

The Missing Protocol

How MCP Bridges LLMs and Data Streams

Viktor Gamov
Principal Developer Advocate, Confluent

[@gamussa](https://linkedin.com/in/vikgamov)

● Model Context Protocol
Topic

● Retrieval-augmented genera...
Topic

+ Add comparison

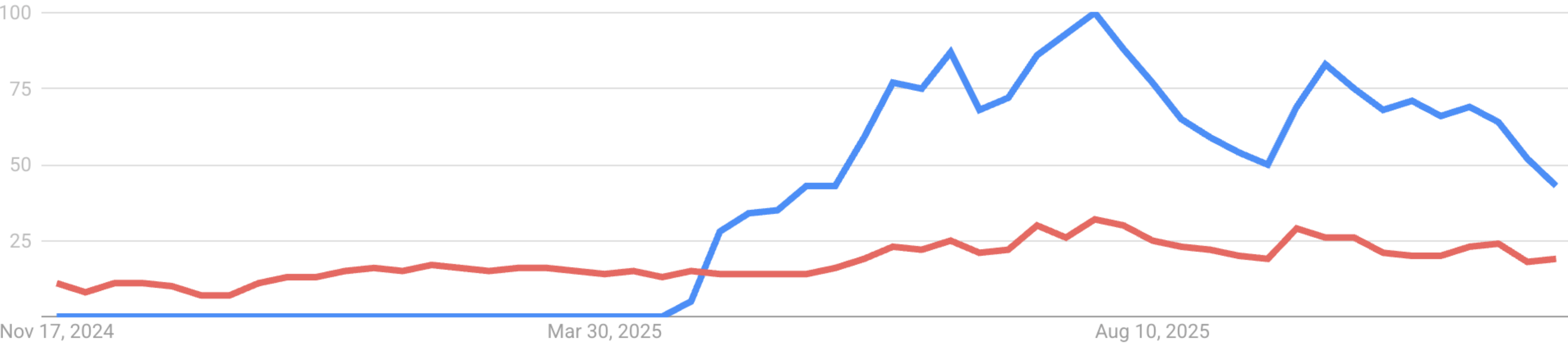
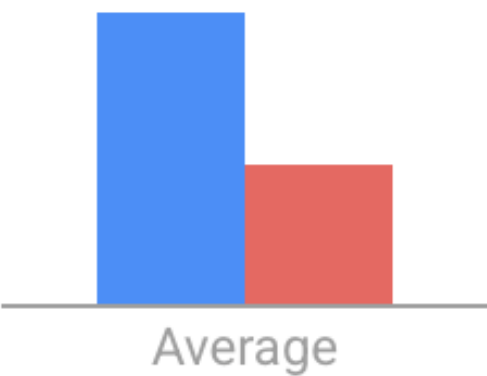
United States ▼

Past 12 months ▼

All categories ▼

Web Search ▼

Interest over time ⓘ

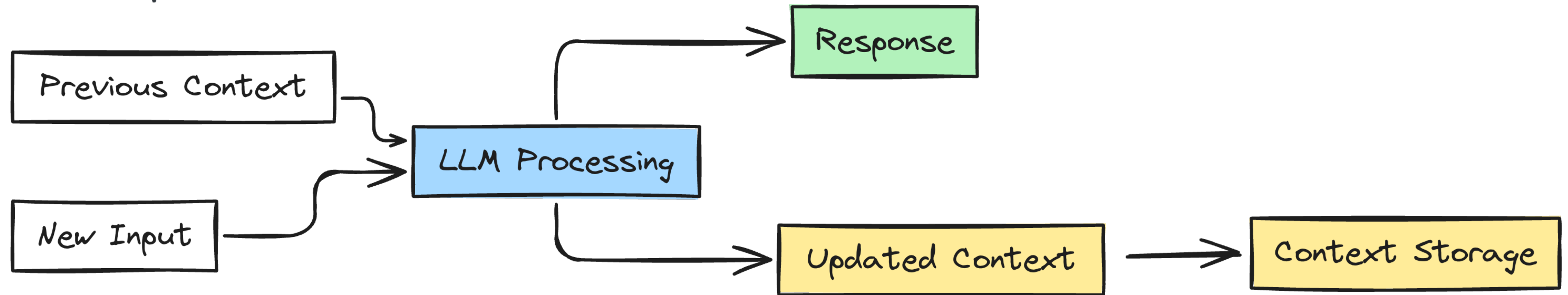


What LLMs do



What LLMs do

Memory



What LLMs don't do

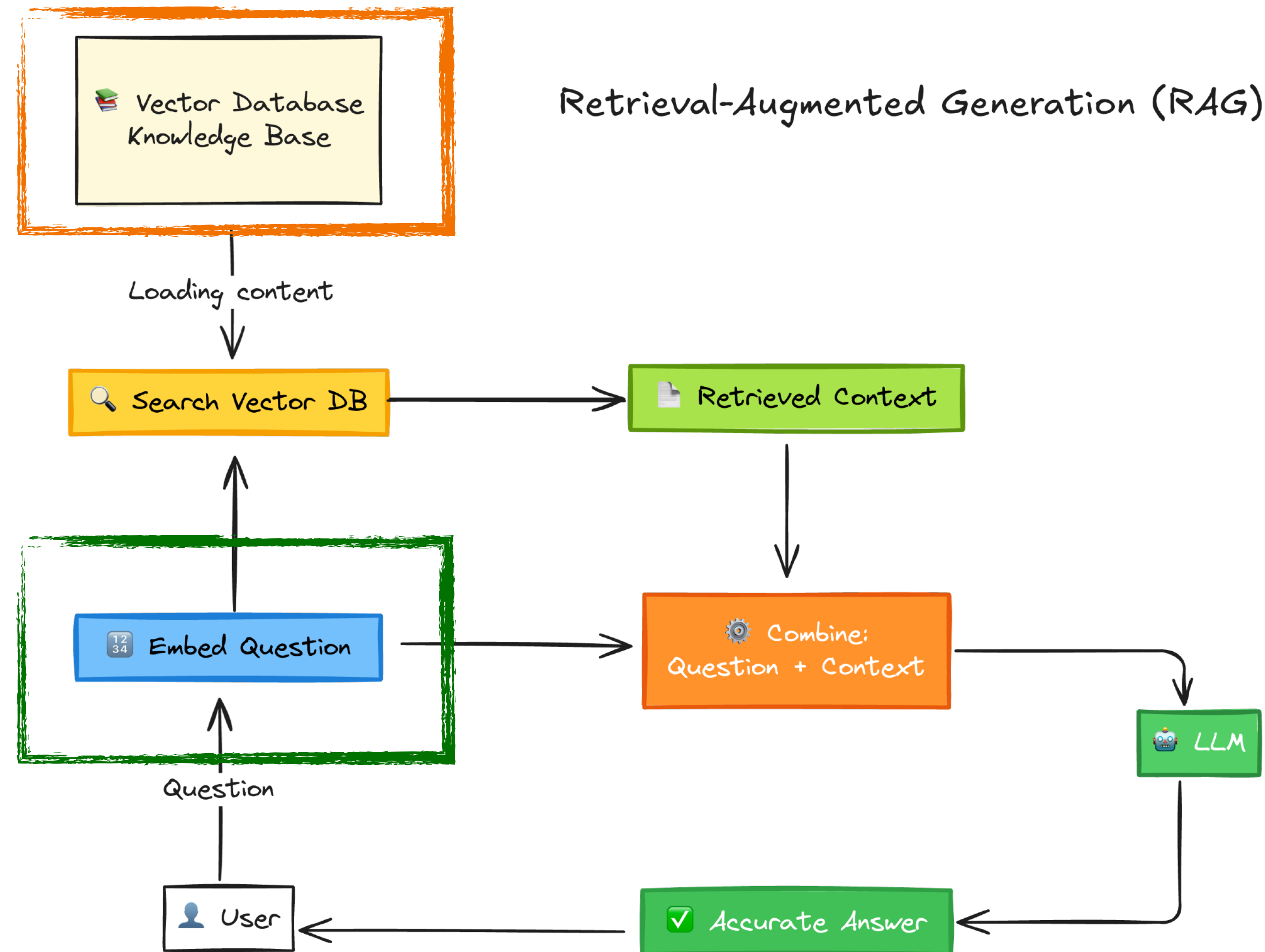
✗ Know your data

✗ Take any action

Adding Your Data



The first pass: RAG



RAG: old and busted?

