LETTING AGENTS CONTROL YOUR BROWSER...

WHAT COULD POSSIBLY GO WRONG?

GEERT VAN DER CRUIJSEN

ZURE

2025

YEAR OF THE AGENTS

AGENTS
AGENTS EVERYWHERE!
ZURE

SO WHAT DEFINES AN AGENT?

SO WHAT DEFINES AN AGENT?

3 LEVELS OF GEN AI

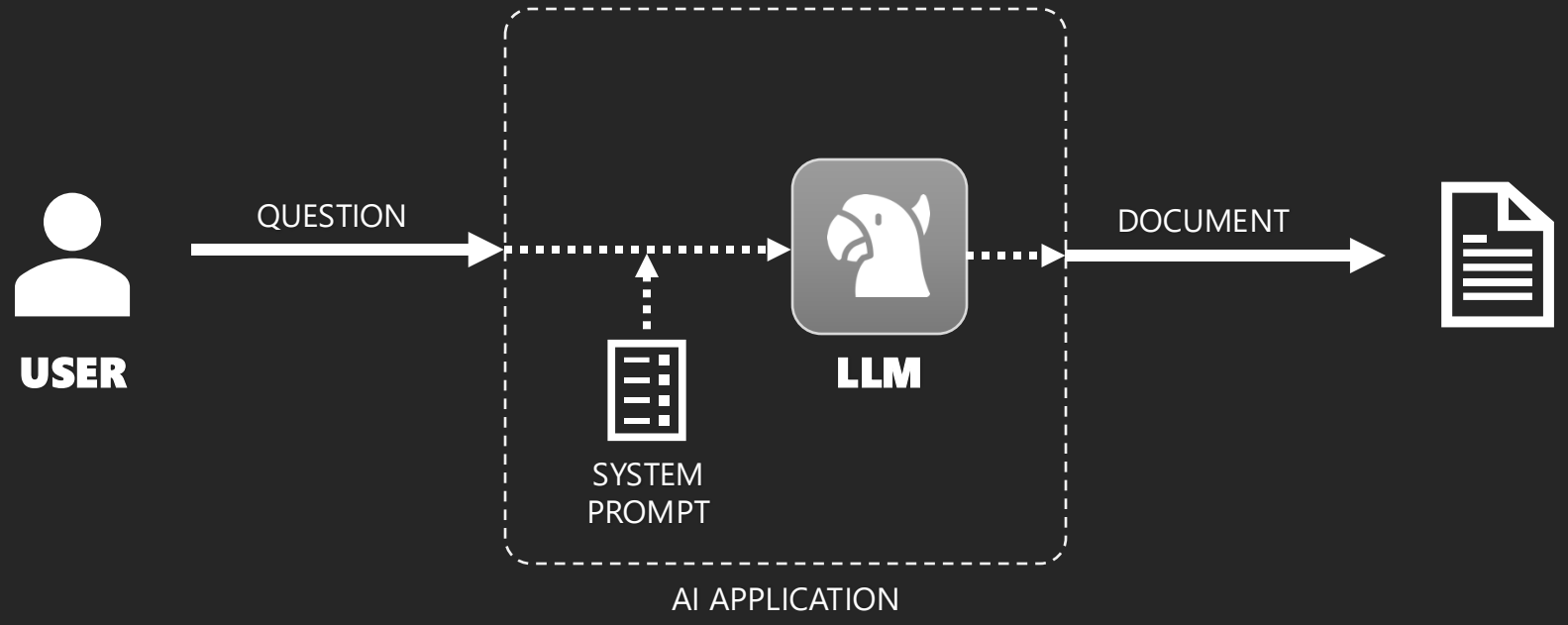
FROM NO AGENTS TO EVERYTHING BEING AN AGENT

