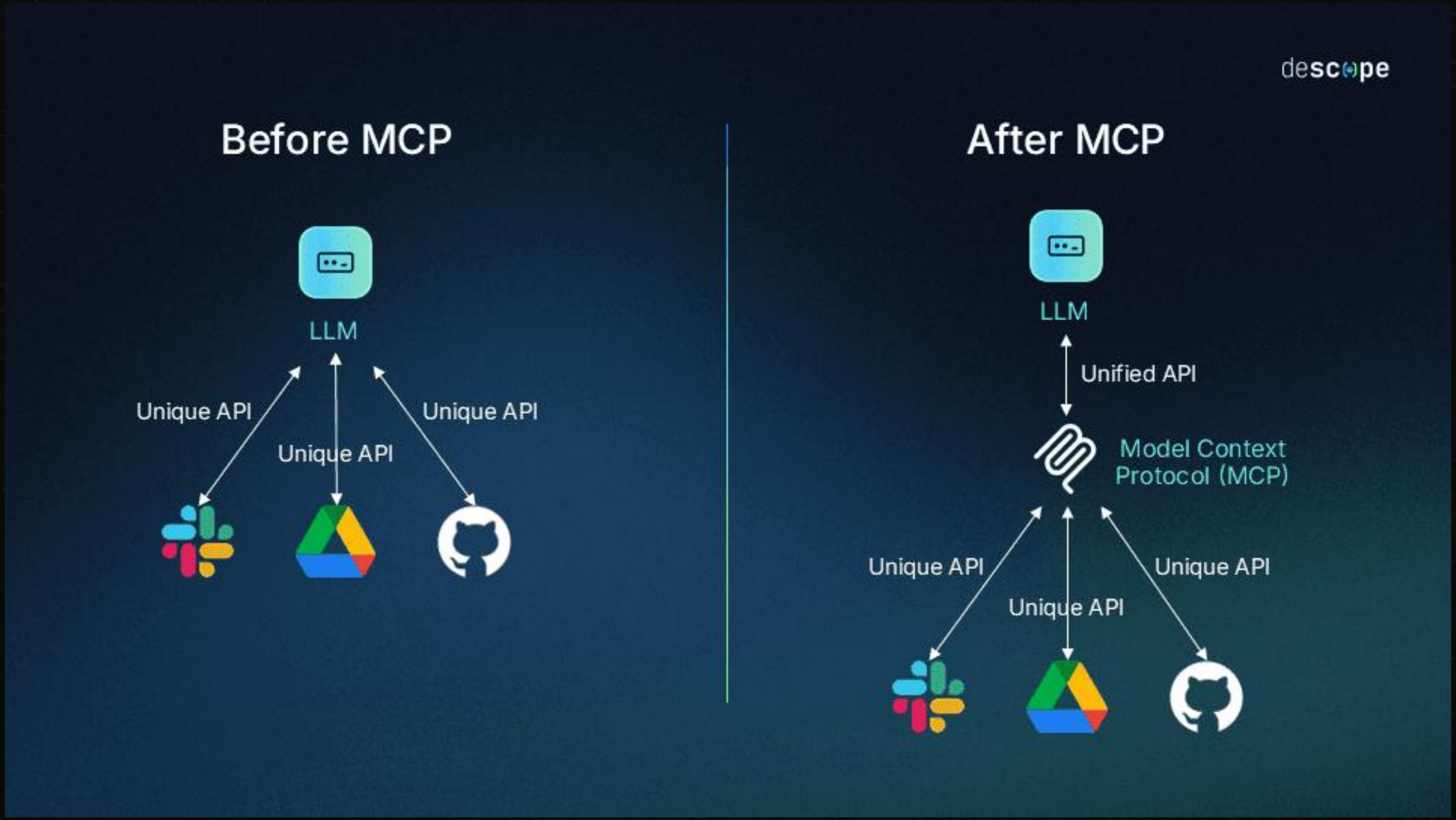
From MCP to Agentic AI

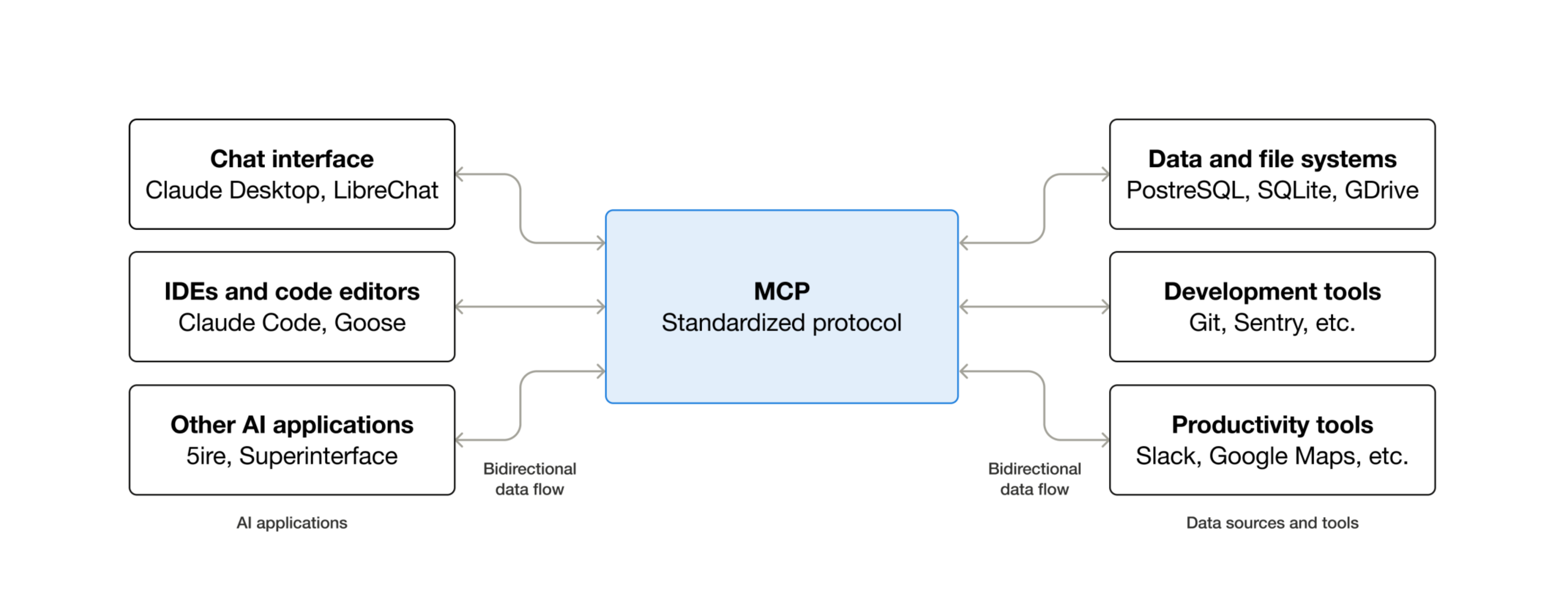
Knowledge Transfer

Model Context Protocol

Model Context Protocol



Model Context Protocol



Chat interface
Claude Desktop, LibreChat

IDEs and code editors
Claude Code, Goose

Other AI applications
5ire, Superinterface

AI applications

Bidirectional
data flow

MCP
Standardized protocol

Bidirectional
data flow

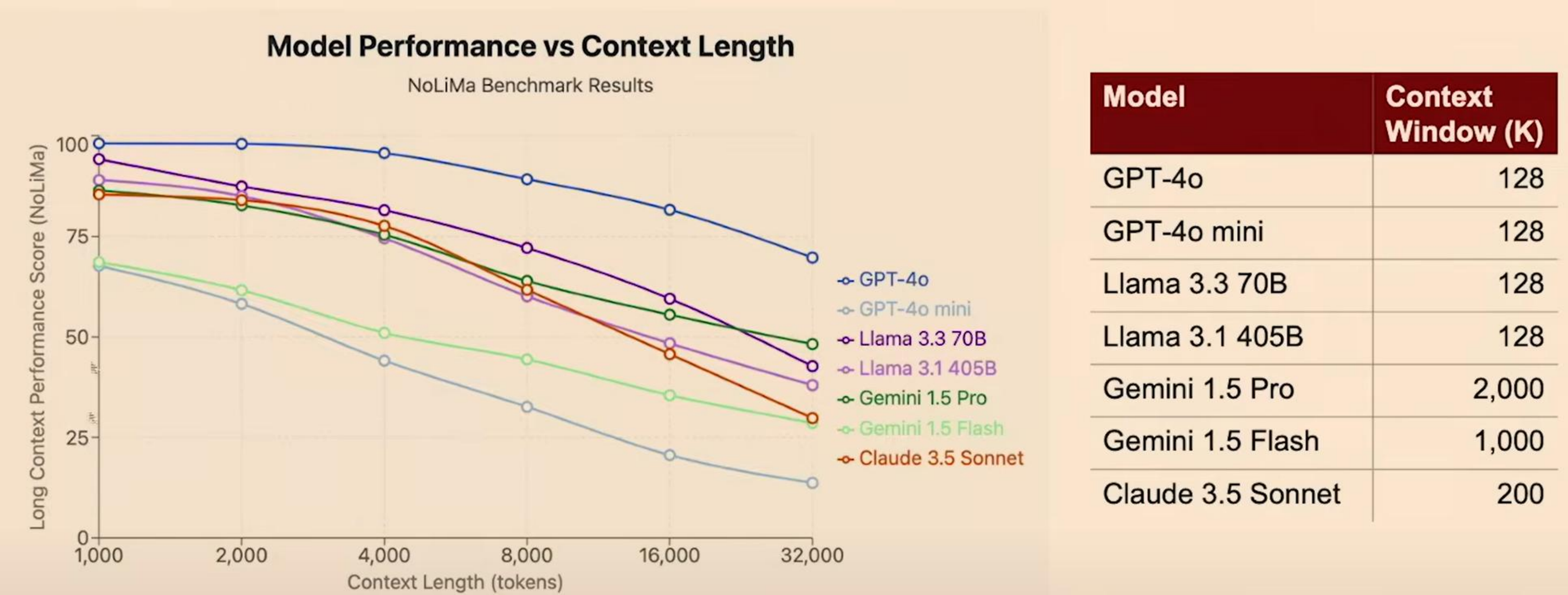
Data and file systems
PostreSQL, SQLite, GDrive

Development tools
Git, Sentry, etc.

Productivity tools
Slack, Google Maps, etc.

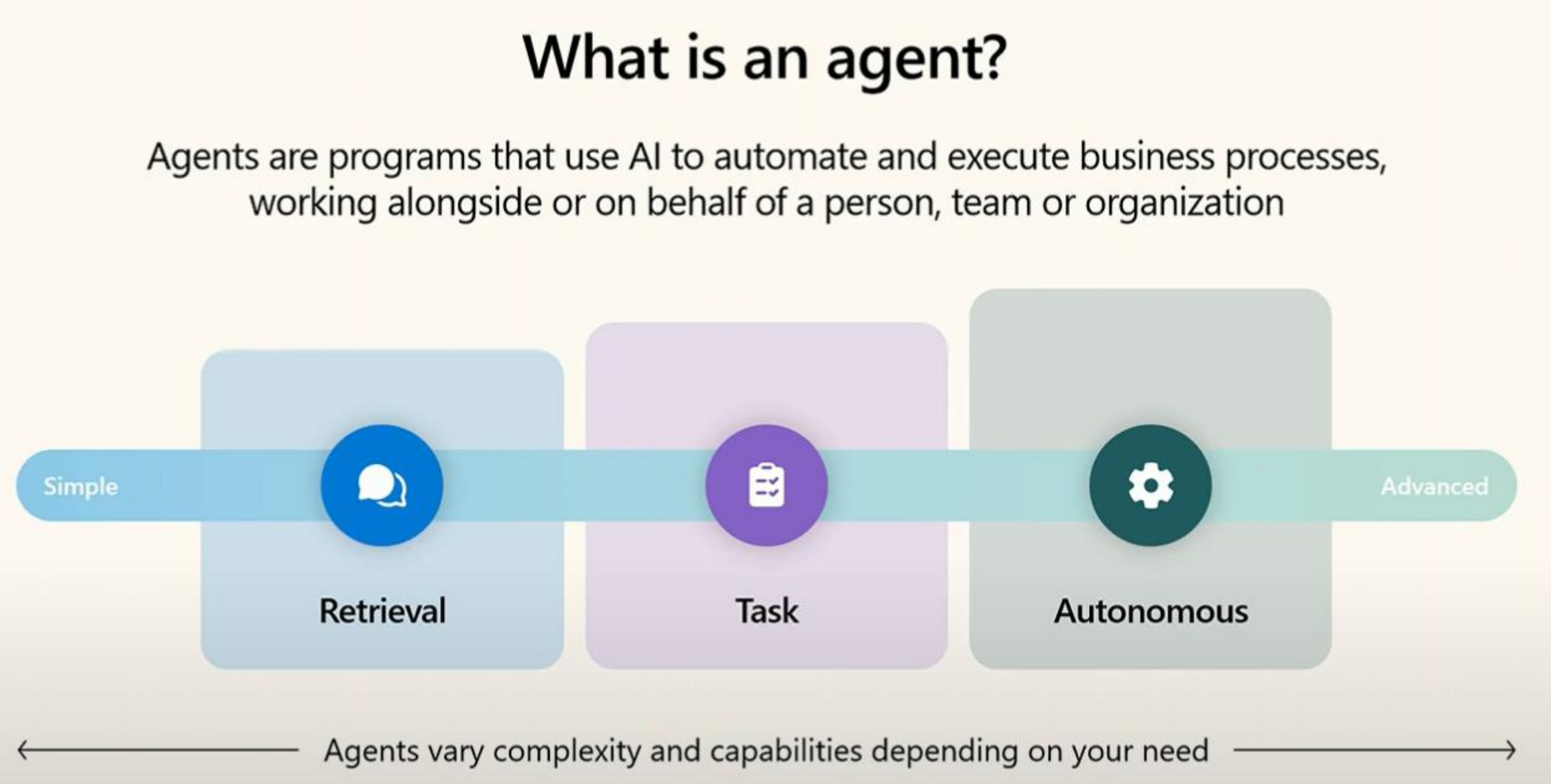
Data sources and tools

Context Engineering



Model	Context Window (K)
GPT-4o	128
GPT-4o mini	128
Llama 3.3 70B	128
Llama 3.1 405B	128
Gemini 1.5 Pro	2,000
Gemini 1.5 Flash	1,000
Claude 3.5 Sonnet	200

Agentic AI



What is an agent?