- ✅ It works just fine
- 🟡 Batch Oriented
- ❌ MCP competes with it



What makes an Agent?

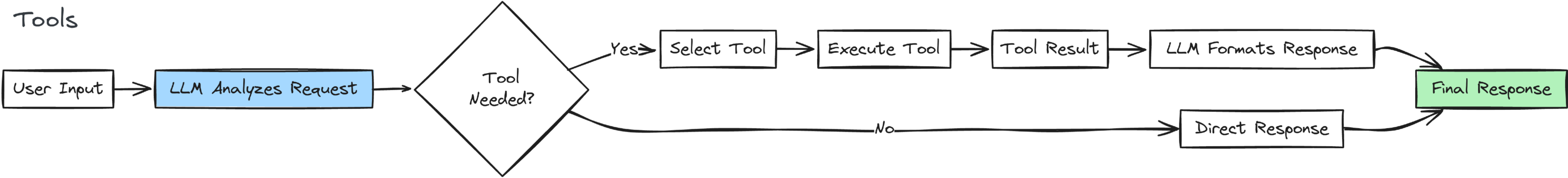
- ✓ small program
- ✓ calls an LLM
- ✓ takes action



Isn't that just a microservice?

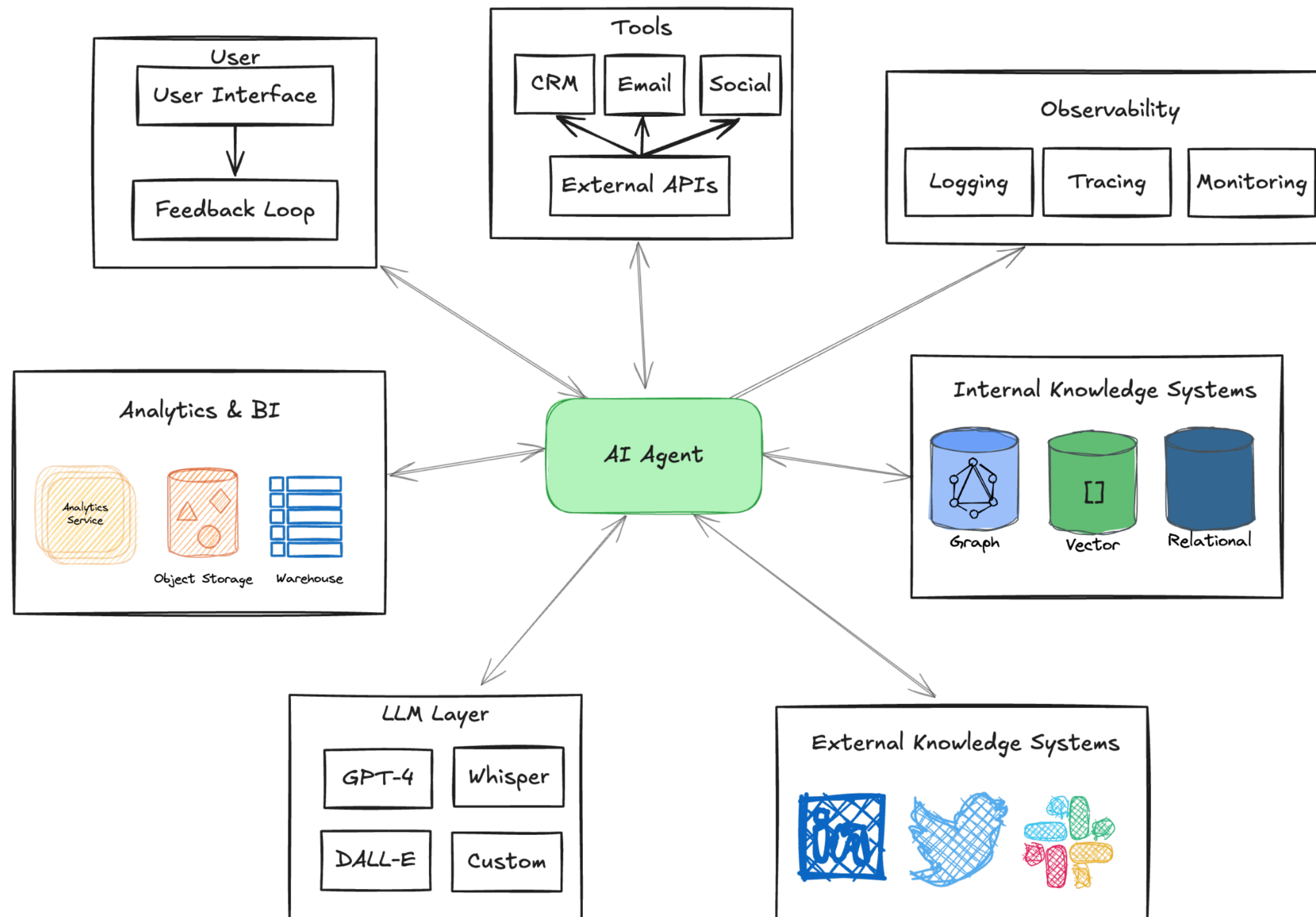


Calling External Tools



Agents at Scale are Complex Systems

They don't exist in isolation, they have many dependencies



The problem with rolling your own

- ✗ Tool integrations
- ✗ Resource integrations
- ✗ Discoverability

Introduction

SDKs

Concepts

Architecture Overview

Server Concepts

Client Concepts

Versioning

Tutorials

Using MCP >

Server Development >

Client Development >

FAQs

Introduction

📄 Copy page



☰ On this page

Choose Your Path

Ready to Build?

Get started with the Model Context Protocol (MCP)

MCP is an open protocol that standardizes how applications provide context to large language models (LLMs). Think of MCP like a USB-C port for AI applications. Just as USB-C provides a standardized way to connect your devices to various peripherals and accessories, MCP provides a standardized way to connect AI models to different data sources and tools. MCP enables you to build agents and complex workflows on top of LLMs and connects your models with the world.