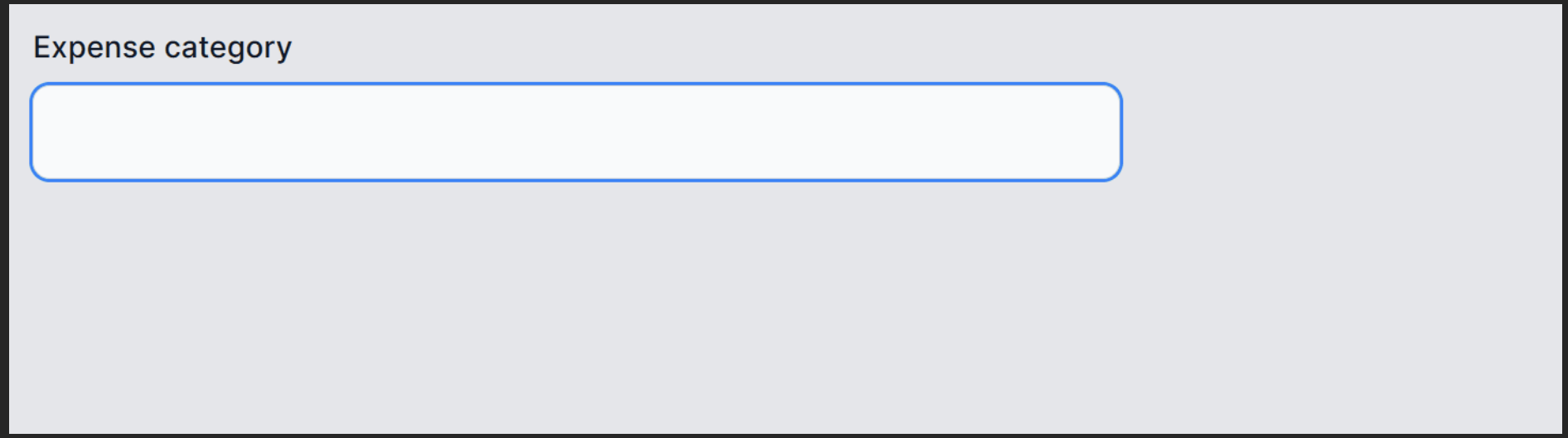
GEN AI LEVEL 1

CLEVER PROMPTING

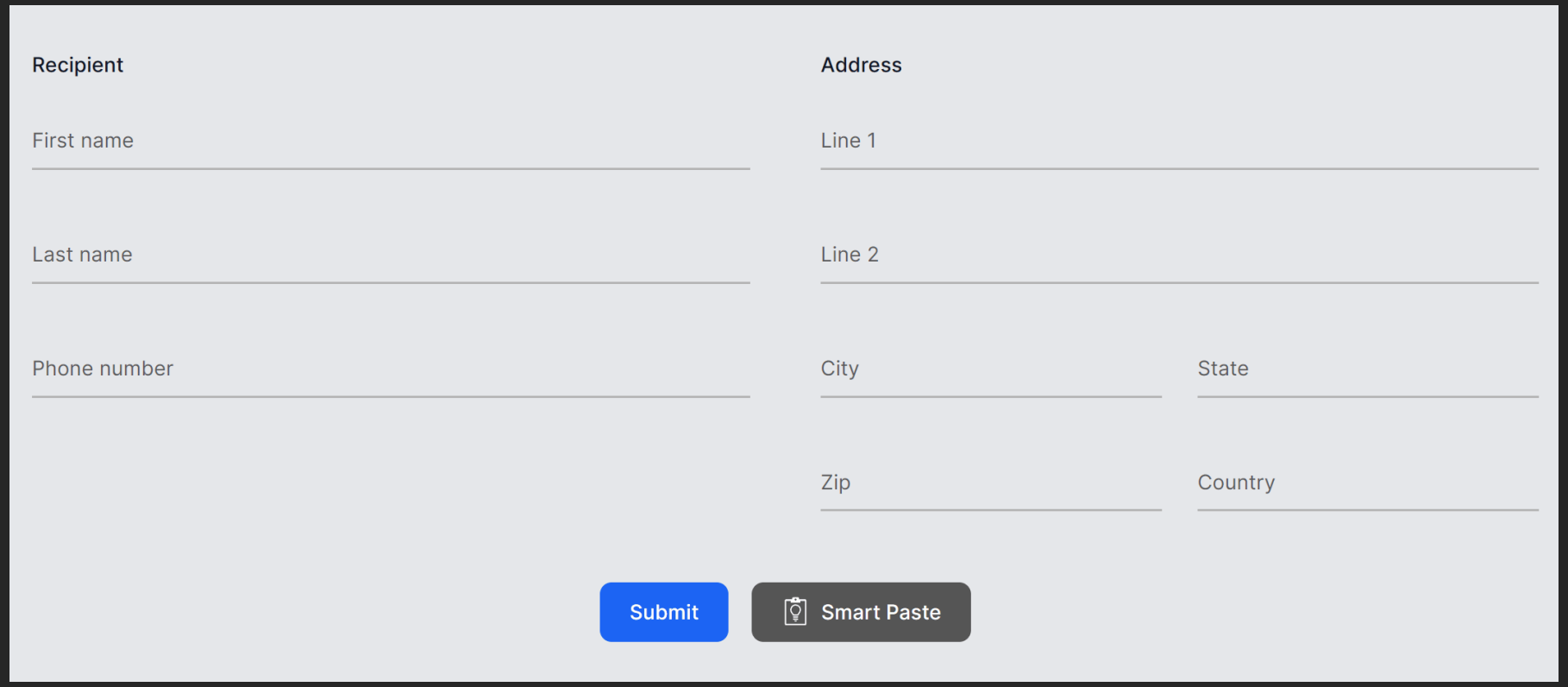
GEN AI LEVEL 1

CLEVER PROMPTING





.NET SMART COMPONENTS – SMART COMBOBOX



.NET SMART COMPONENTS – SMART PASTE

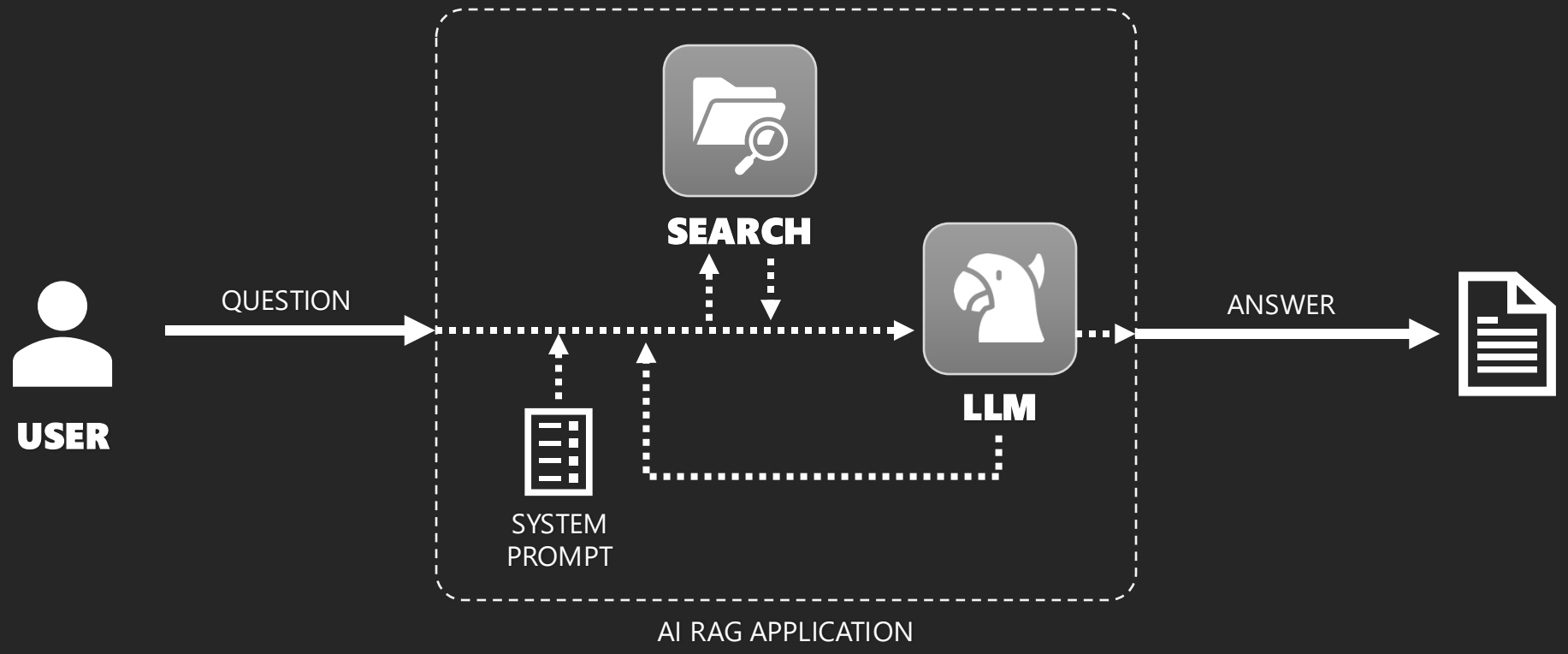