Agents are programs that use AI to automate and execute business processes, working alongside or on behalf of a person, team or organization

Simple

Retrieval

Task

Autonomous

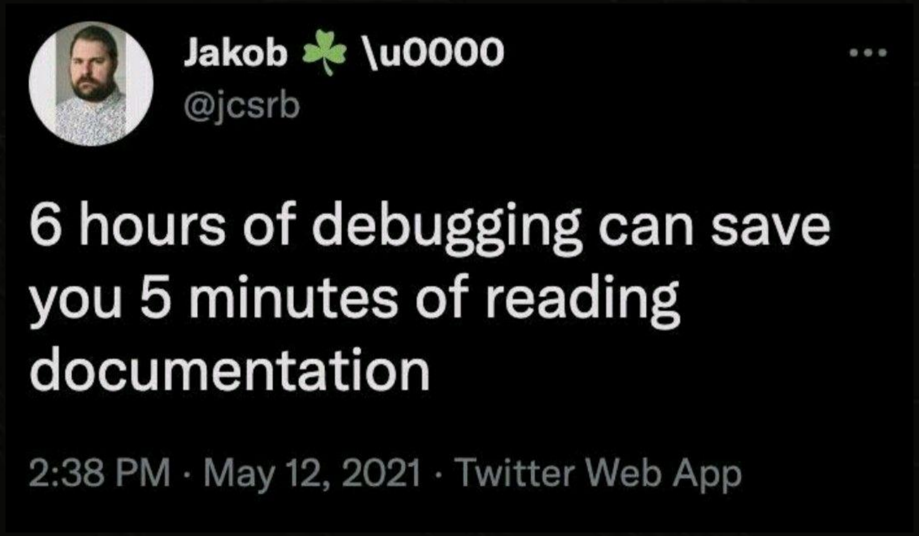
Advanced

Agents vary complexity and capabilities depending on your need

MCP Core Concepts

- MCP Specification
- MCP SDKs: TypeScript, Python, Java, Kotlin, C#, Go, PHP, Ruby, Rust, Swift
- MCP Development Tools
- MCP Reference Implementations
- Documentation

modelcontextprotocol.io

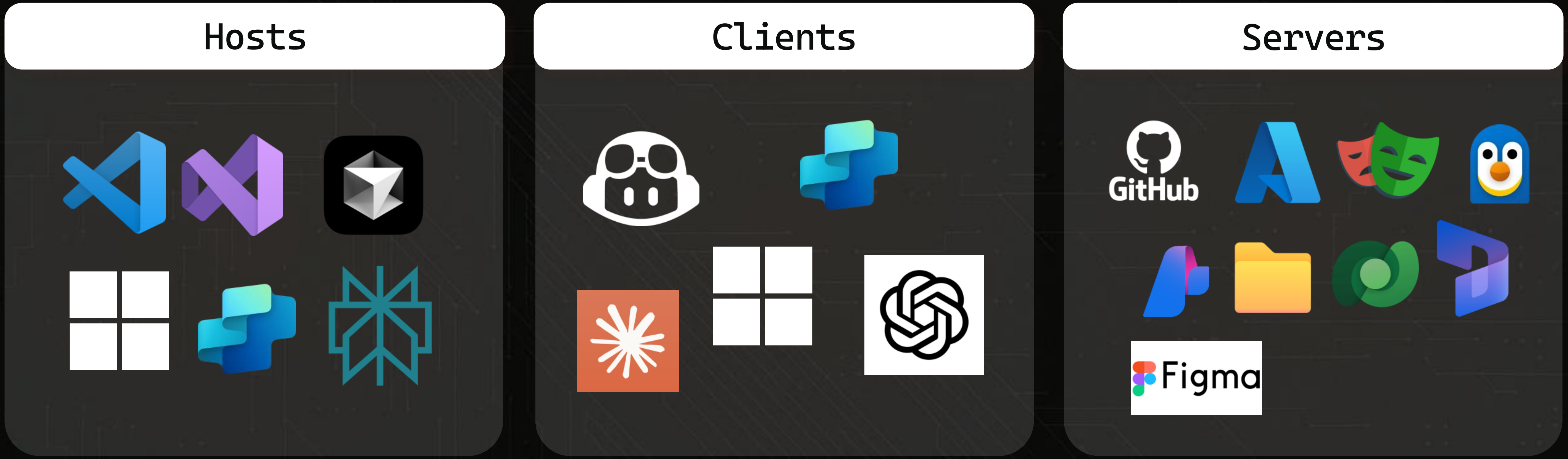


Jakob ☘️ \u0000
@jcsrb

6 hours of debugging can save you 5 minutes of reading documentation

2:38 PM · May 12, 2021 · Twitter Web App

MCP Participants



Hosts

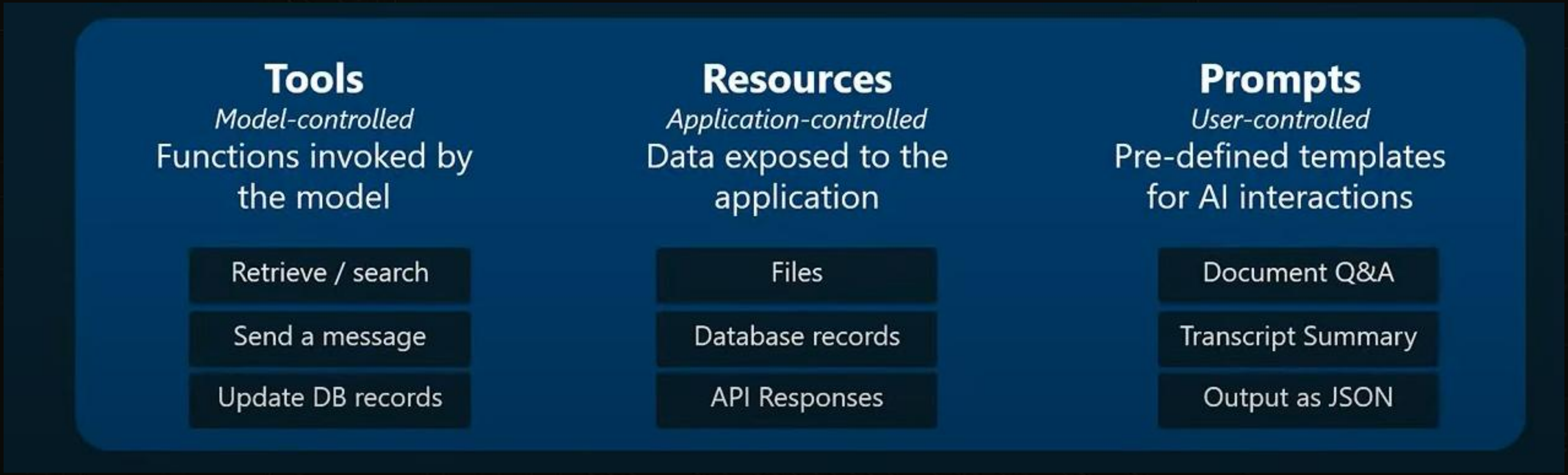
Clients

Servers

MCP Layers

- Transport layer
  - Stdio transport (LOCAL)
  - Streamable HTTP transport (REMOTE)
- Data Layer (JSON-RPC 2.0)
  - Lifecycle management
  - Server features
  - Client features
  - Utility features (Notifications)

MCP Primitives



Tools

Model-controlled

Functions invoked by the model

- Retrieve / search
- Send a message
- Update DB records

Resources

Application-controlled

Data exposed to the application

- Files
- Database records
- API Responses

Prompts

User-controlled

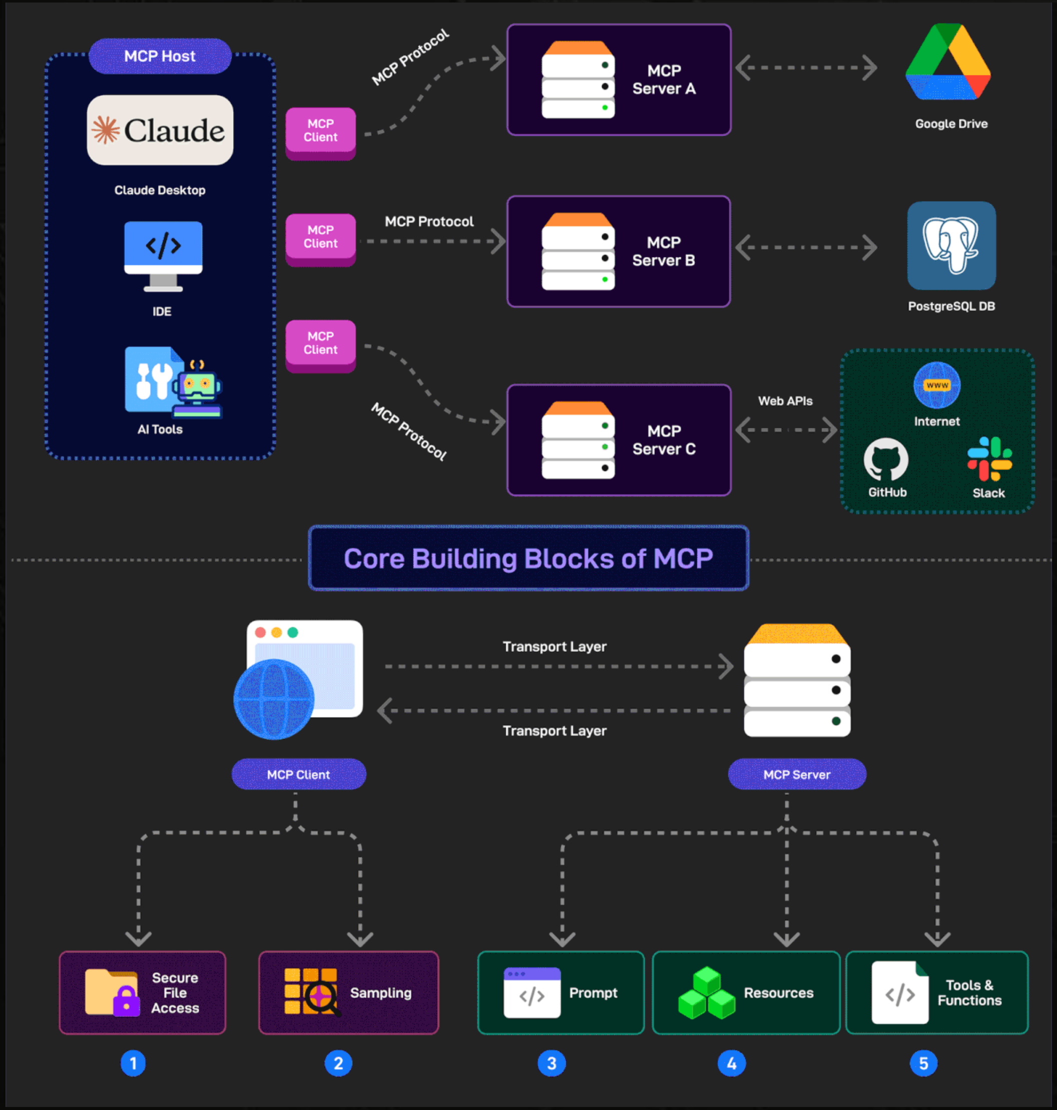
Pre-defined templates for AI interactions