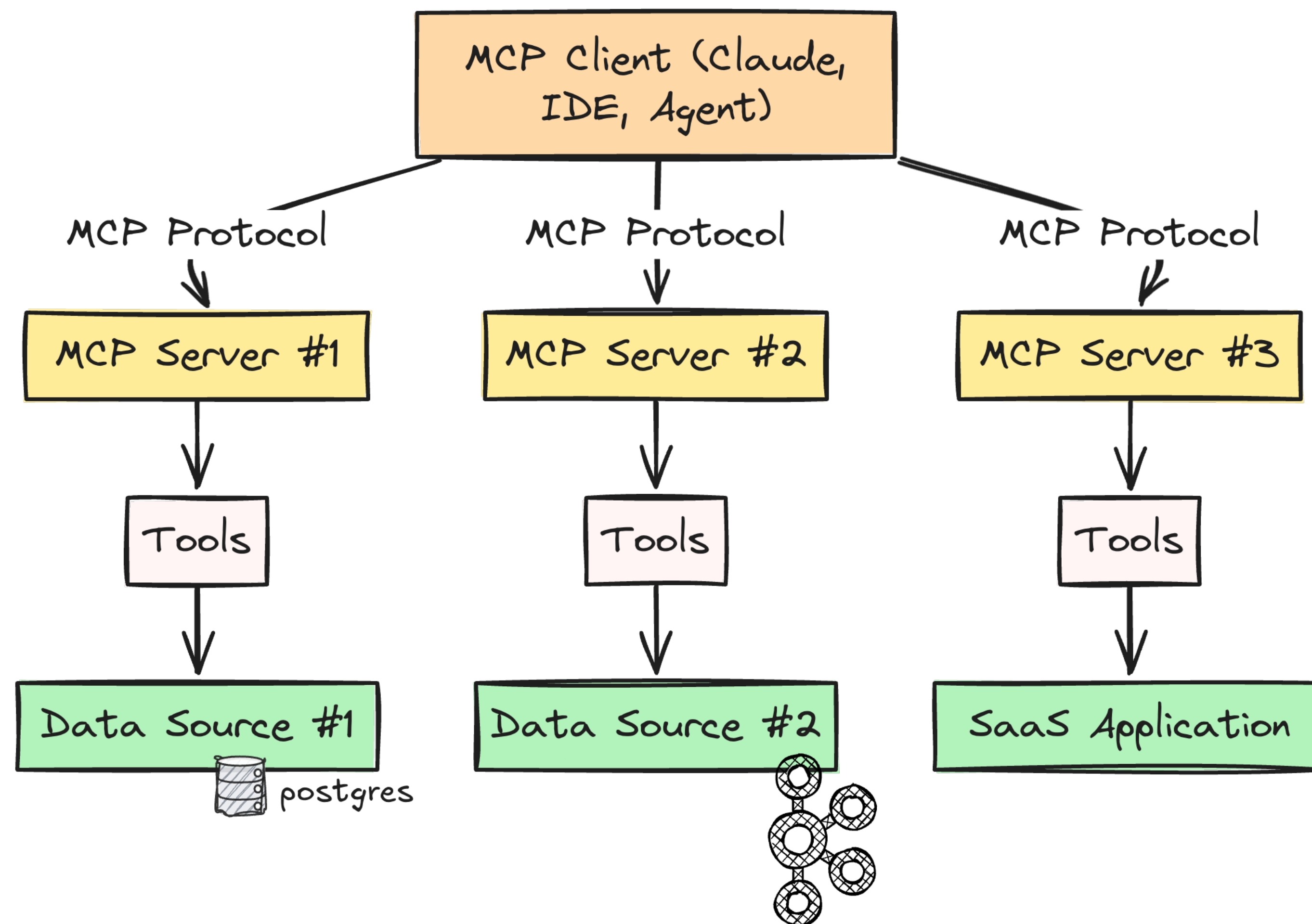
MCP provides:

- **A growing list of pre-built integrations** that your LLM can directly plug into
- **A standardized way** to build custom integrations for AI applications
- **An open protocol** that everyone is free to implement and use
- **The flexibility to change** between different apps and take your context with you