GEN AI LEVEL 2

AI APPS WITH BUSINESS CONTEXT

AKA: RAG

GEN AI LEVEL 2

AI APPS WITH BUSINESS CONTEXT



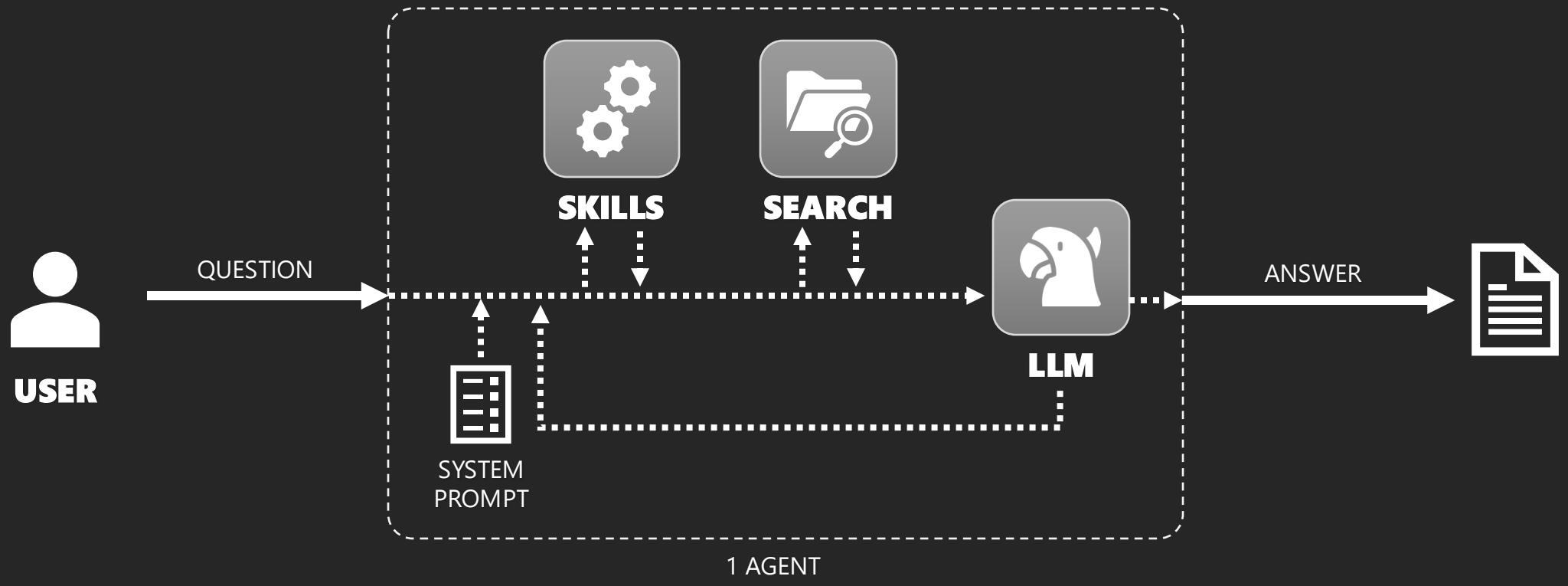
GEN AI LEVEL 3

CONNECTED AGENTS

ENDGAME

GEN AI LEVEL 3

CONNECTED AGENTS

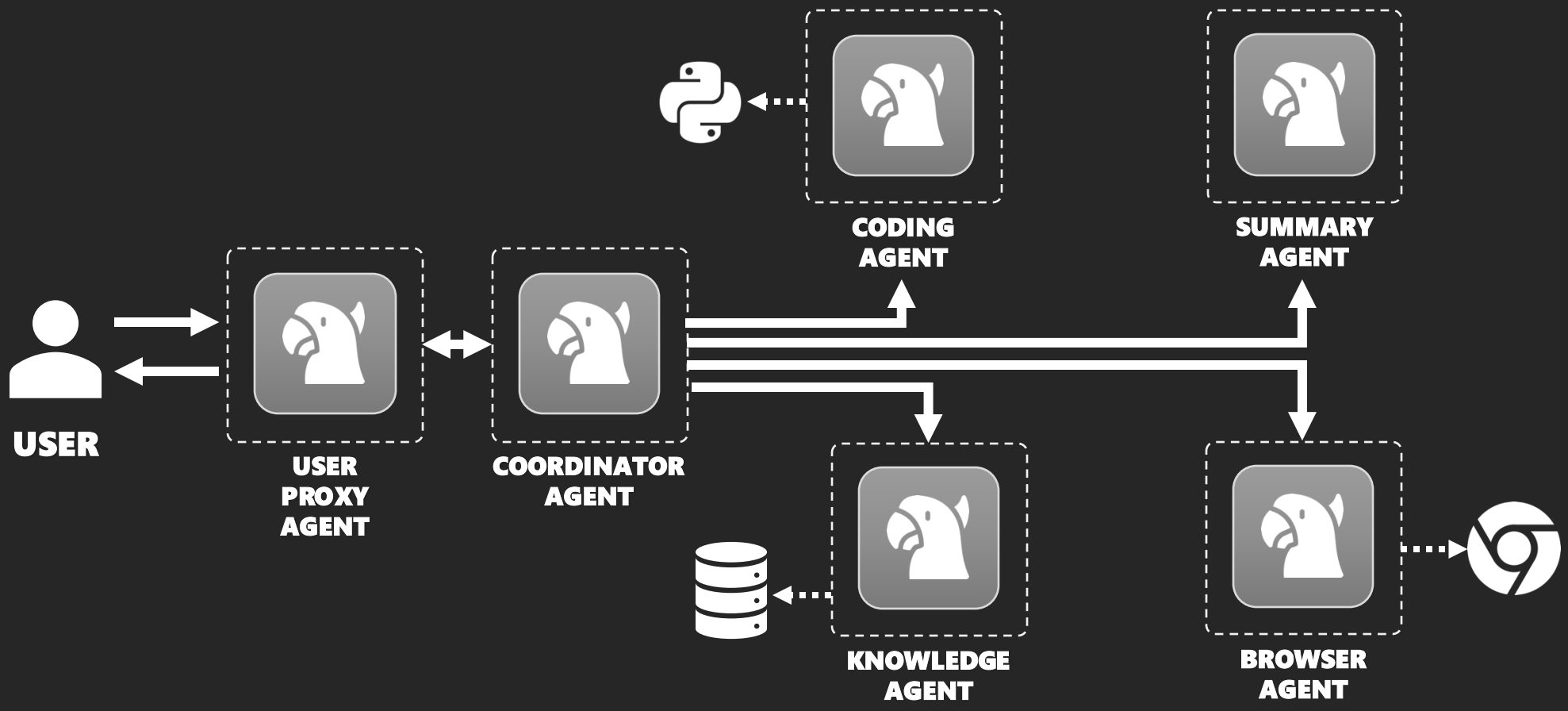