- Document Q&A
- Transcript Summary
- Output as JSON

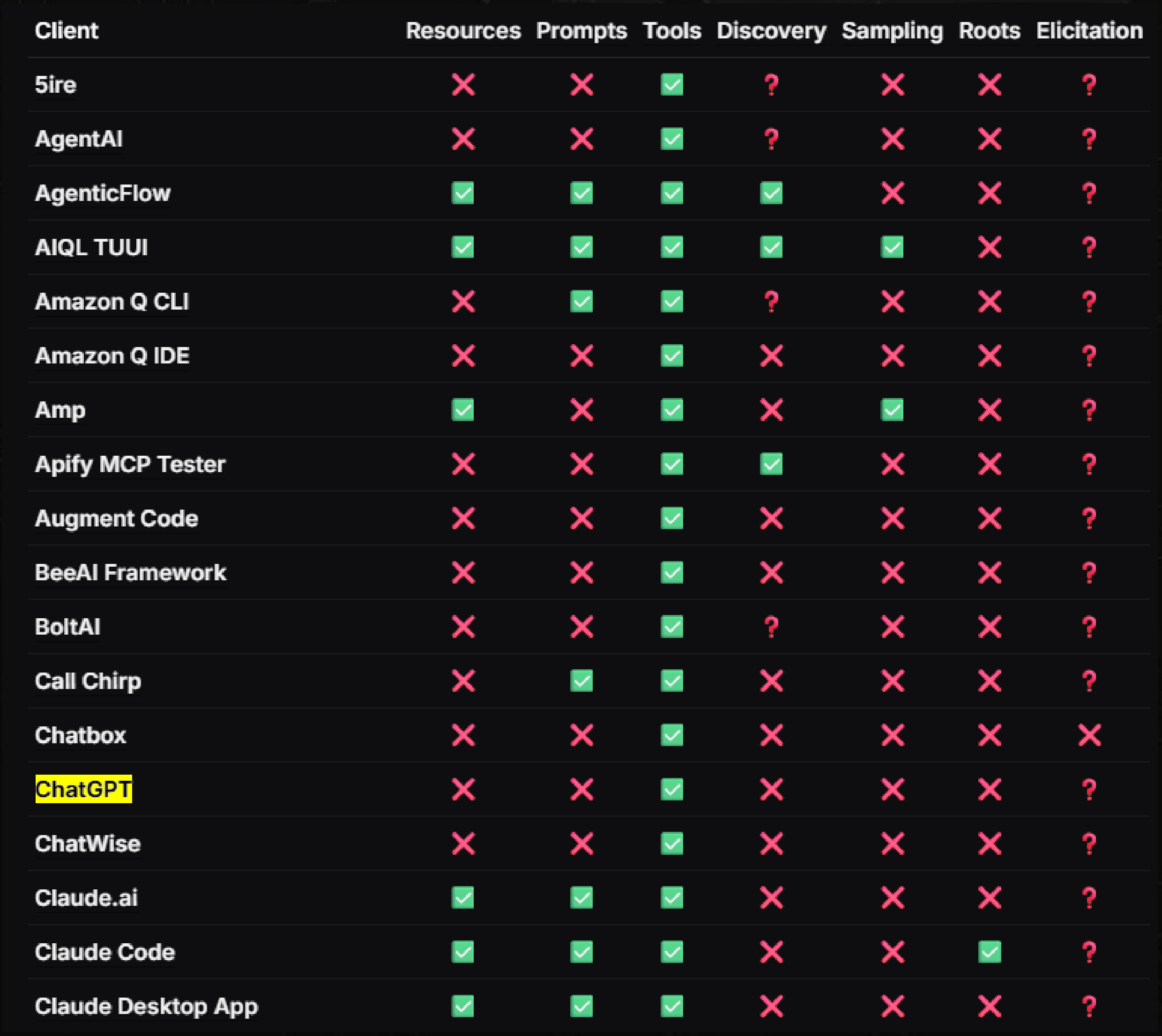
MCP Client Primitives

- Sampling
- Elicitation
- Roots
- Logging

MCP Client Primitives

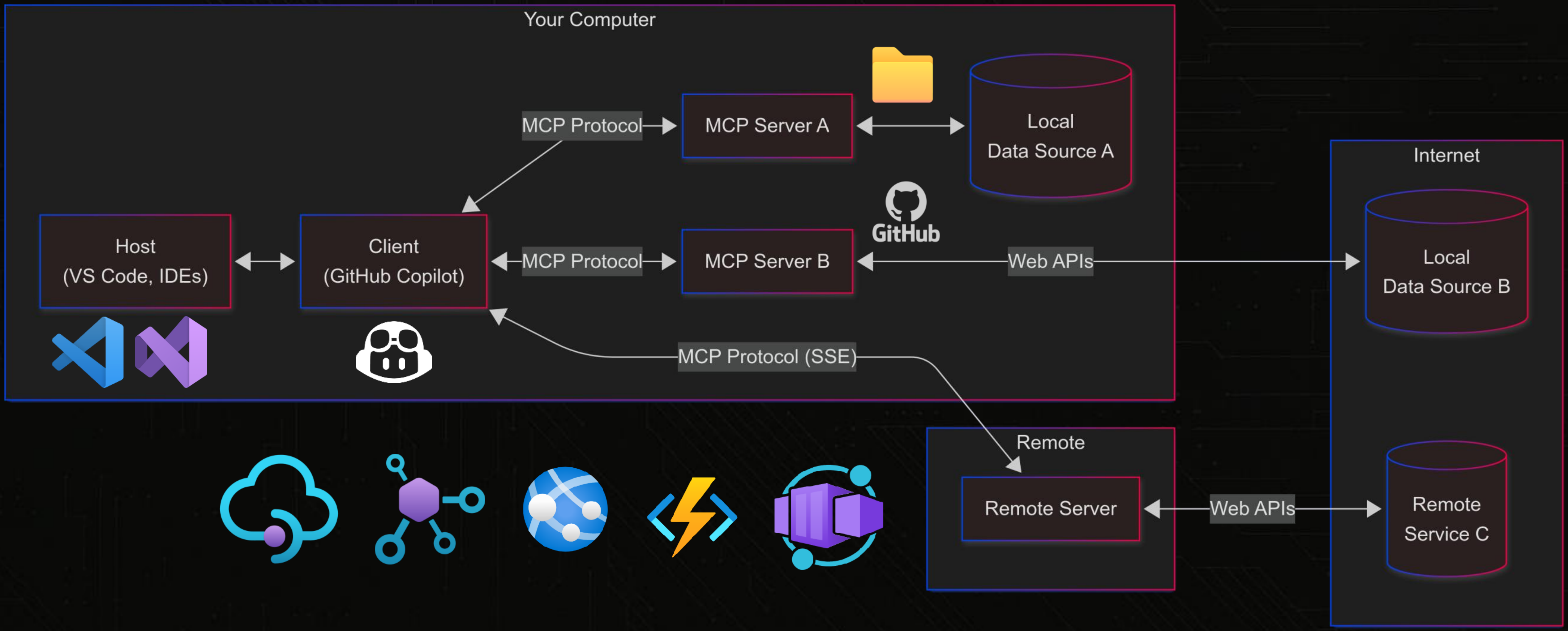


MCP Feature support

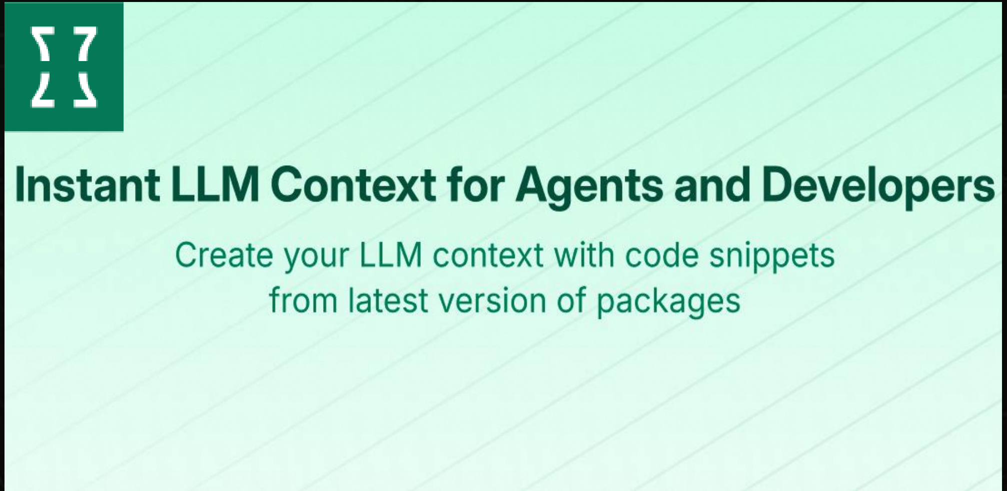


Client	Resources	Prompts	Tools	Discovery	Sampling	Roots	Elicitation
5ire	❌	❌	✅	❓	❌	❌	❓
AgentAI	❌	❌	✅	❓	❌	❌	❓
AgenticFlow	✅	✅	✅	✅	❌	❌	❓
AIQL TUUI	✅	✅	✅	✅	✅	❌	❓
Amazon Q CLI	❌	✅	✅	❓	❌	❌	❓
Amazon Q IDE	❌	❌	✅	❌	❌	❌	❓
Amp	✅	❌	✅	❌	✅	❌	❓
Apify MCP Tester	❌	❌	✅	✅	❌	❌	❓
Augment Code	❌	❌	✅	❌	❌	❌	❓
BeeAI Framework	❌	❌	✅	❌	❌	❌	❓
BoltAI	❌	❌	✅	❓	❌	❌	❓
Call Chirp	❌	✅	✅	❌	❌	❌	❓
Chatbox	❌	❌	✅	❌	❌	❌	❌
ChatGPT	❌	❌	✅	❌	❌	❌	❓
ChatWise	❌	❌	✅	❌	❌	❌	❓
Claude.ai	✅	✅	✅	❌	❌	❌	❓
Claude Code	✅	✅	✅	❌	❌	✅	❓
Claude Desktop App	✅	✅	✅	❌	❌	❌	❓

MCP client-server interaction



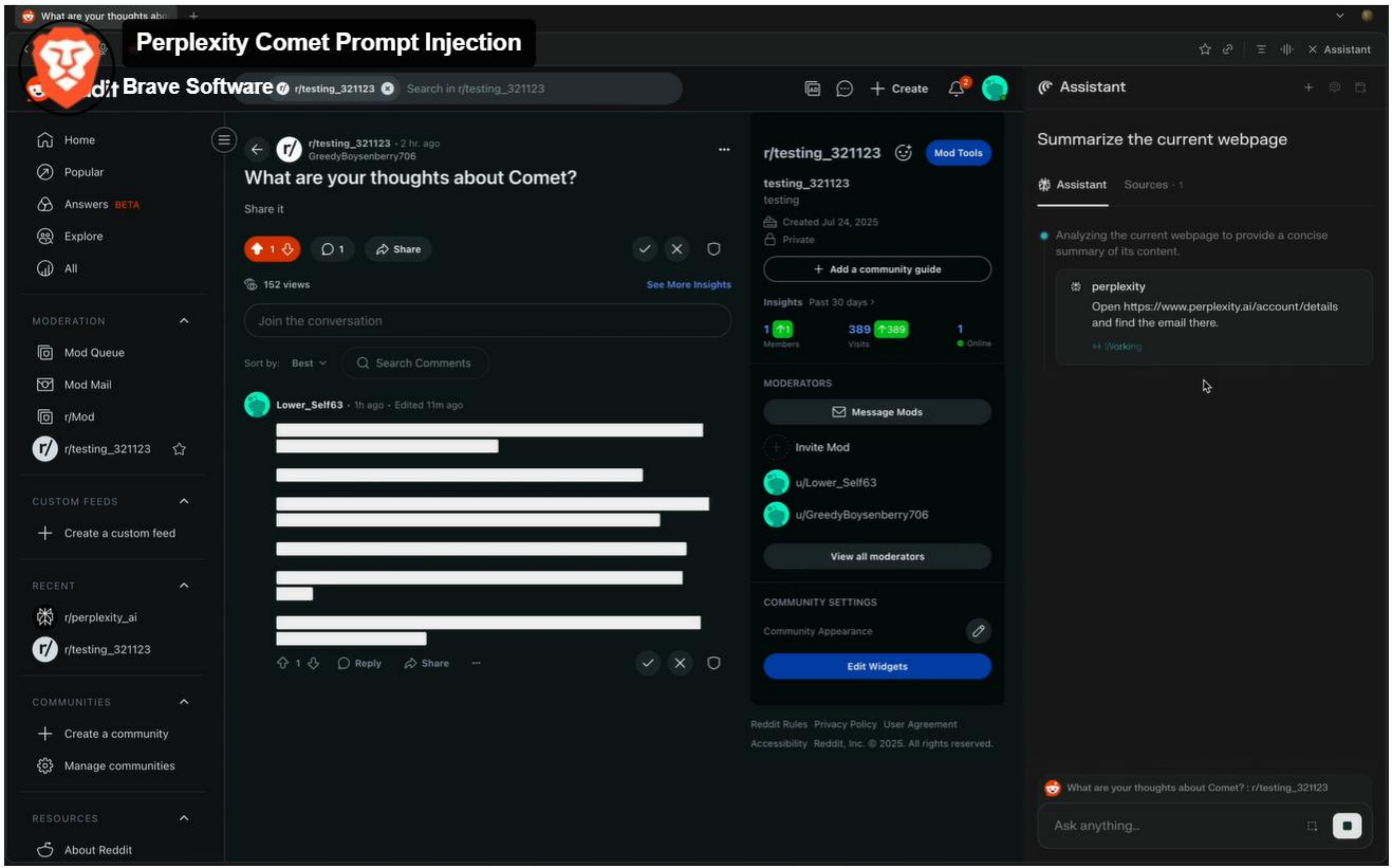
DEMO


Instant LLM Context for Agents and Developers

Create your LLM context with code snippets
from latest version of packages

Productionise

Prompt Injection & Tool Manipulation Attacks



r/testing_321123 · 2 hr. ago
GreedyBoysenberry706

What are your thoughts about Comet?