Choose Your Path



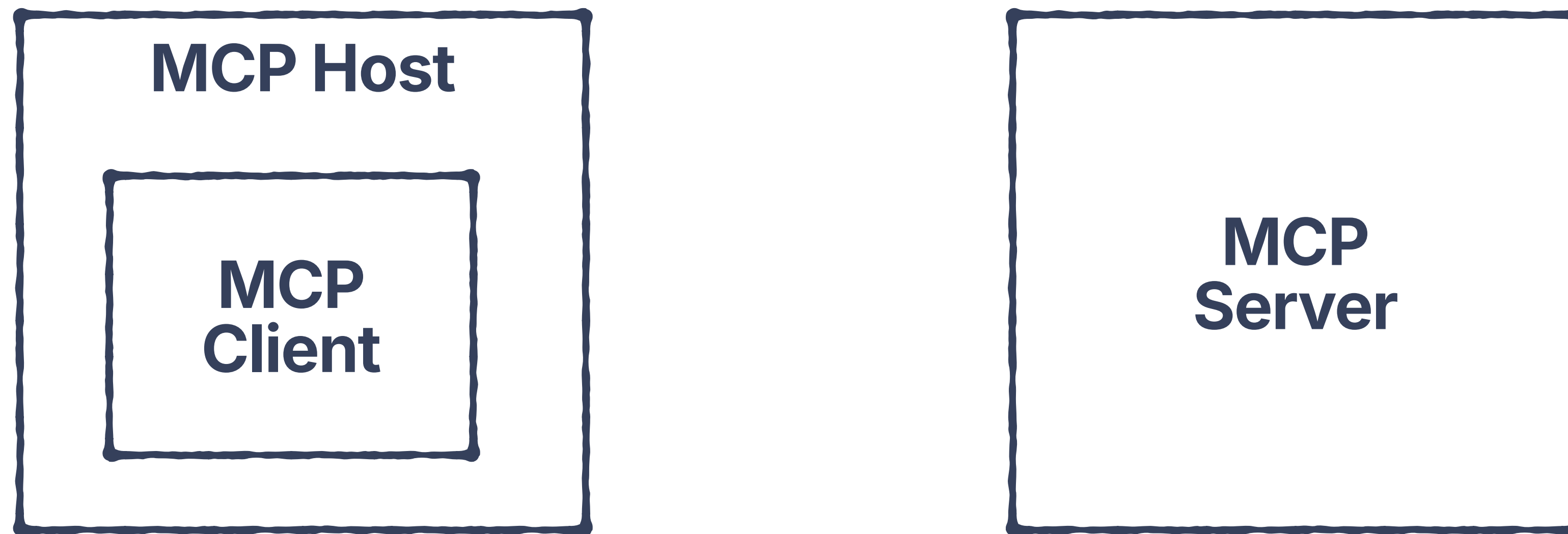
Model Context Protocol in a nutshell



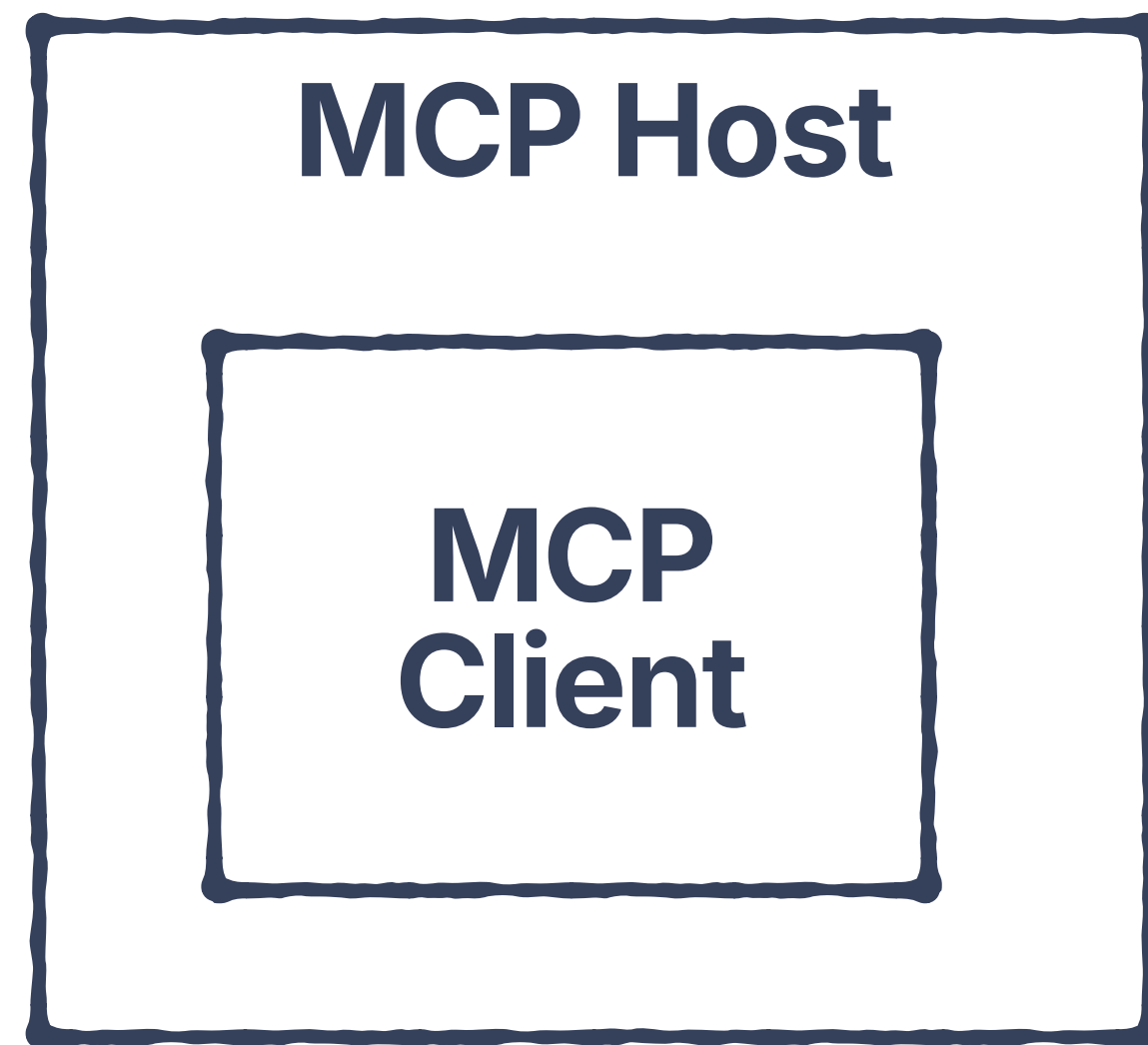
Model Context Protocol



Model Context Protocol

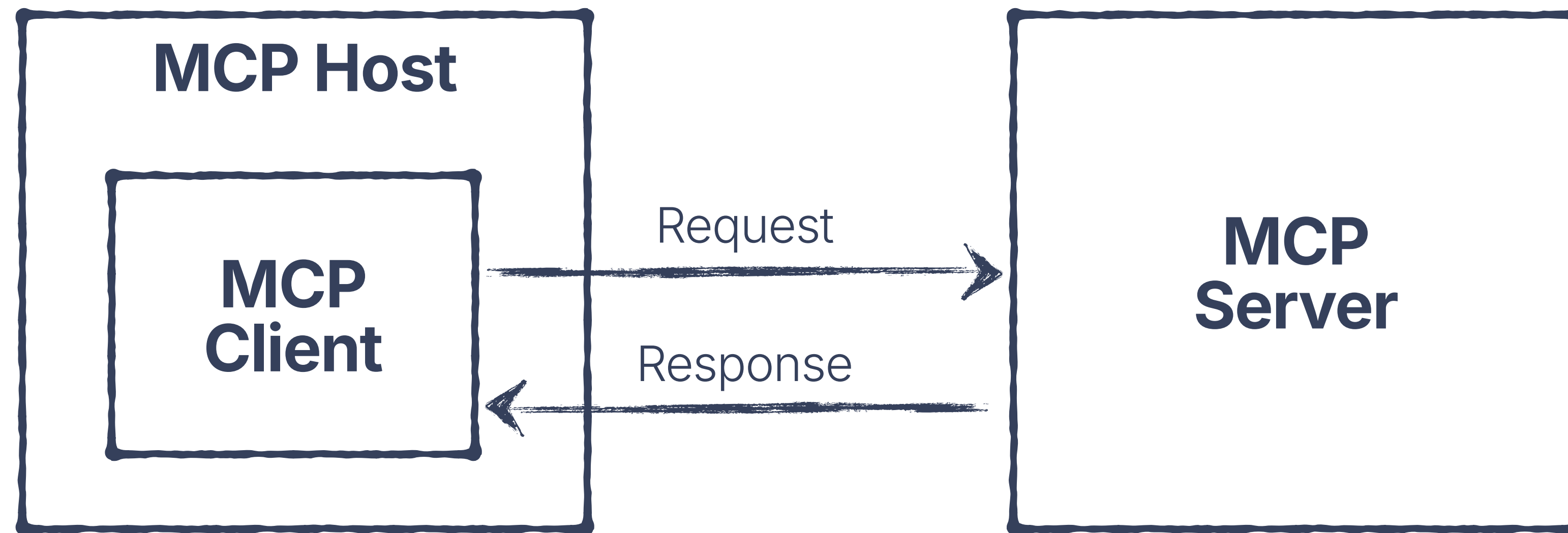


Model Context Protocol - Host

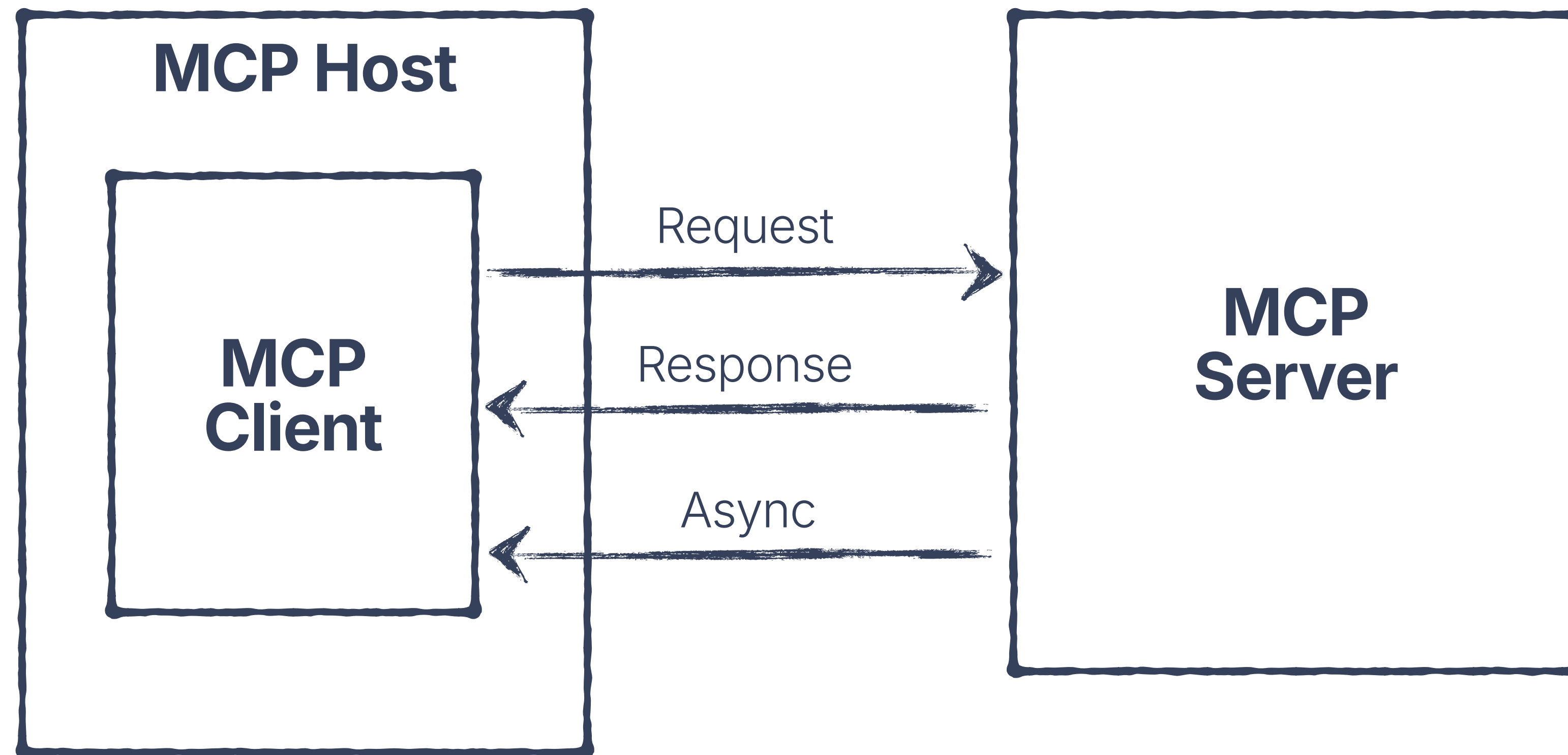