GEN AI LEVEL 3

CONNECTED AGENTS

GEN AI LEVEL 3

CONNECTED AGENTS



3 LEVELS OF GENAI

CONNECTED AGENTS

RAG

CLEVER PROMPTING

2023

2024

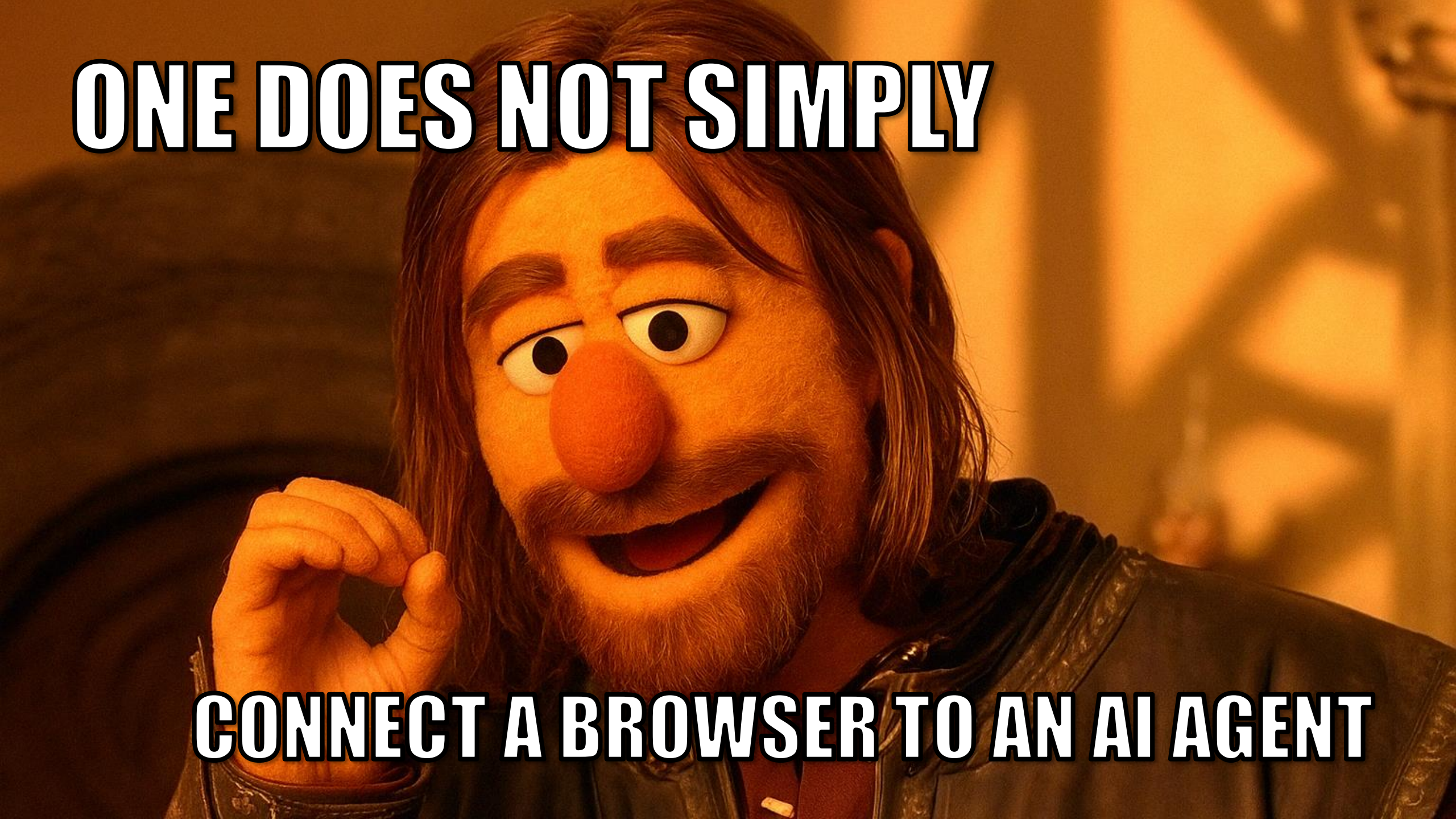
2025

GEERT,

YOU PROMISED US AI CONTROLLING WEB BROWSERS!