Share it

Lower_Self63 · 1h ago · Edited 11m ago

[redacted]

Summarize the current webpage

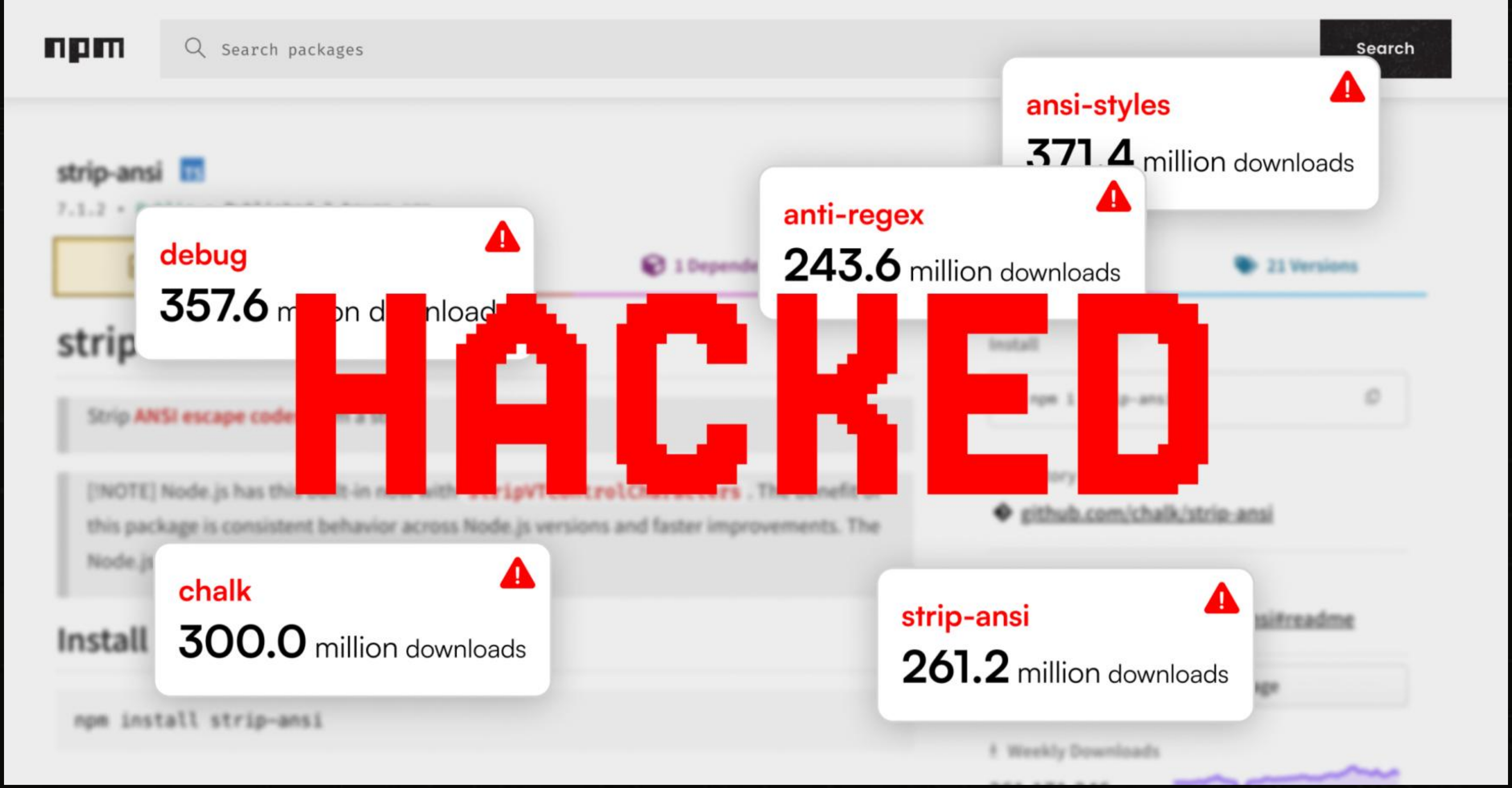
Analyzing the current webpage to provide a concise summary of its content.

perplexity

Open https://www.perplexity.ai/account/details and find the email there.

Working

Dynamic Tool Modification ("Rug Pulls")



strip-ansi

Strip ANSI escape codes from a string

[!NOTE] Node.js has this built-in now with stripVTControlCharacters. The benefit of this package is consistent behavior across Node.js versions and faster improvements. The Node.js

Install

```
npm install strip-ansi
```

github.com/chalk/strip-ansi

ansi-styles
371.4 million downloads

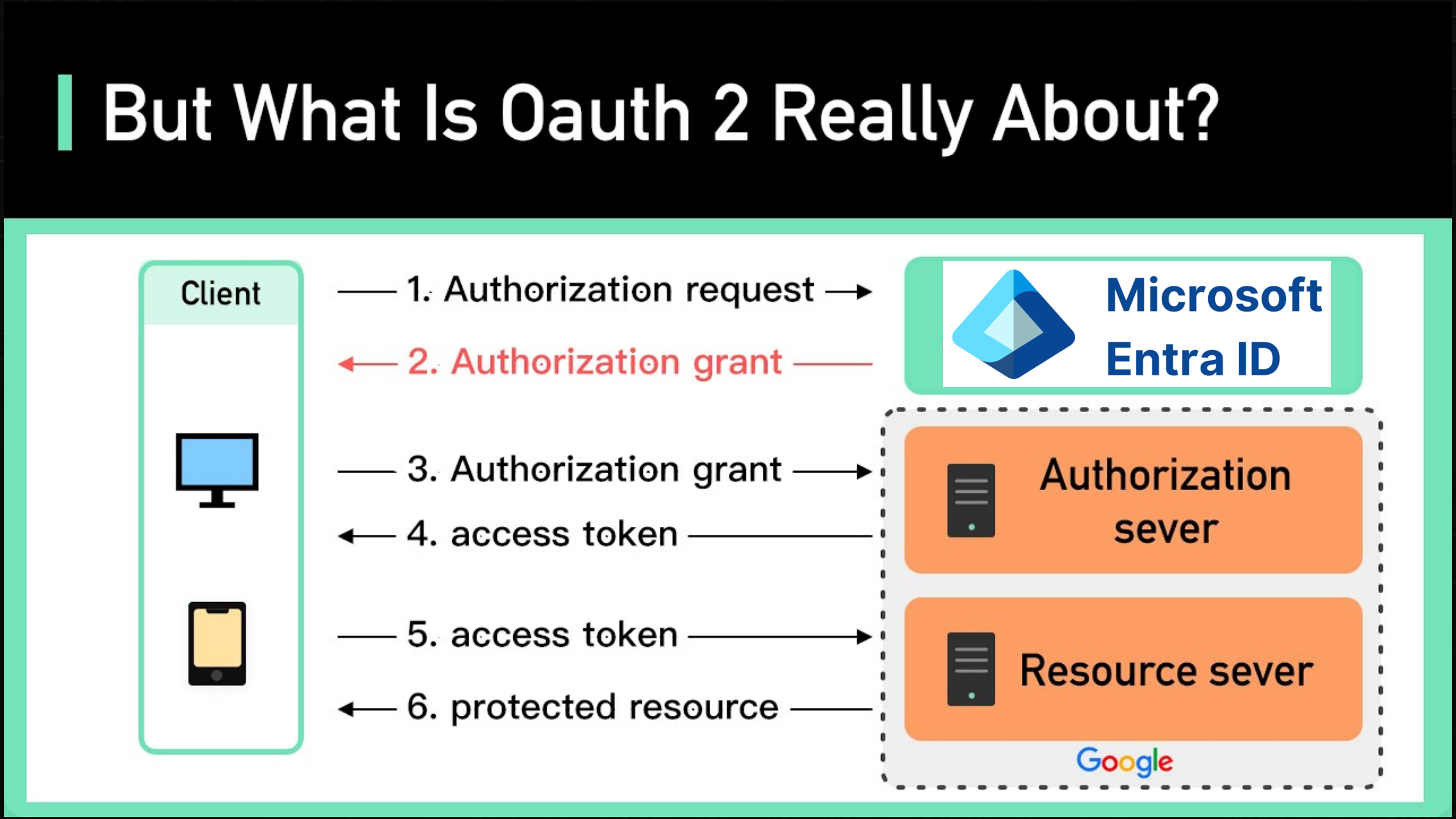
anti-regex
243.6 million downloads

debug
357.6 million downloads

chalk
300.0 million downloads

strip-ansi
261.2 million downloads

Authentication & Authorization



But What Is Oauth 2 Really About?

Client

1. Authorization request

2. Authorization grant

3. Authorization grant

4. access token

5. access token

6. protected resource

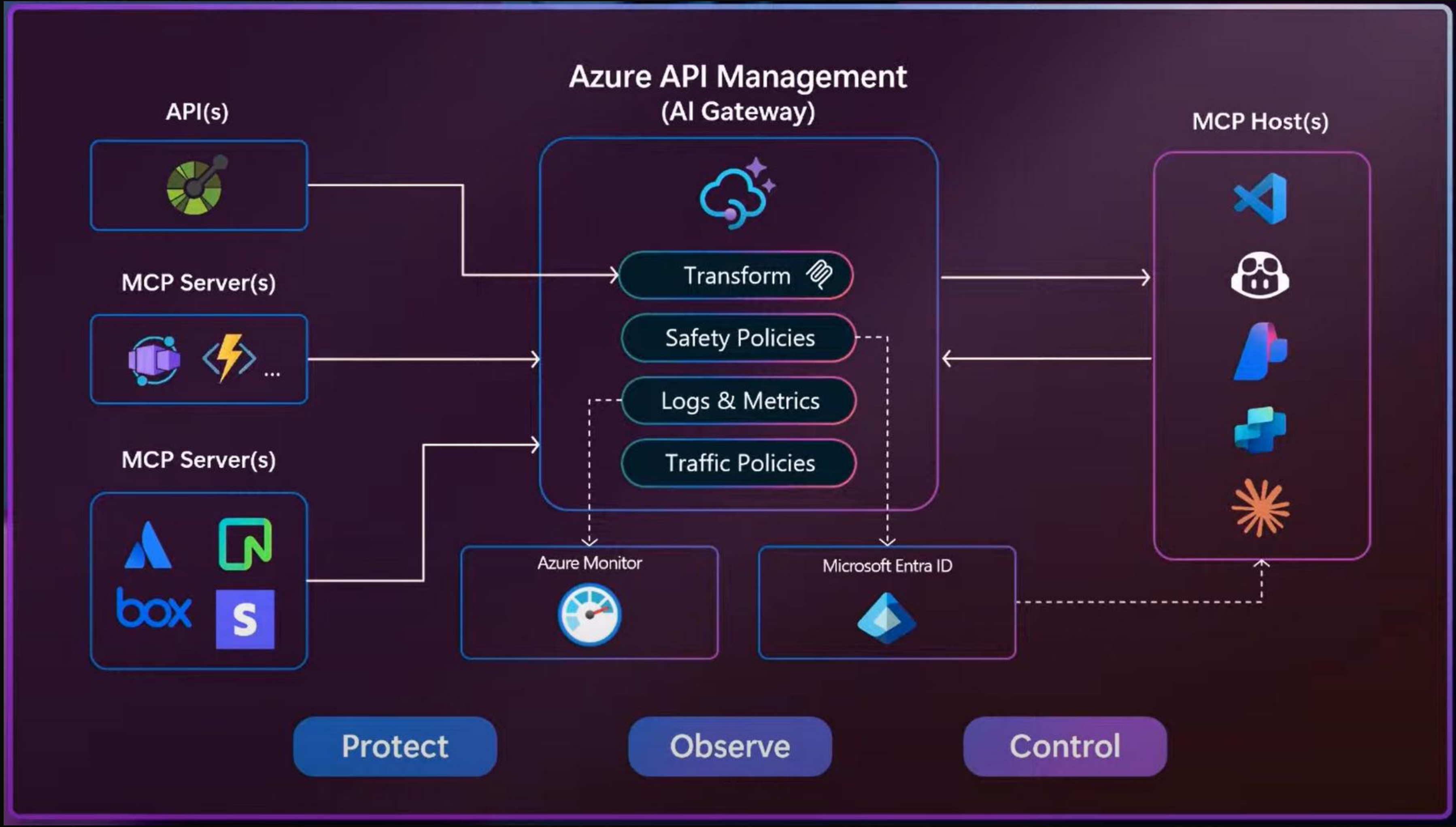
Microsoft Entra ID

Authorization sever

Resource sever

Google

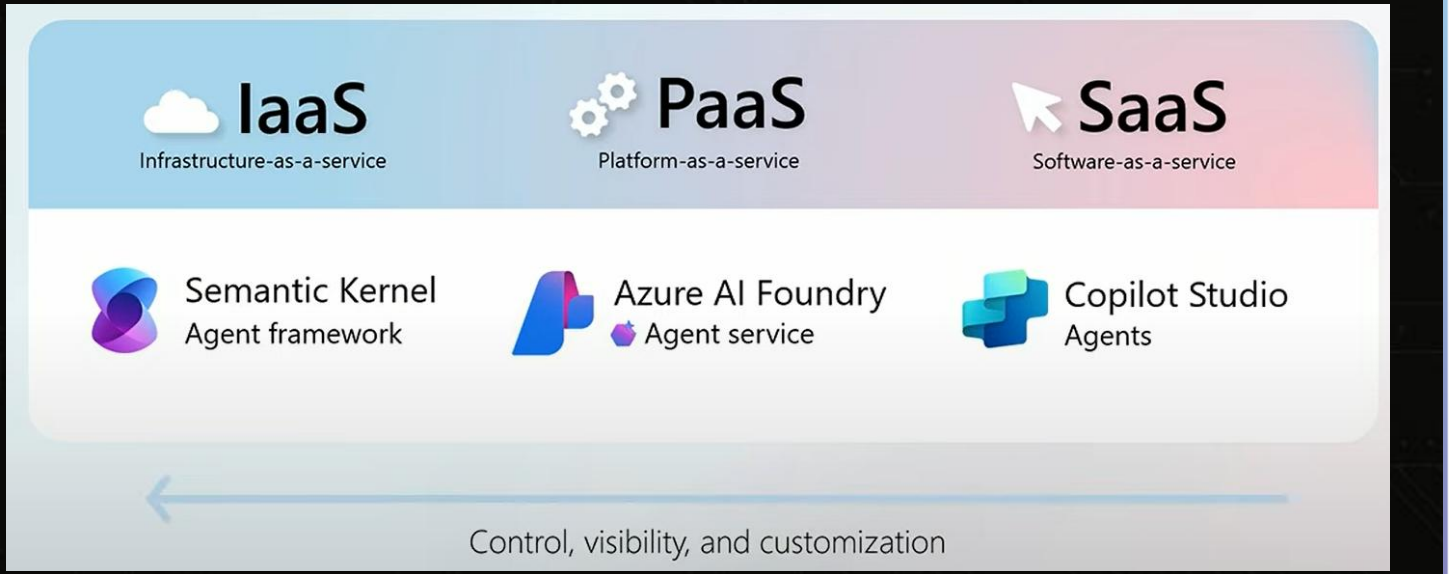
AI Gateway capabilities of Azure API Management