- Microservice
- Claude Desktop, etc.
- May contain multiple clients

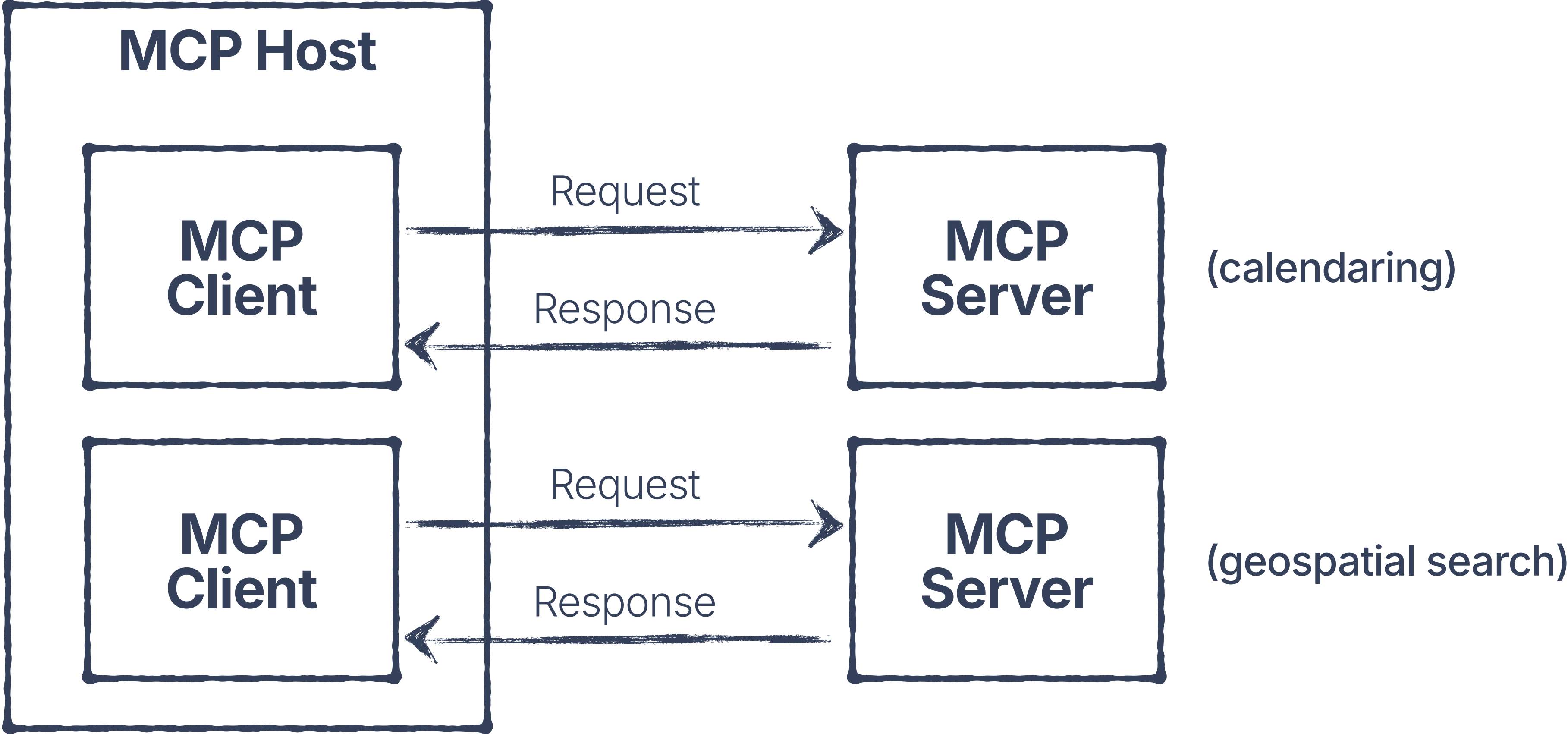
Model Context Protocol



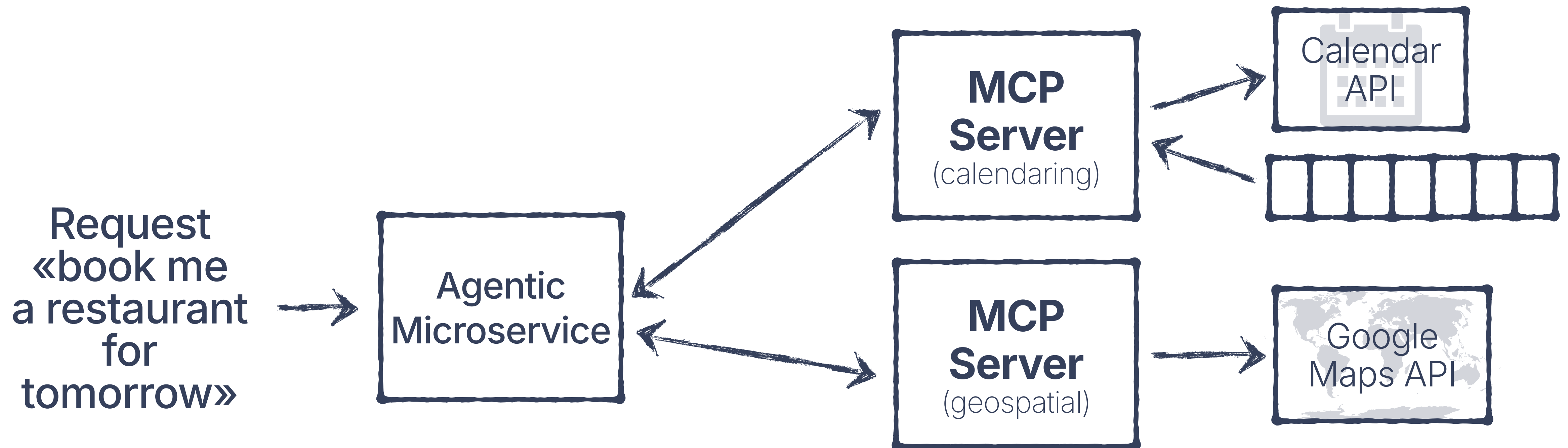
Model Context Protocol



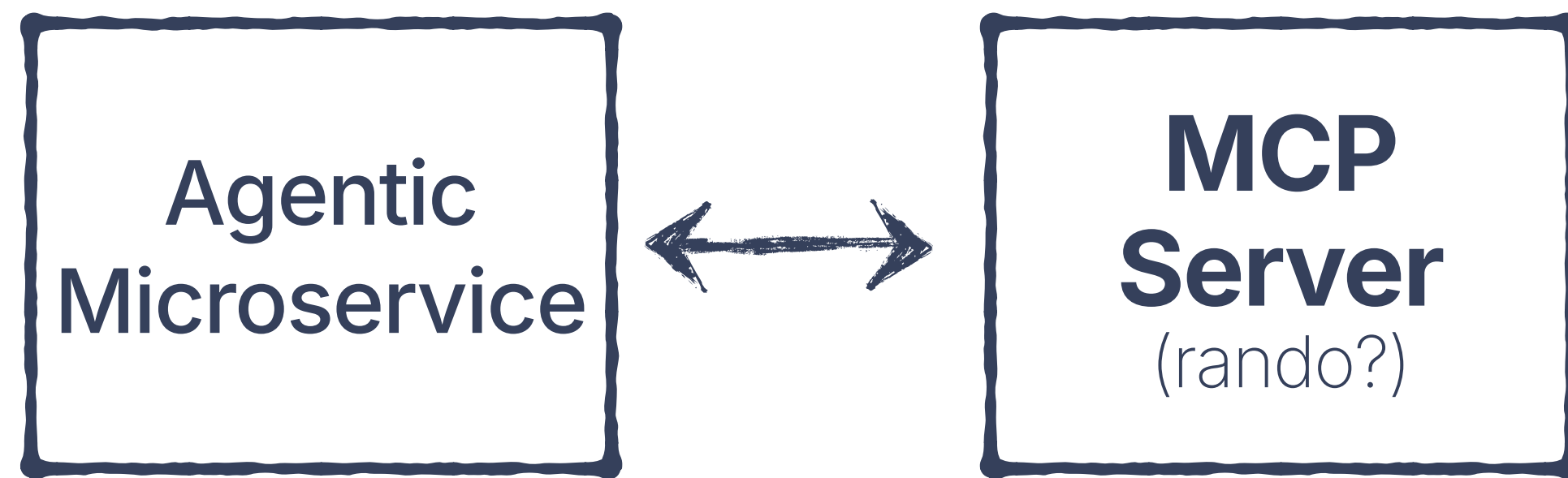
Model Context Protocol