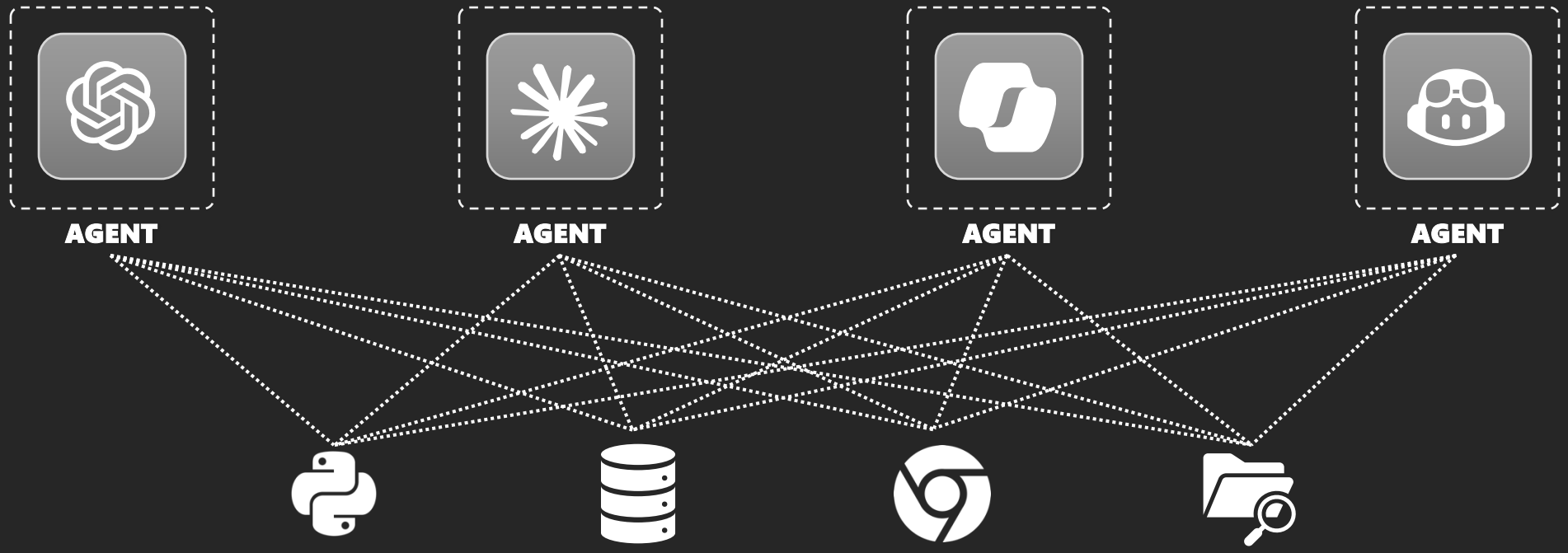
WHEN??