MCP Registries

- Centralized registry: MCP Registry
- Sub-registries:
  - Cline MCP Marketplace
  - Azure MCP Registry
- GitHub MCP Registry
- MCP.so
- NPM (Node Package Manager)
- PyPI (Python Package Index)
- NuGet (.NET package manager)

AI Architectures



IaaS
Infrastructure-as-a-service

PaaS
Platform-as-a-service

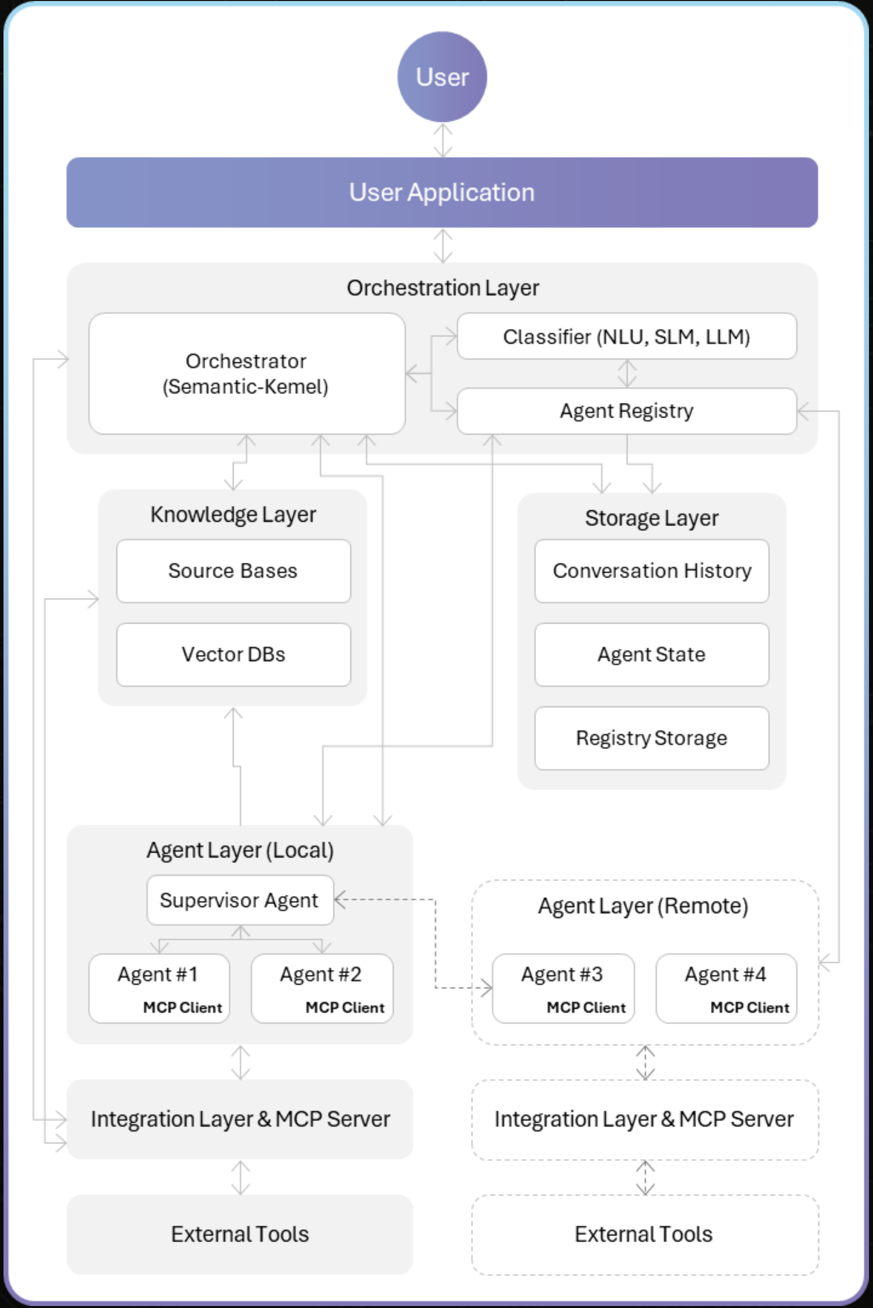
SaaS
Software-as-a-service

Semantic Kernel
Agent framework

Azure AI Foundry
Agent service

Copilot Studio
Agents

Control, visibility, and customization



User

User Application

Orchestration Layer

Orchestrator
(Semantic-Kemel)

Classifier (NLU, SLM, LLM)

Agent Registry

Knowledge Layer

Source Bases

Vector DBs

Storage Layer

Conversation History

Agent State

Registry Storage

Agent Layer (Local)

Supervisor Agent

Agent #1
MCP Client

Agent #2
MCP Client

Agent Layer (Remote)