Agents with MCP

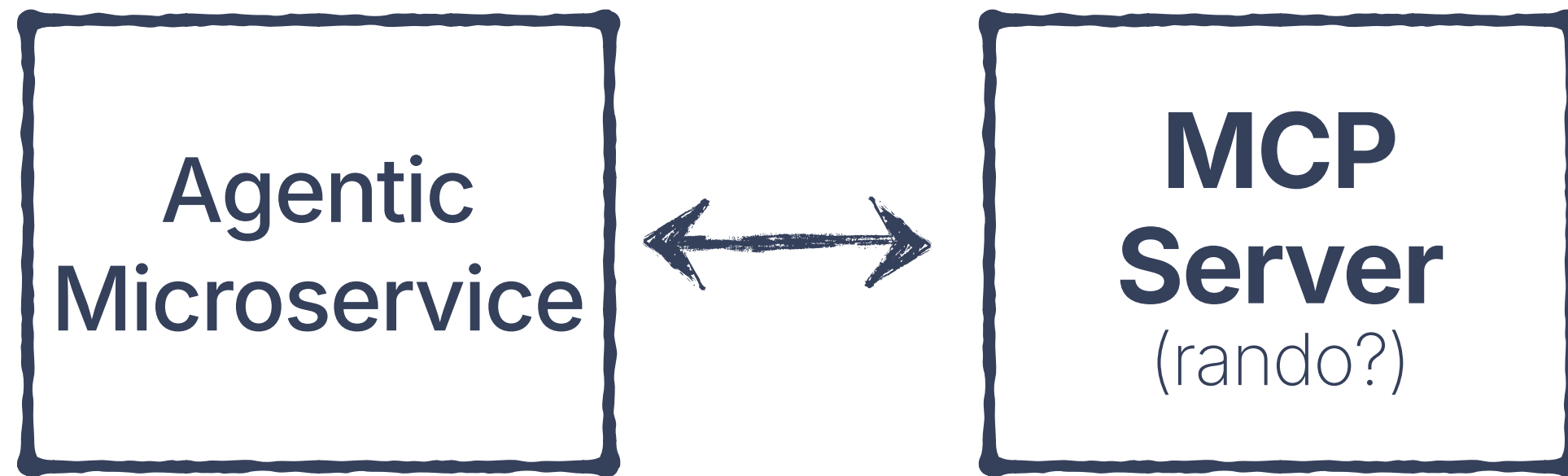


Discovery



- Agent exposes /capabilities (tools? prompts? resources?)
- Each resource has a description. These can be aggregated into the prompt.

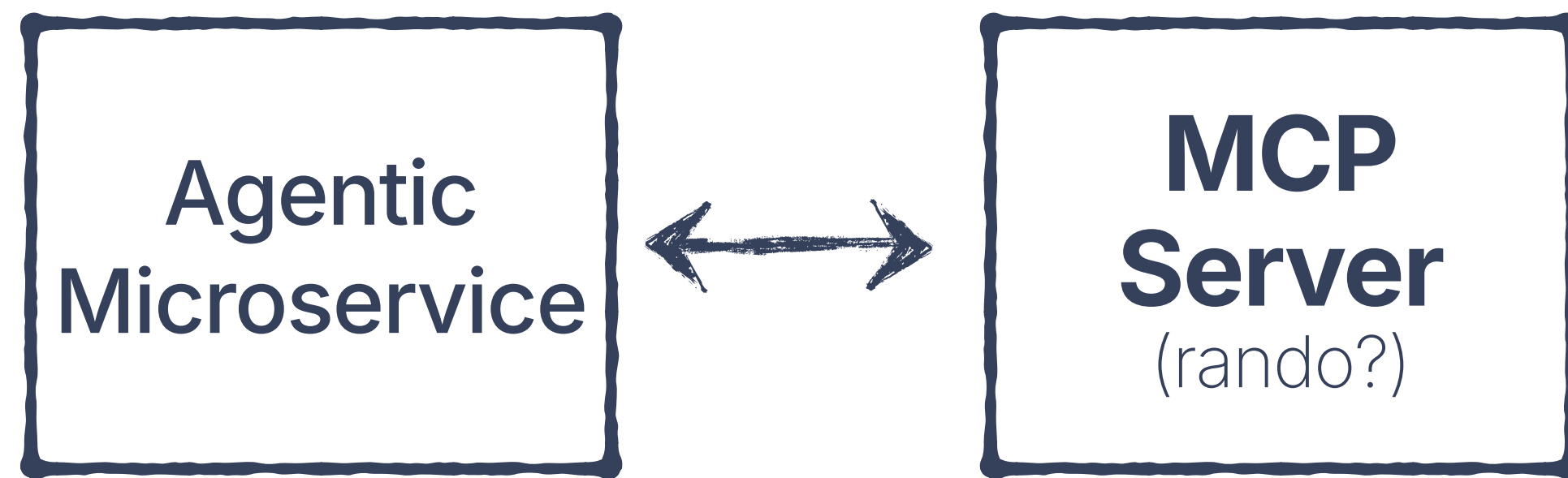
Discovery



"Set up coffee with me and Neal."