ZURE


ONE DOES NOT SIMPLY
CONNECT A BROWSER TO AN AI AGENT

A CLOSER LOOK

AGENT SKILLS



MCP

MODEL CONTEXT PROTOCOL

THE BIGGEST HYPE IN CURRENT GENAI SPACE

MCP

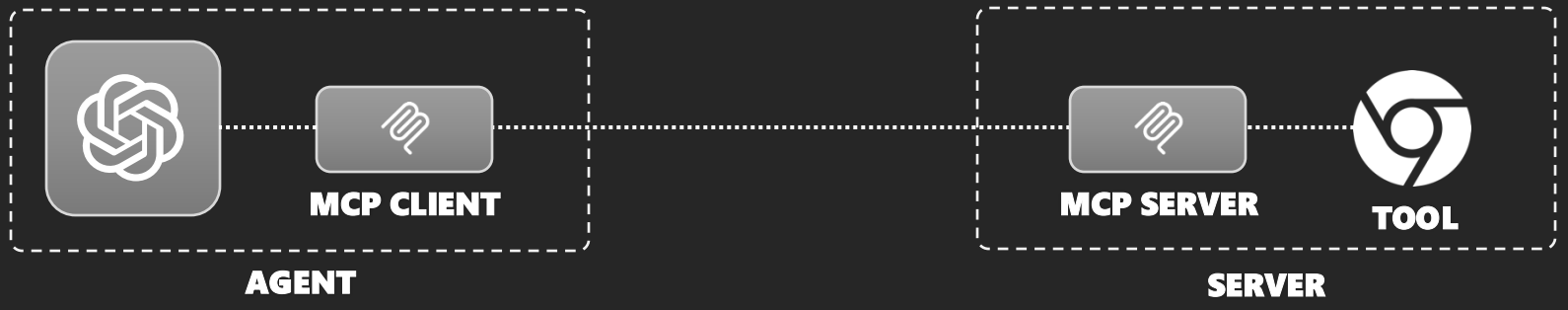
MODEL CONTEXT PROTOCOL

MCP

MODEL CONTEXT PROTOCOL

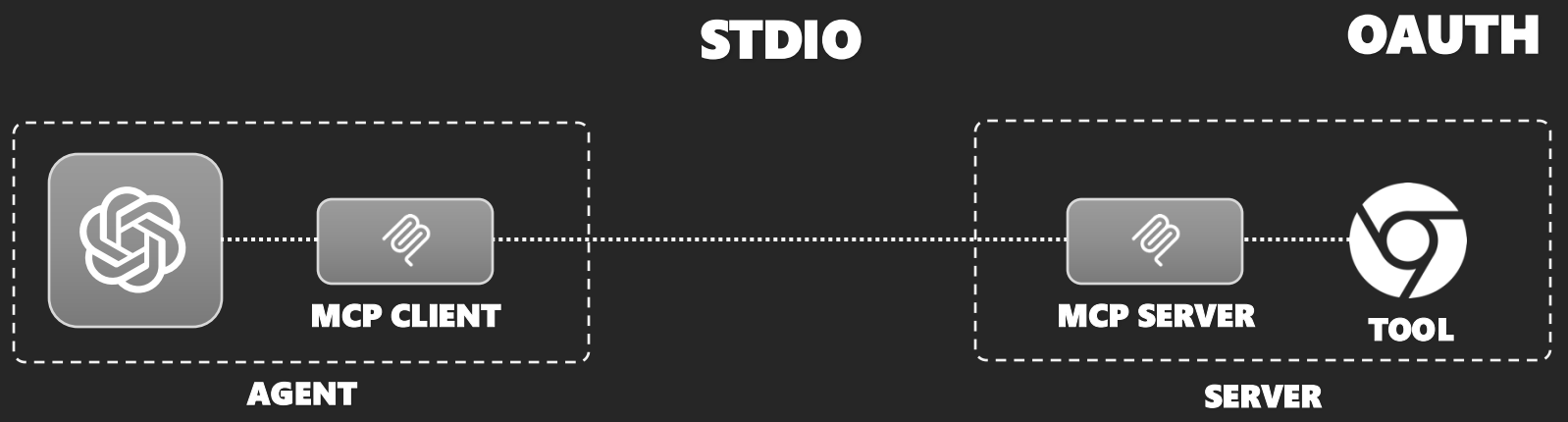
MCP

MODEL CONTEXT PROTOCOL



MCP

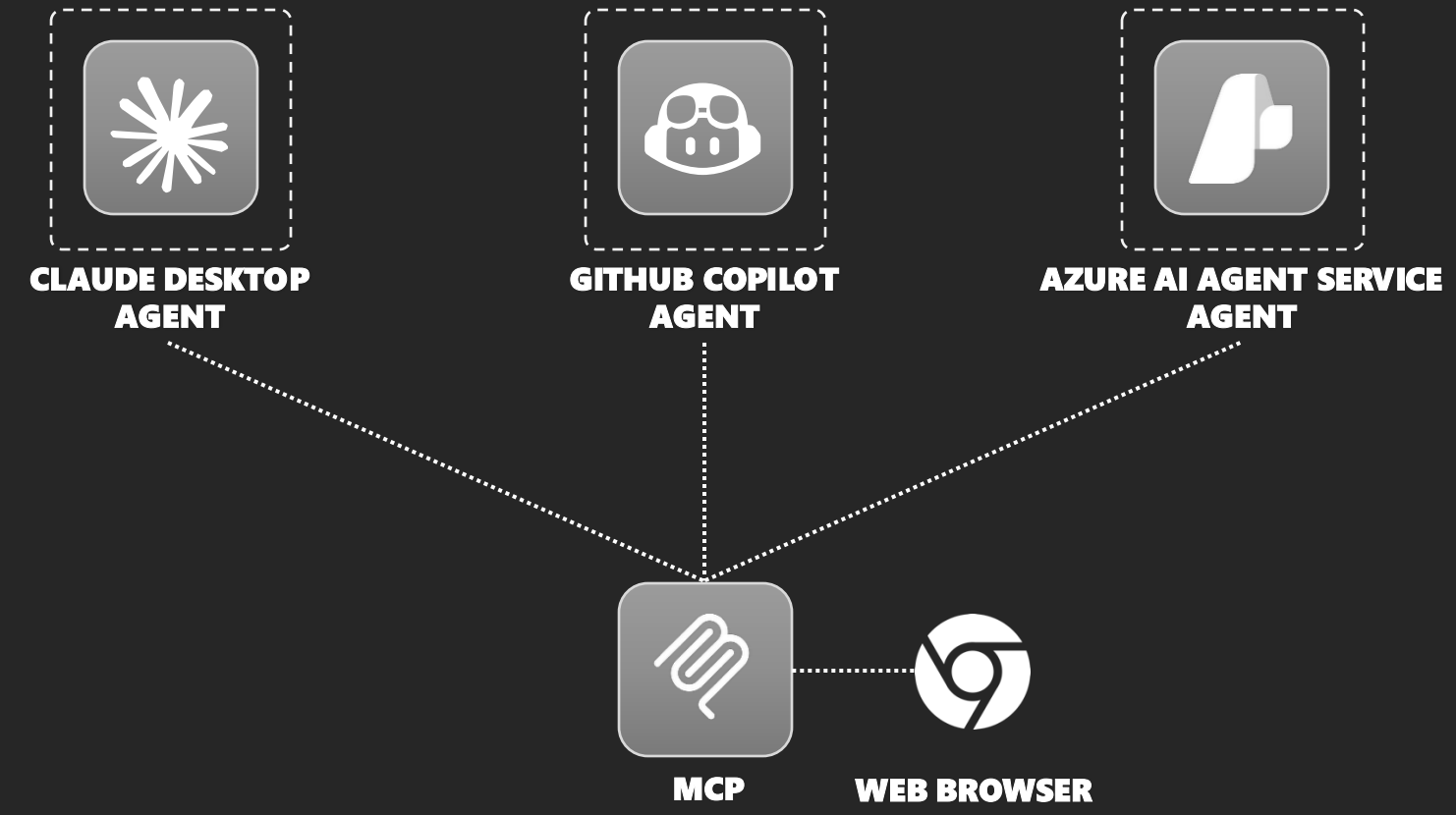
MODEL CONTEXT PROTOCOL



SERVER SIDE EVENTS (SSE)

