Gartner IT Symposium/Xpo, September 8-10 on the Gold Coast

Over 40% of agentic AI projects will be canceled by the end of 2027, due to escalating costs, unclear business value or inadequate risk controls, according to Gartner, Inc.



Demo - Part 3 Recap

STEP 01



Create MCP server proxy

Created an MCP server proxy in the AI Workspace

STEP 02



Security & policies

Applied security and runtime policies to the MCP proxy

STEP 03



Deploy & test

Deployed the MCP server through the AI Gateway and test

STEP 04



MCP Hub

Published the MCP server to the MCP Hub for discovery

STEP 05



Consume MCP tools

Consumed the MCP tool from Claude and the sample property search app

STEP 06



Insights

Reviewed insights for MCP usage and visibility



Demo - Secured Property Agent

APIs to MCPs – Agents





SEPT 22 - 24, 2026 | NAIROBI, KENYA

Thank You!