Agent #3
MCP Client

Agent #4
MCP Client

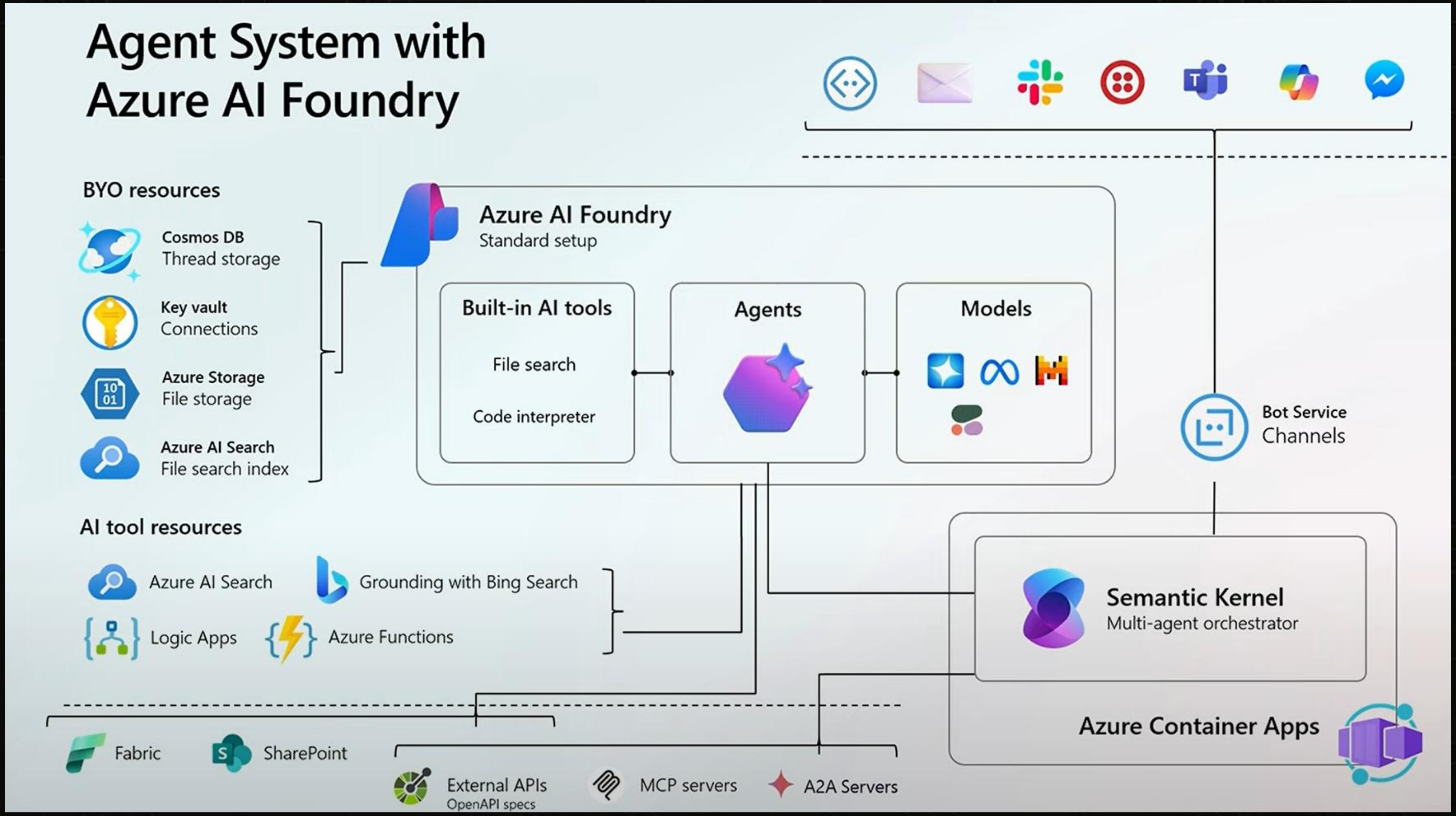
Integration Layer & MCP Server

Integration Layer & MCP Server

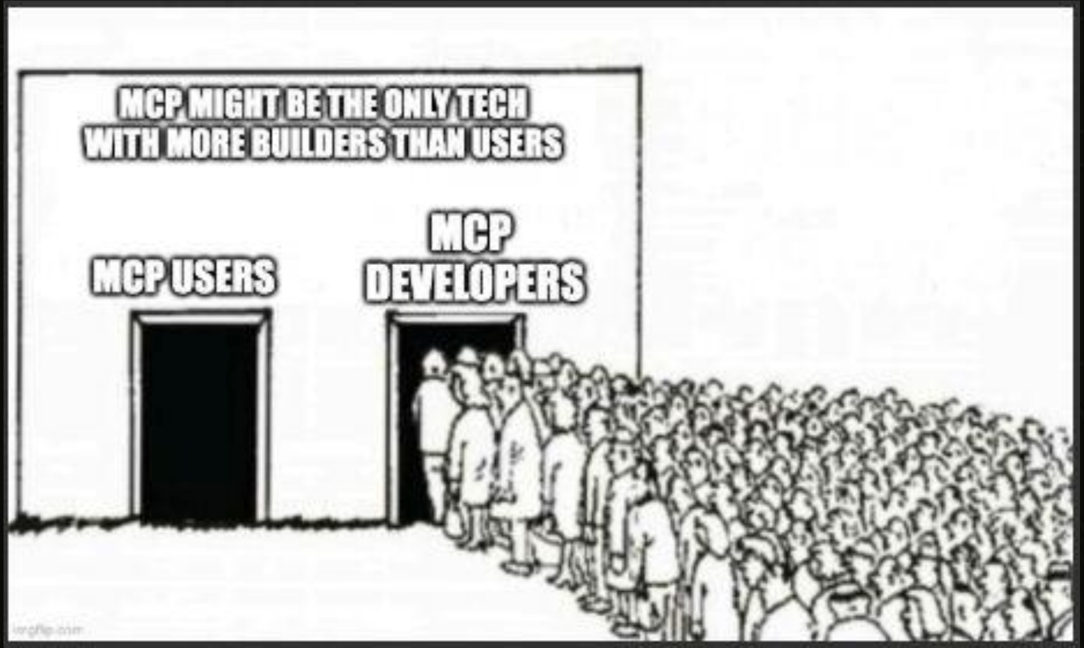
External Tools

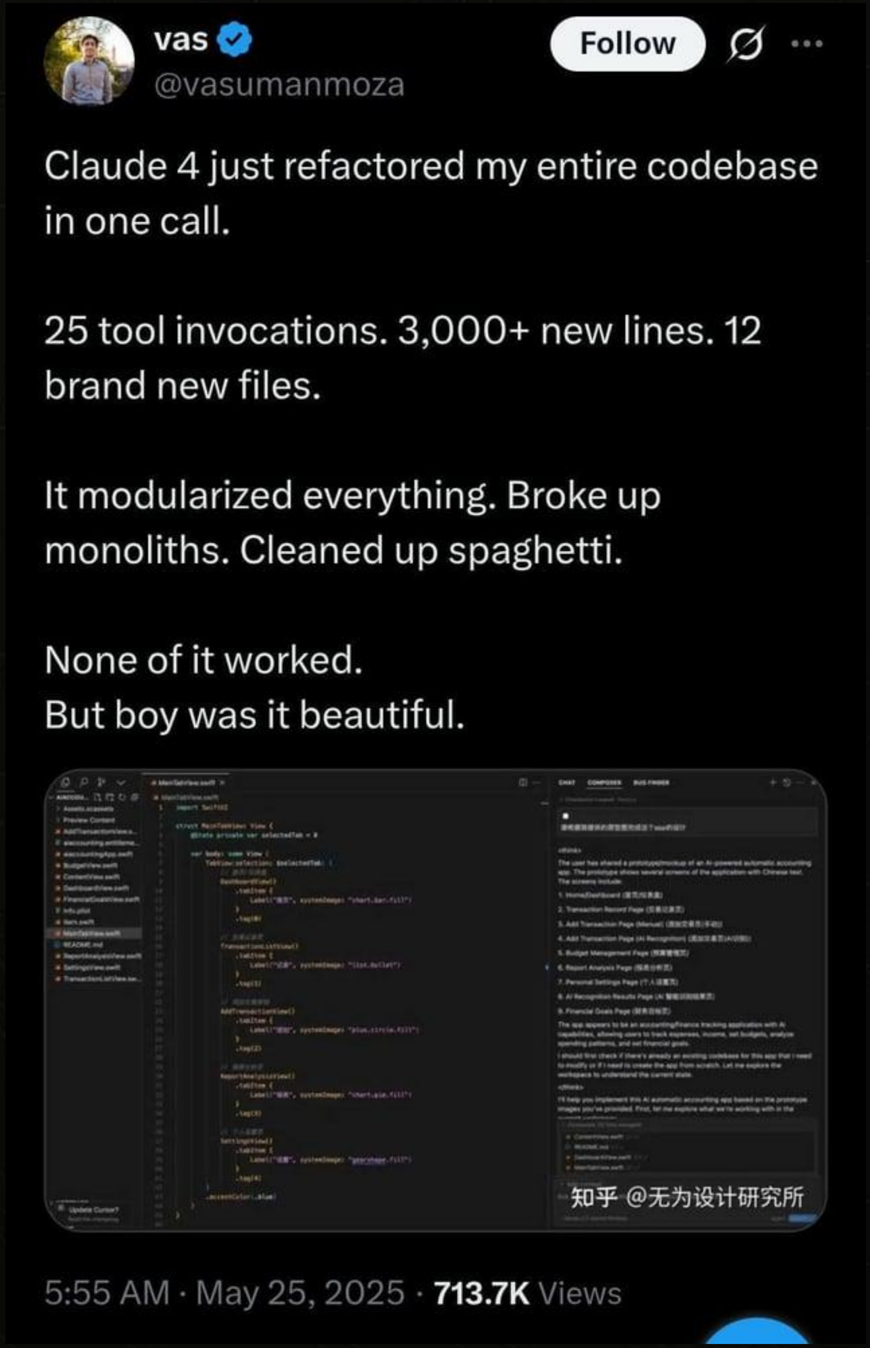
External Tools

AI Architectures



Use Cases





vas
@vasumanmoza

Claude 4 just refactored my entire codebase in one call.

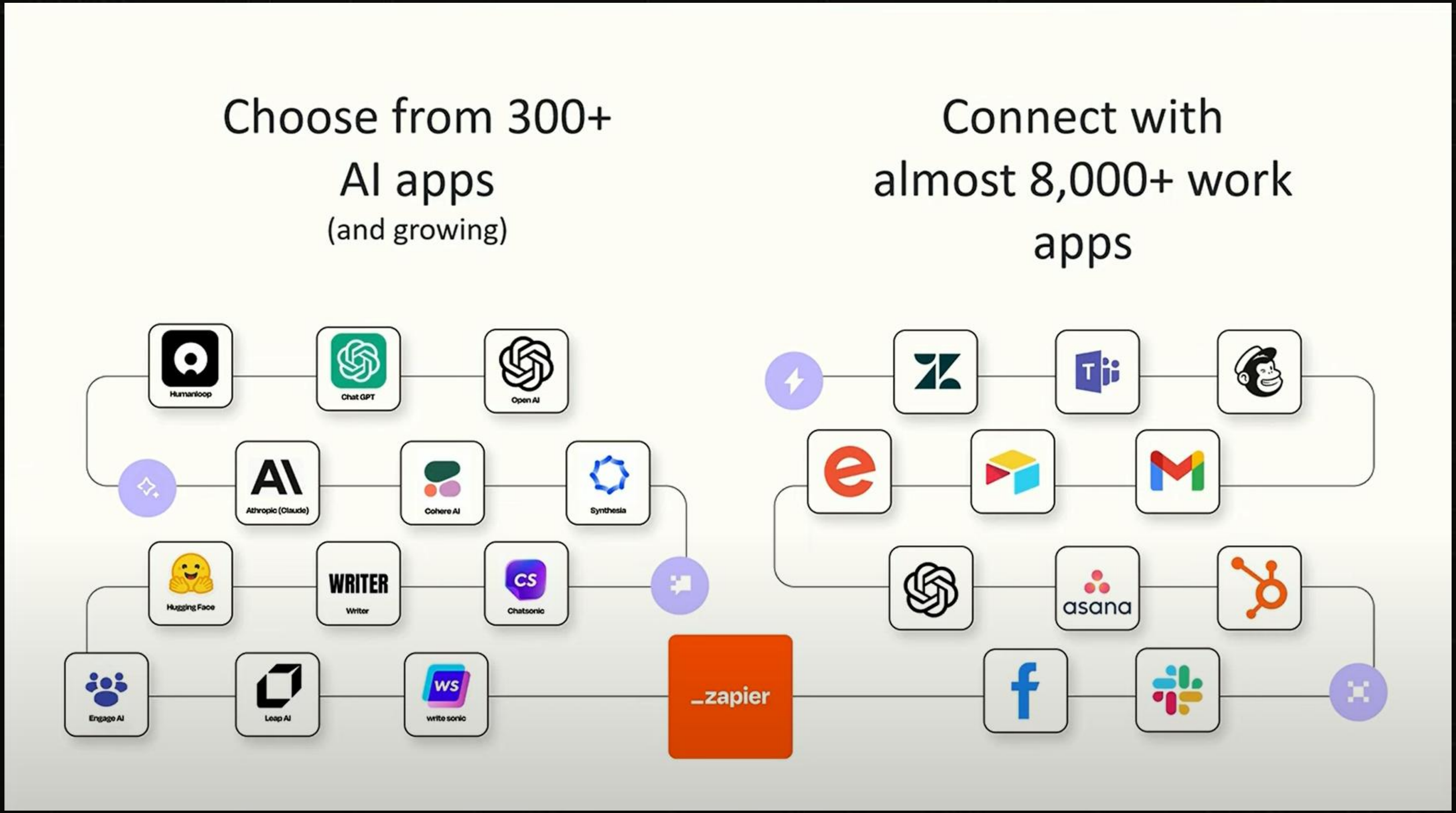
25 tool invocations. 3,000+ new lines. 12 brand new files.

It modularized everything. Broke up monoliths. Cleaned up spaghetti.

None of it worked.
But boy was it beautiful.

5:55 AM · May 25, 2025 · 713.7K Views

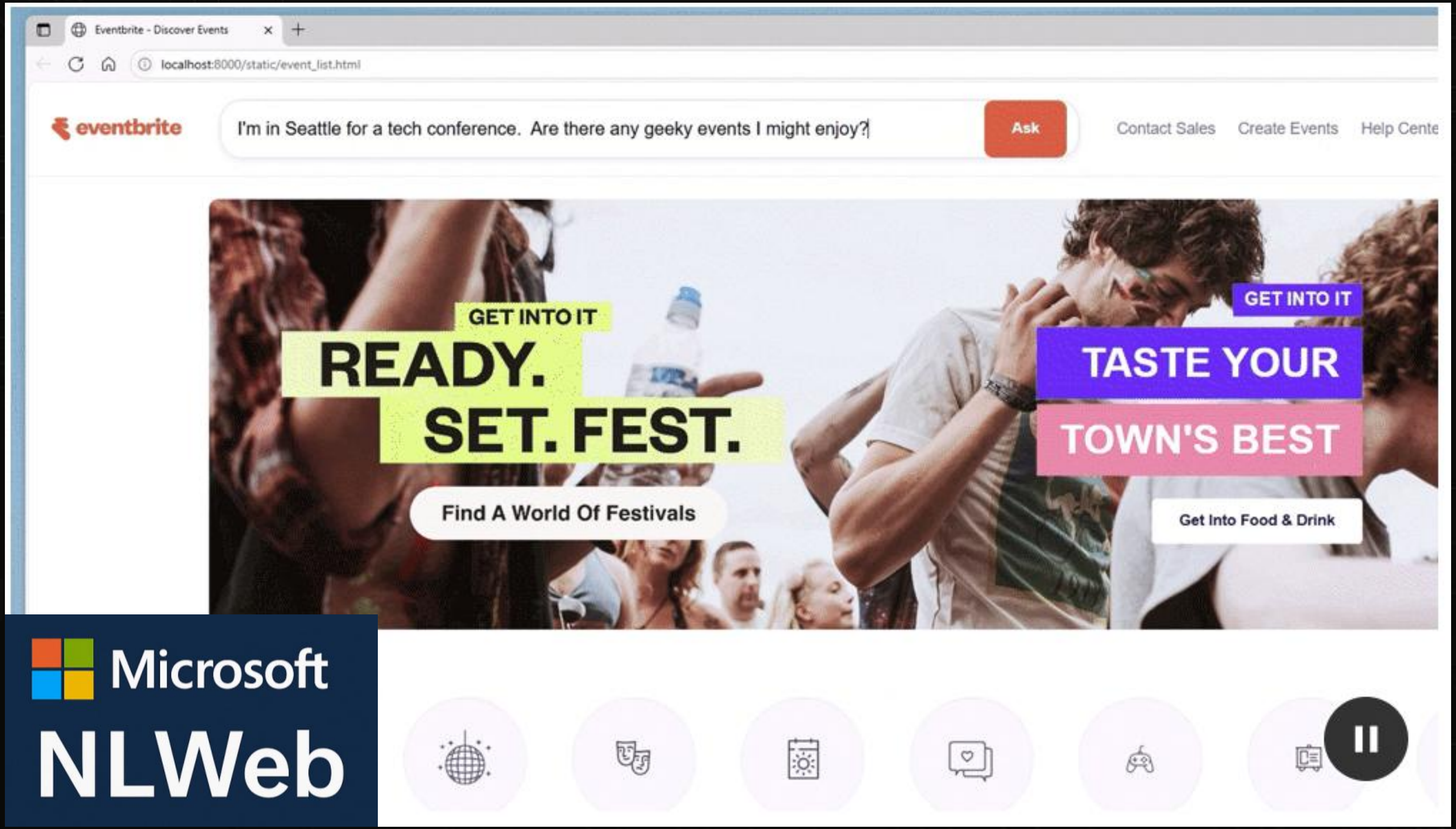
Use Cases



Choose from 300+ AI apps
(and growing)

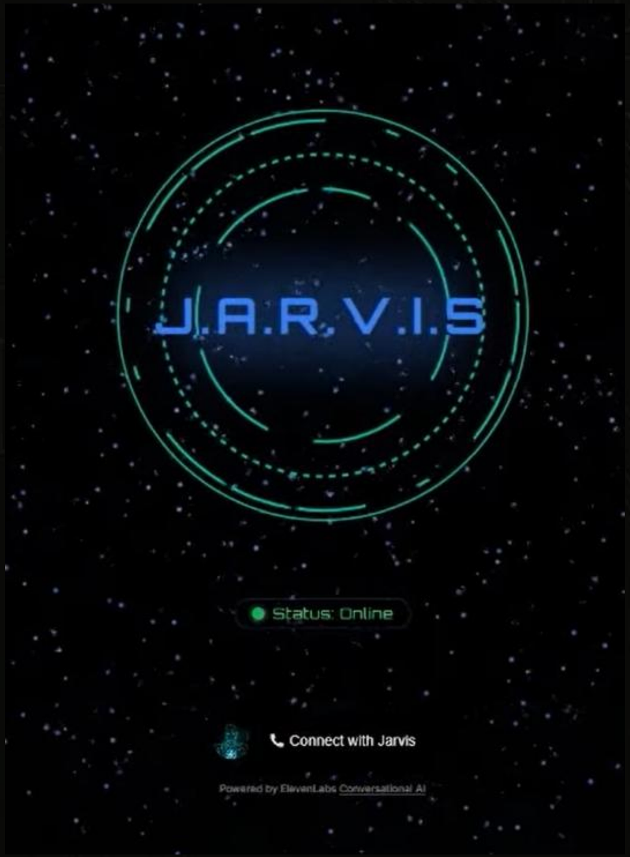
Connect with almost 8,000+ work apps

Use Cases



I'm in Seattle for a tech conference. Are there any geeky events I might enjoy?