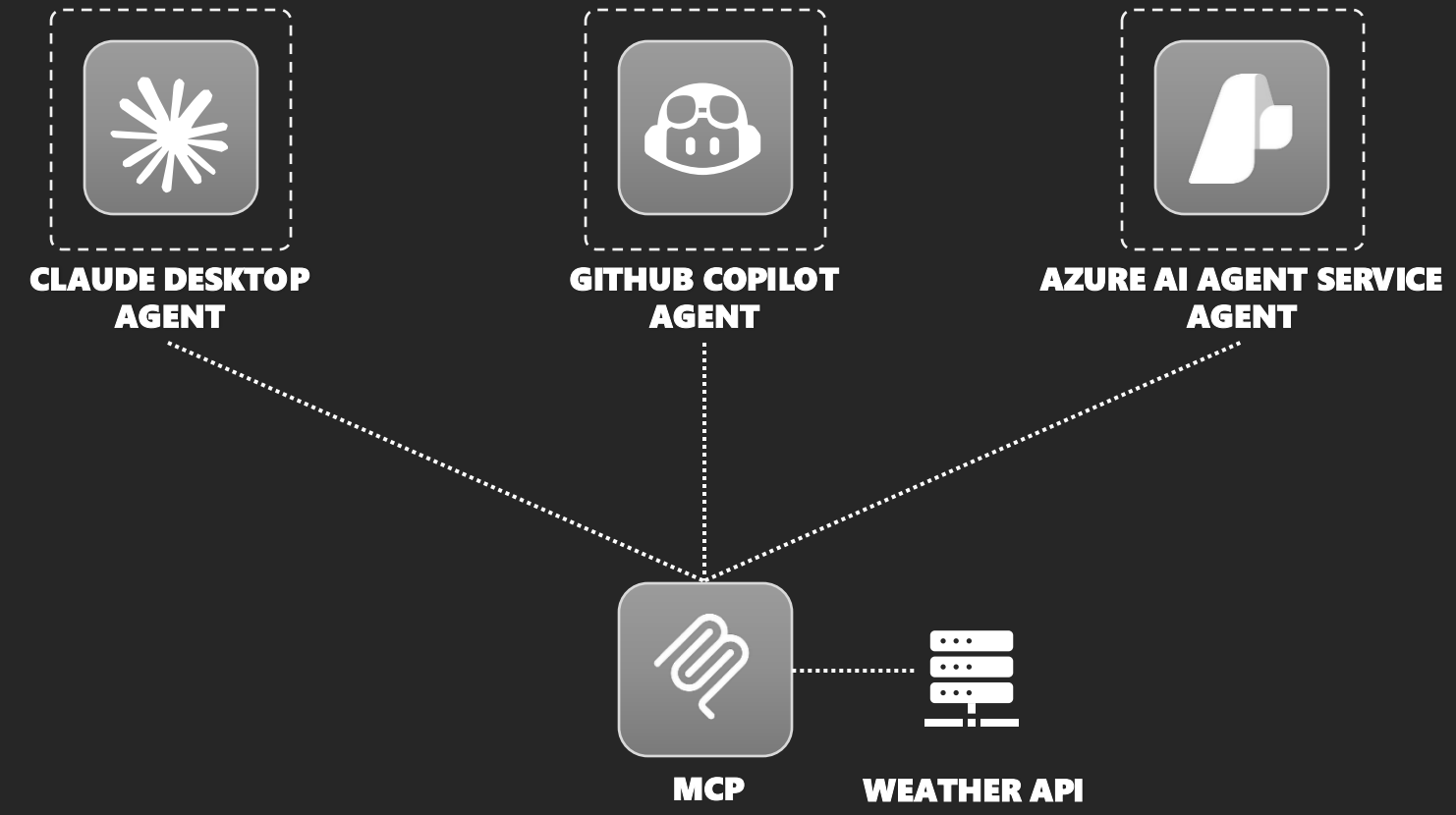
MCP

DEMO


CLAUDE DESKTOP AGENT
GITHUB COPILOT AGENT
AZURE AI AGENT SERVICE AGENT
MCP
WEB BROWSER

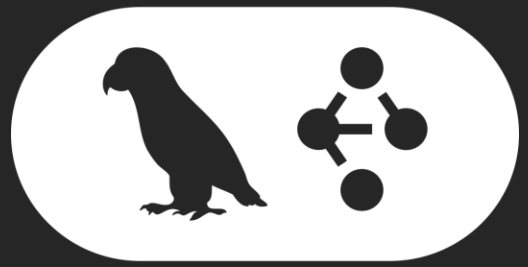
MCP

DEMO


CLAUDE DESKTOP AGENT
GITHUB COPILOT AGENT
AZURE AI AGENT SERVICE AGENT
MCP
WEATHER API

GEN AI LEVEL 3

CONNECTED AGENTS FRAMEWORKS

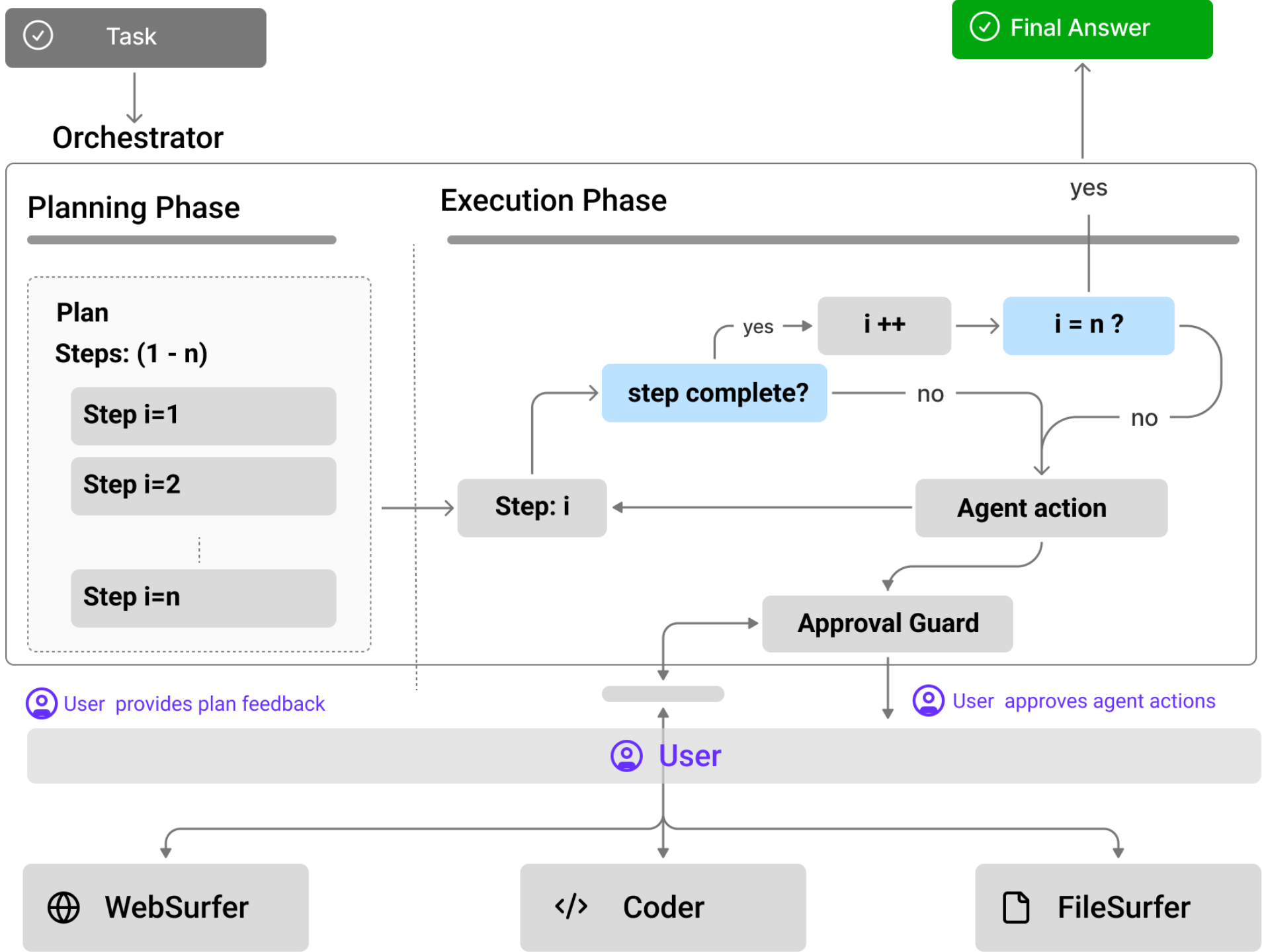


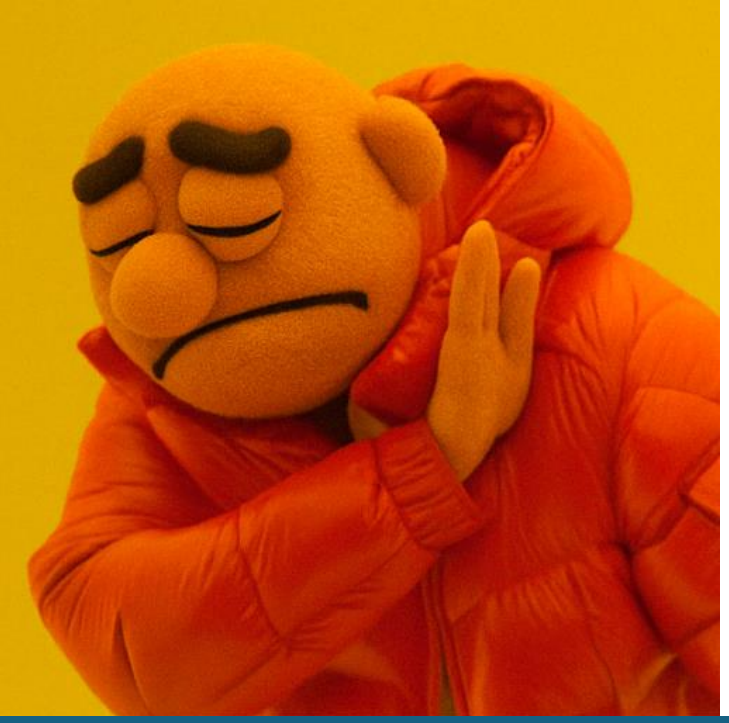
LANGCHAIN
LANG GRAPH

SEMANTIC
KERNEL

AUTOGEN
MAGENTIC
ONE

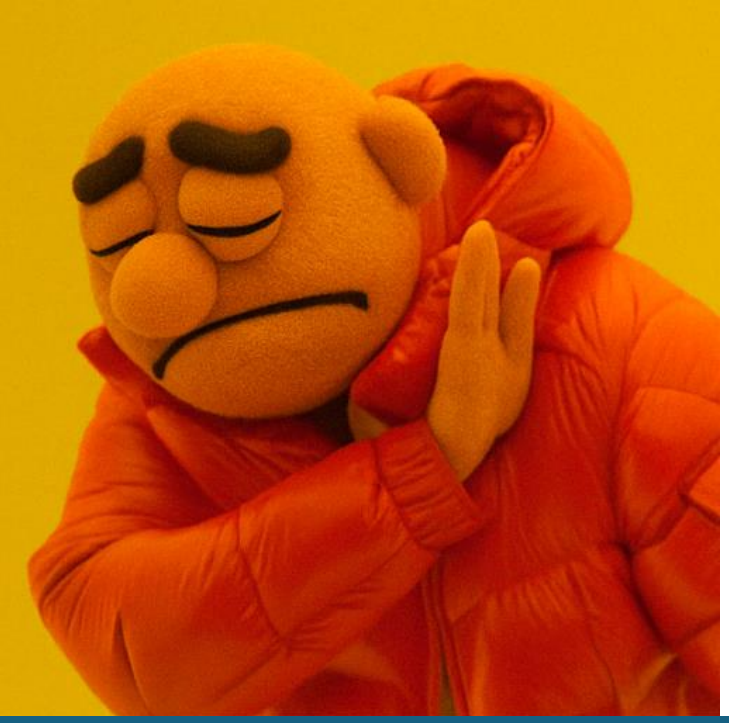