- Agent exposes /capabilities (tools? prompts? resources?)
- Each resource has a description. These can be aggregated into the prompt.

Discovery



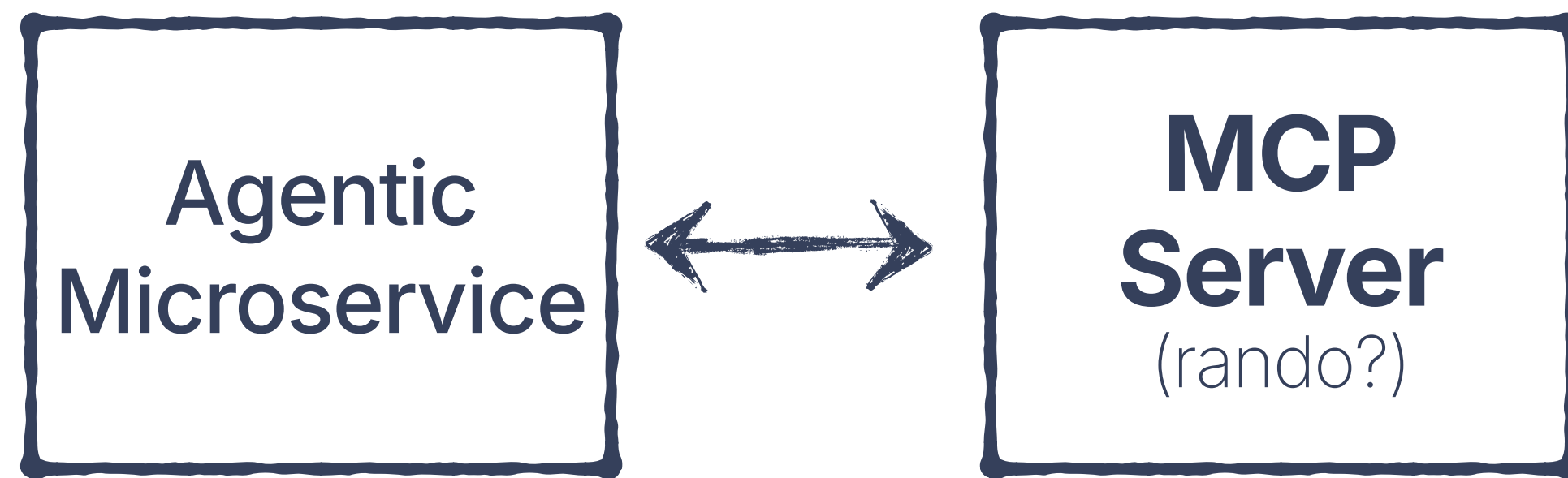
"Set up coffee with me and Dom."

You are a helpful scheduling agent with access to (upon request):

- * A geospatial API that can find meeting places near a location in a given price range and meeting style
- * Complete access to my calendar

- Agent exposes /capabilities (tools? prompts? resources?)
- Each resource has a description. These can be aggregated into the prompt.

Discovery



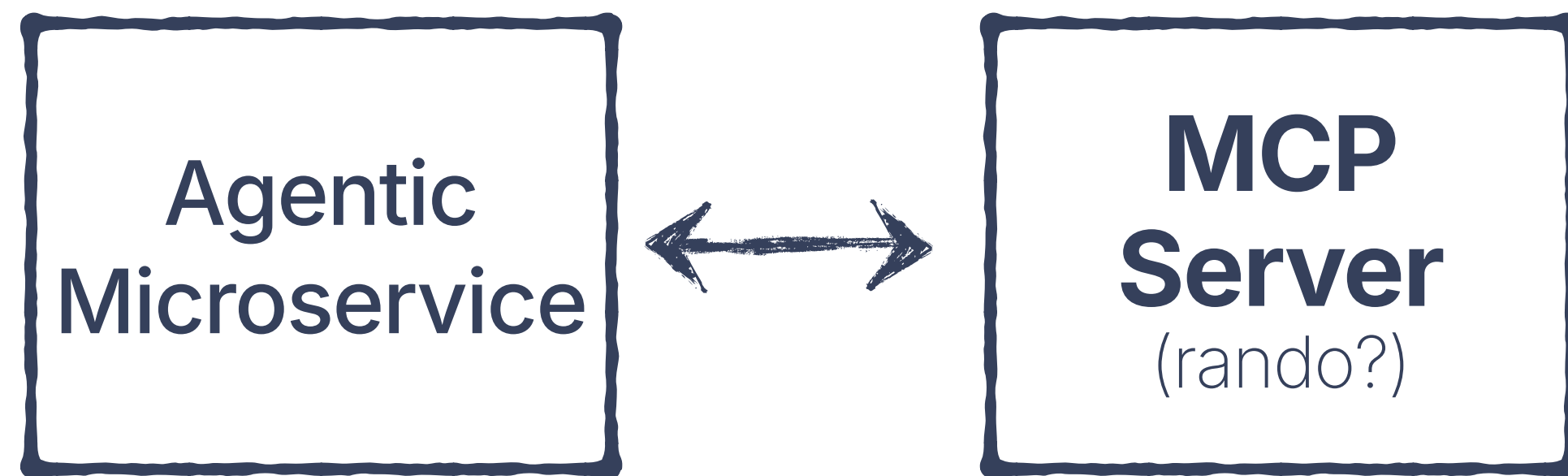
"Set up coffee with me and Neal."

You are a helpful scheduling agent with access to (upon request):

- * A geospatial API that can find meeting places near a location in a given price range and meeting style
- * Complete access to my calendar

- Agent exposes /capabilities (tools? prompts? resources?)
- Each resource has a description. These can be aggregated into the prompt.
- Each tool has a description and a schema. Common foundation model APIs directly support tool descriptions.

Discovery



Q: What do you, as the microservice author, need to enable this?