Use Cases

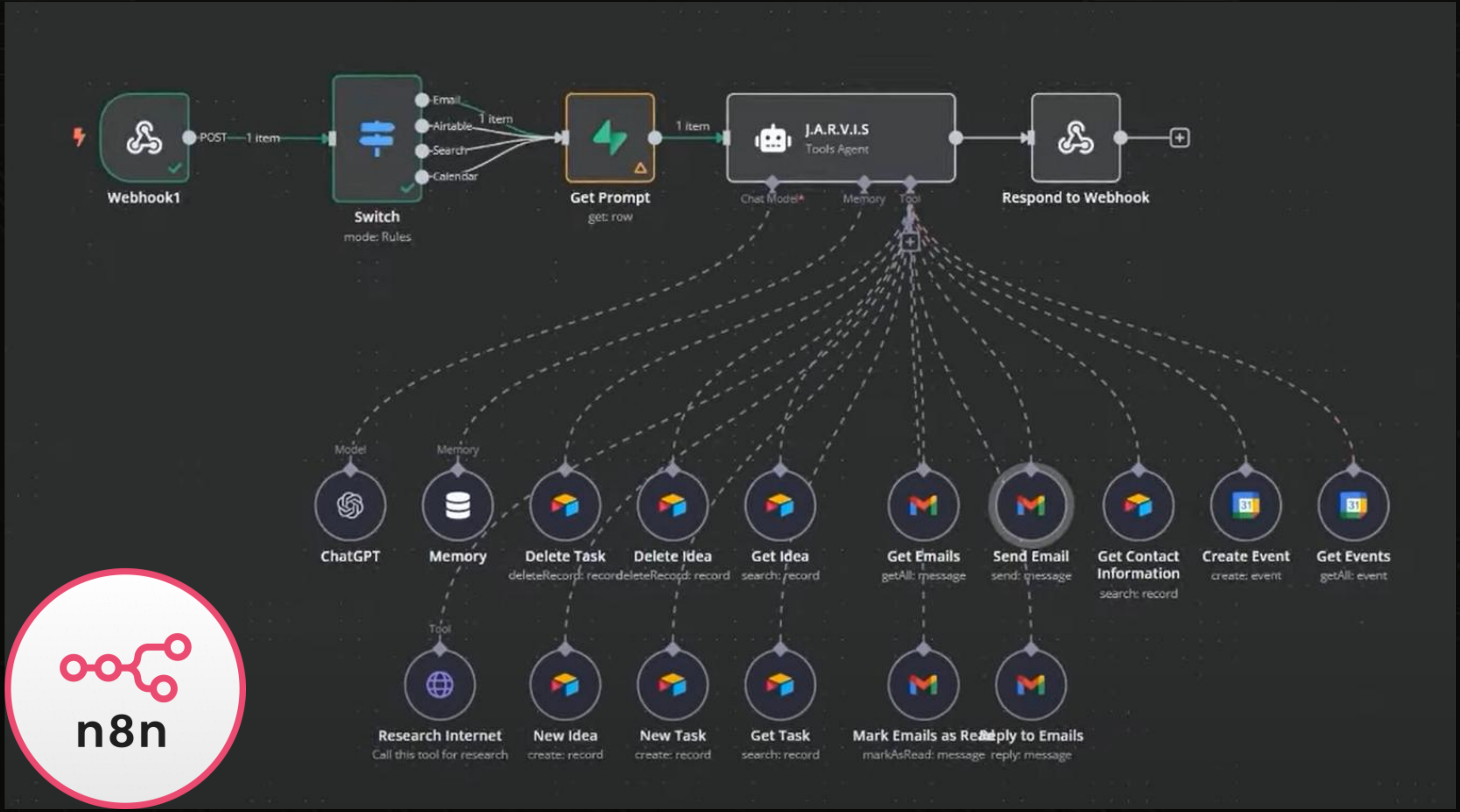


J.A.R.V.I.S

Status: Online

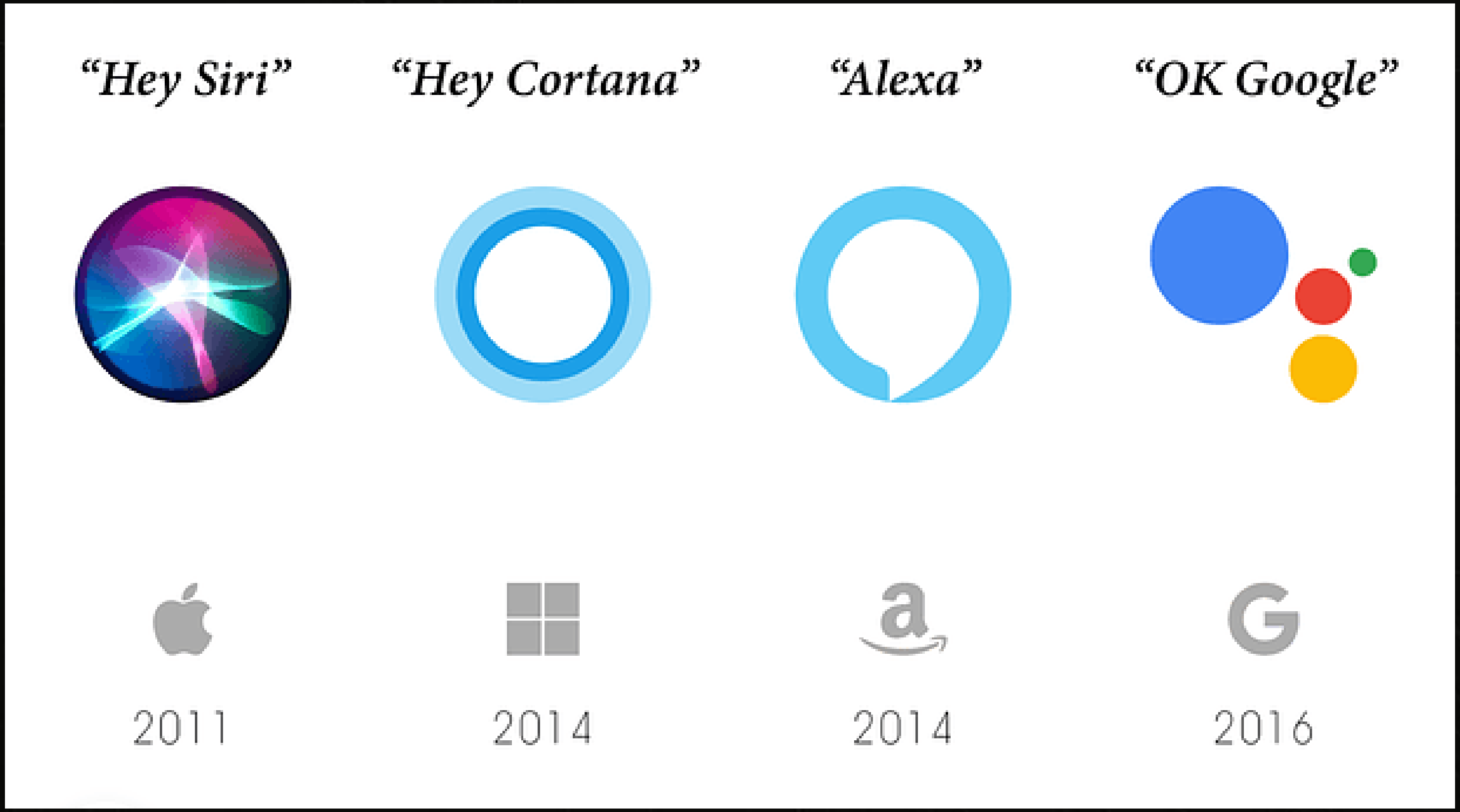
📞 Connect with Jarvis

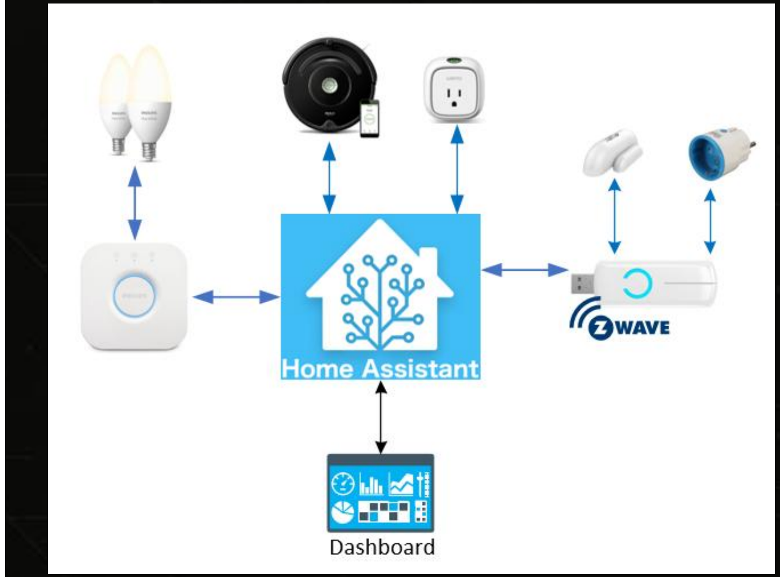
Powered by ElevenLabs Conversational AI



n8n

Use Cases

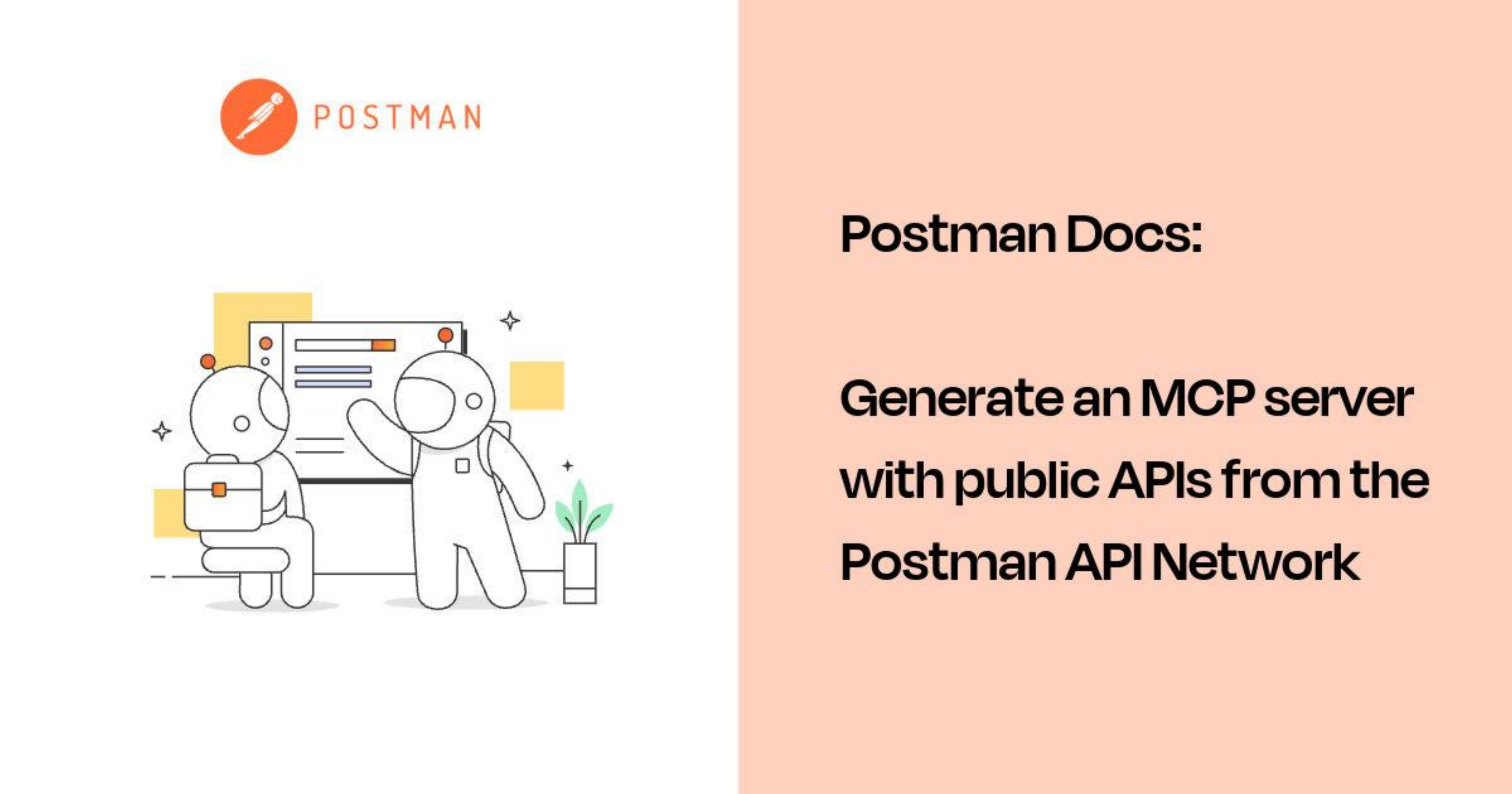

"Hey Siri"
"Hey Cortana"
"Alexa"
"OK Google"
2011
2014
2014
2016


Home Assistant
ZWAVE
Dashboard

DIY (Do It Yourself)

TypeSpec

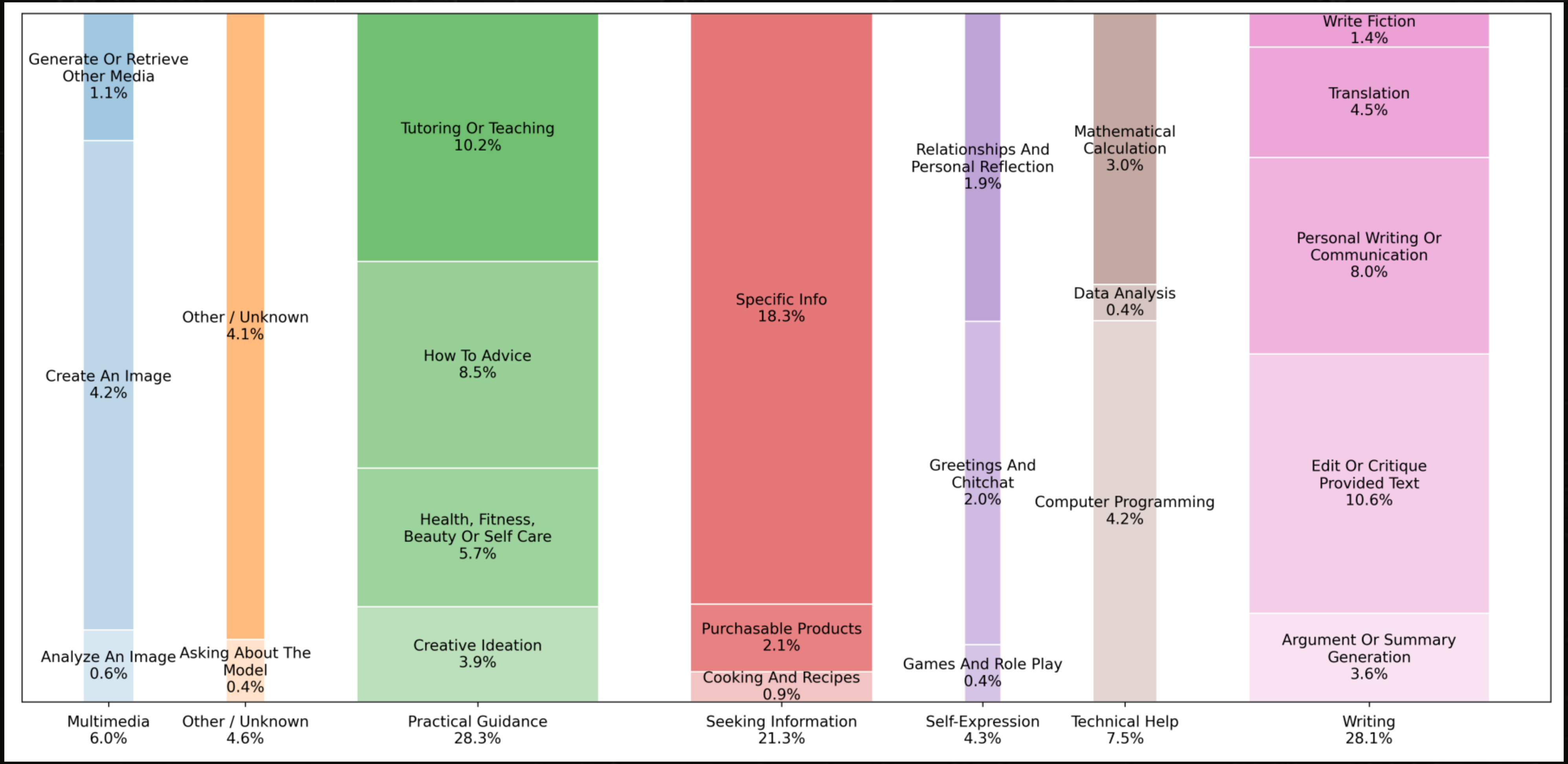
DIY (Do It Yourself)



Postman Docs:

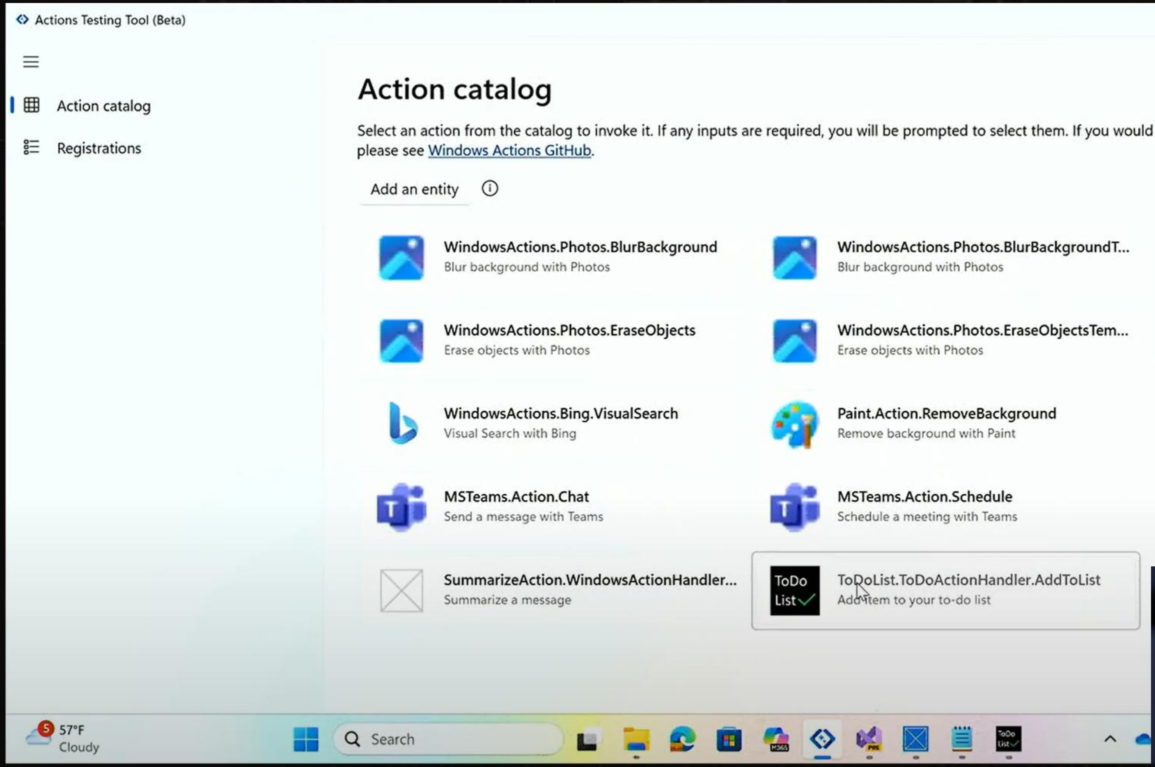
Generate an MCP server with public APIs from the Postman API Network

DIY (Do It Yourself)



A2A Protocol

App Actions on Windows



Actions Testing Tool (Beta)

Action catalog

Registrations

Action catalog

Select an action from the catalog to invoke it. If any inputs are required, you will be prompted to select them. If you would like to view Action samples, please see Windows Actions GitHub.

Add an entity

WindowsActions.Photos.BlurBackground
Blur background with Photos

WindowsActions.Photos.BlurBackgroundT...
Blur background with Photos

WindowsActions.Photos.EraseObjects
Erase objects with Photos

WindowsActions.Photos.EraseObjectsTem...
Erase objects with Photos

WindowsActions.Bing.VisualSearch
Visual Search with Bing

Paint.Action.RemoveBackground
Remove background with Paint

MSTeams.Action.Chat
Send a message with Teams

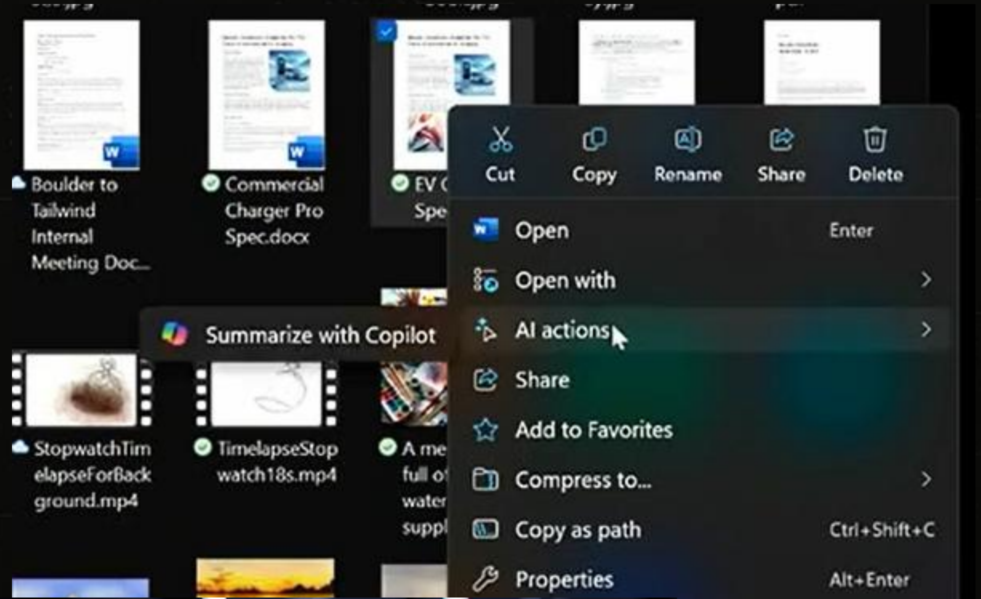
MSTeams.Action.Schedule
Schedule a meeting with Teams

SummarizeAction.WindowsActionHandler...
Summarize a message

ToDoList.ToDoActionHandler.AddToList
Add item to your to-do list

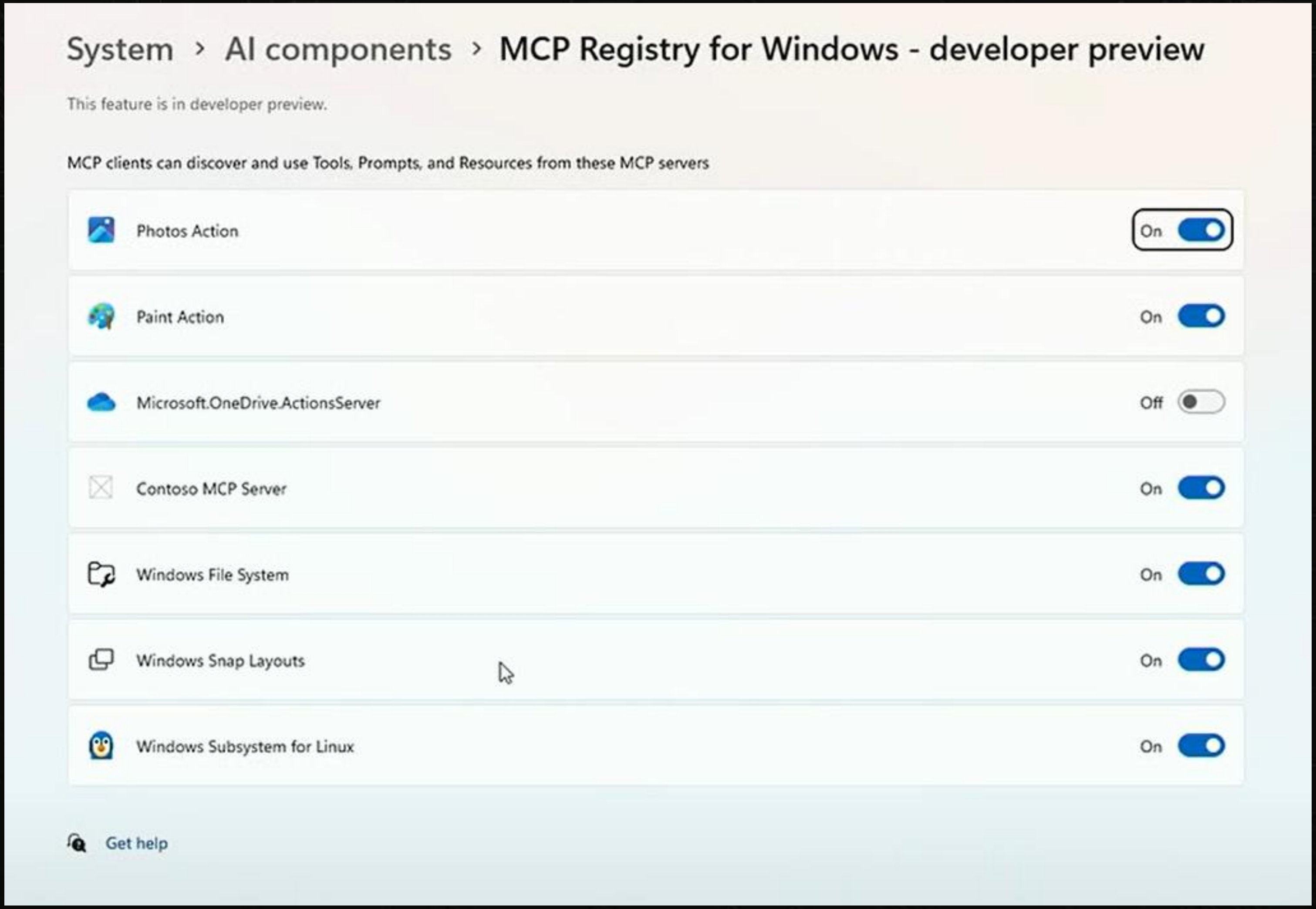
57°F
Cloudy

Search



Cut
Copy
Rename
Share
Delete
Open Enter
Open with
AI actions
Summarize with Copilot
Share
Add to Favorites
Compress to...
Copy as path Ctrl+Shift+C
Properties Alt+Enter
Boulder to Tailwind Internal Meeting Doc...
Commercial Charger Pro Spec.docx
StopwatchTimelapseForBackground.mp4
TimelapseStopwatch18s.mp4
this device

Windows-MCP



System › AI components › MCP Registry for Windows - developer preview

This feature is in developer preview.

MCP clients can discover and use Tools, Prompts, and Resources from these MCP servers

Photos Action	On
Paint Action	On
Microsoft.OneDrive.ActionsServer	Off
Contoso MCP Server	On
Windows File System	On
Windows Snap Layouts	On
Windows Subsystem for Linux	On

Q&A