A: a URL

What MCP gives you

- ✓ Context Management
- ✓ Tool invocation
- ✓ Discovery
- ✓ Composition

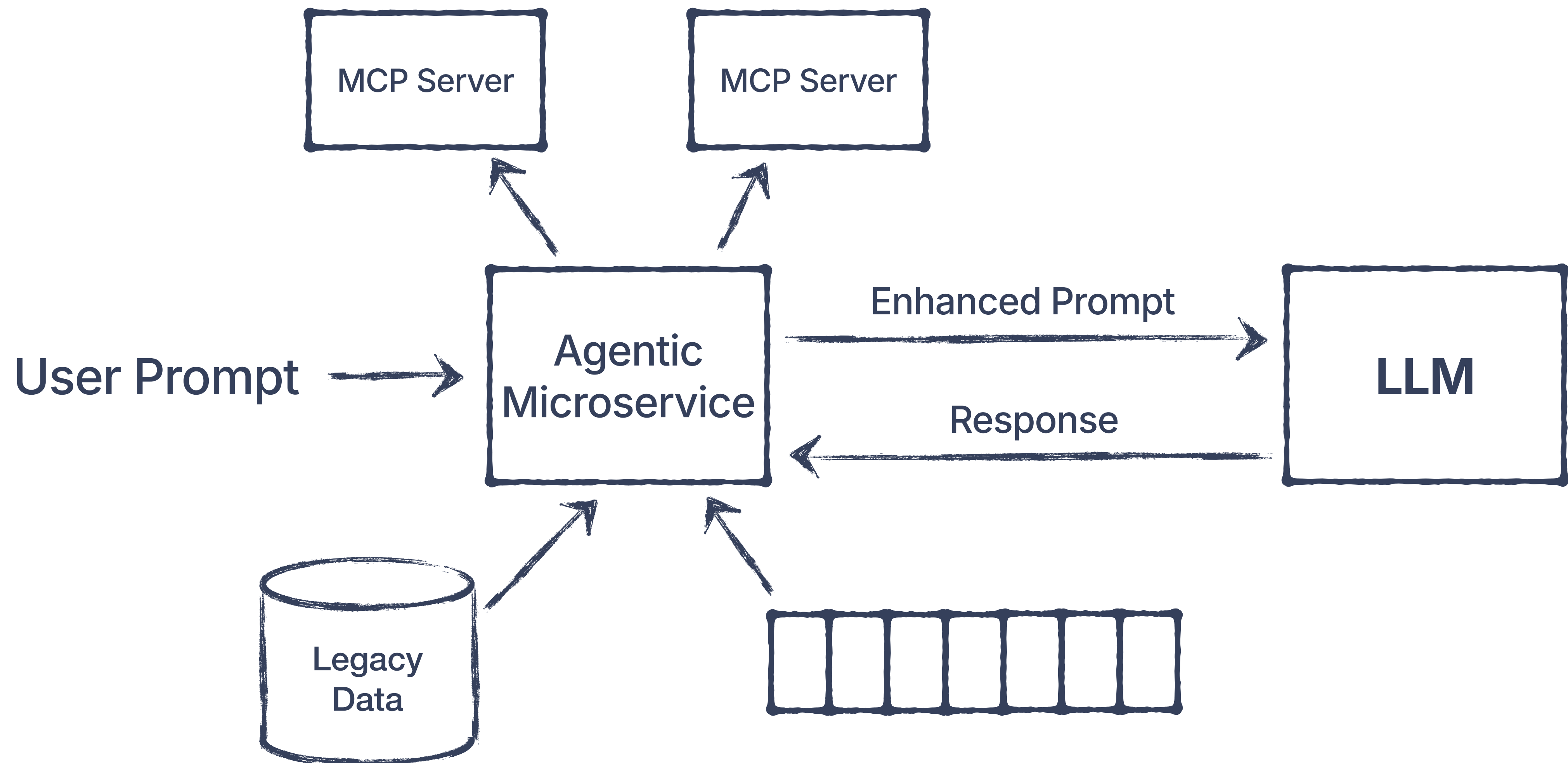
When not to use MCP

 When it's all internal

When to write agents in the first place

- ✓ Natural language input
- ✓ Probabilistic results
- ✗ LinkedInfluencer said so

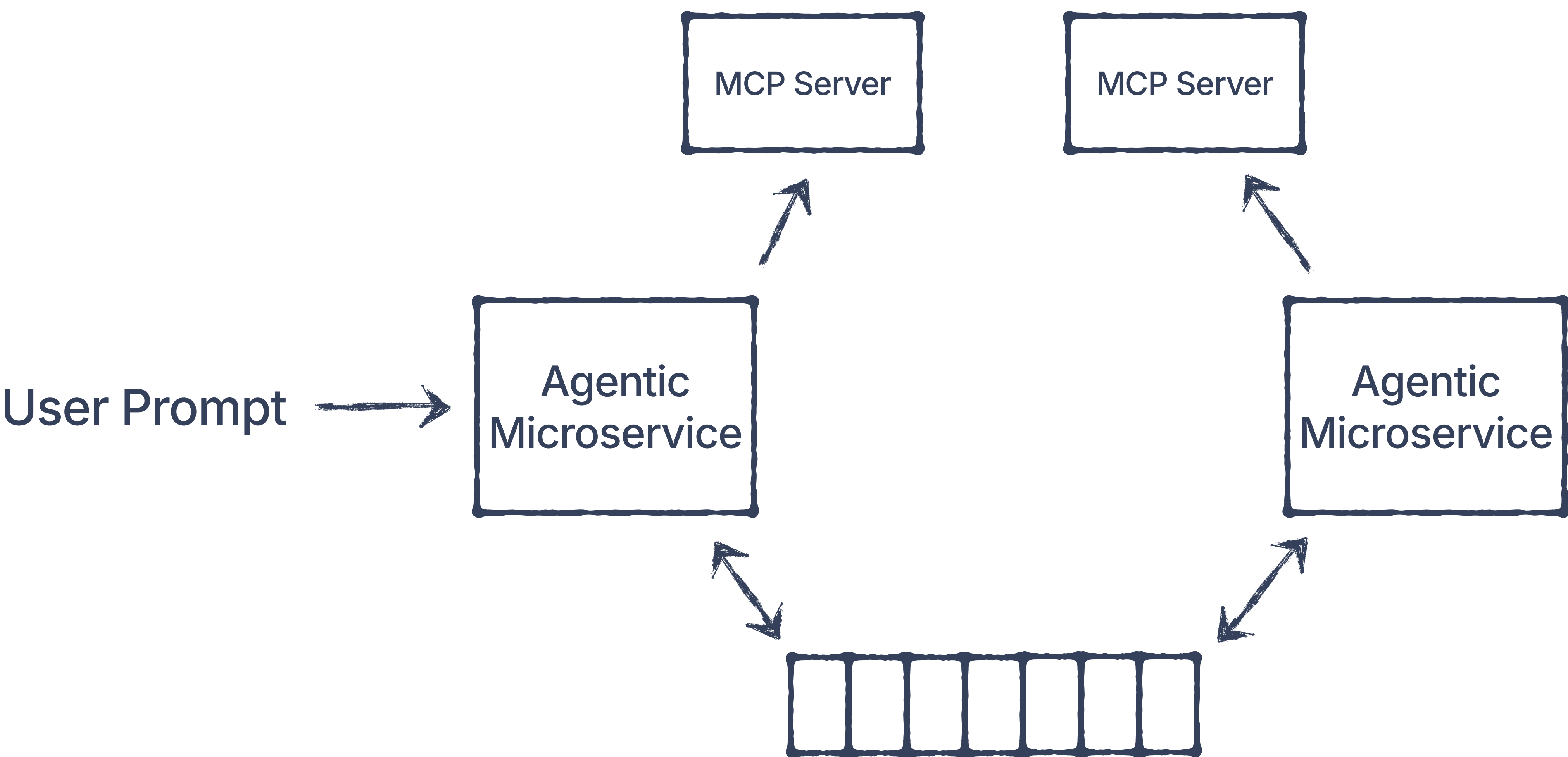
How agents will evolve



Multi-agent architecture (A2A)



Multi-agent architecture (streaming)



As always,

Have a Nice Day...

**X/Bluesky:
@gamussa**

<http://speaking.gamov.io>