CREW AI


Task
Orchestrator
Final Answer
Planning Phase
Execution Phase
yes
Plan
Steps: (1 - n)
Step i=1
Step i=2
Step i=n
yes
i ++
i = n ?
step complete?
no
no
Step: i
Agent action
Approval Guard
User provides plan feedback
User approves agent actions
User
WebSurfer
Coder
FileSurfer



ROBOTIC PROCESS AUTOMATION

AI



ROBOTIC
PROCESS
AUTOMATION

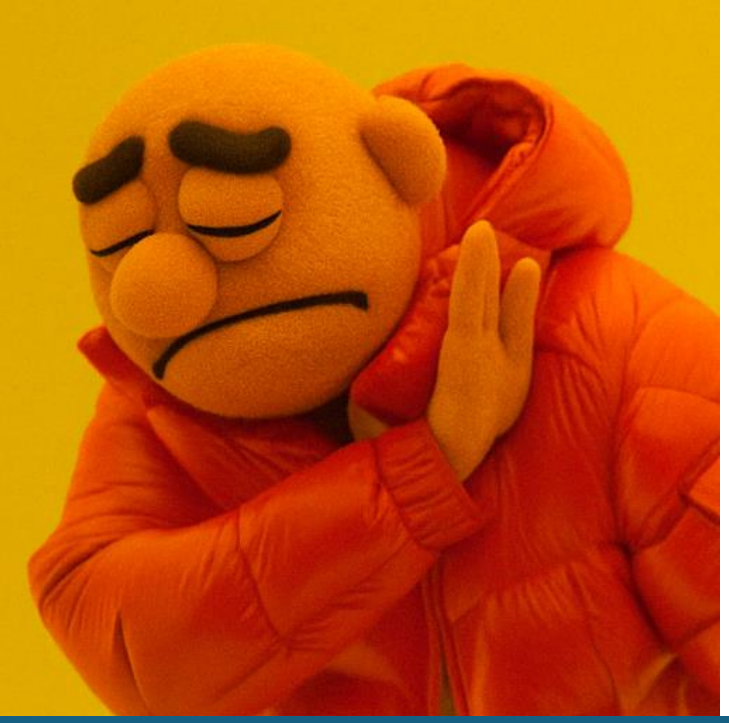
AI

REALLY?

DETERMINISTIC

SPEED

COST



ROBOTIC PROCESS AUTOMATION

AI

ACTUAL USE

BACKUP FOR RPA FAILING

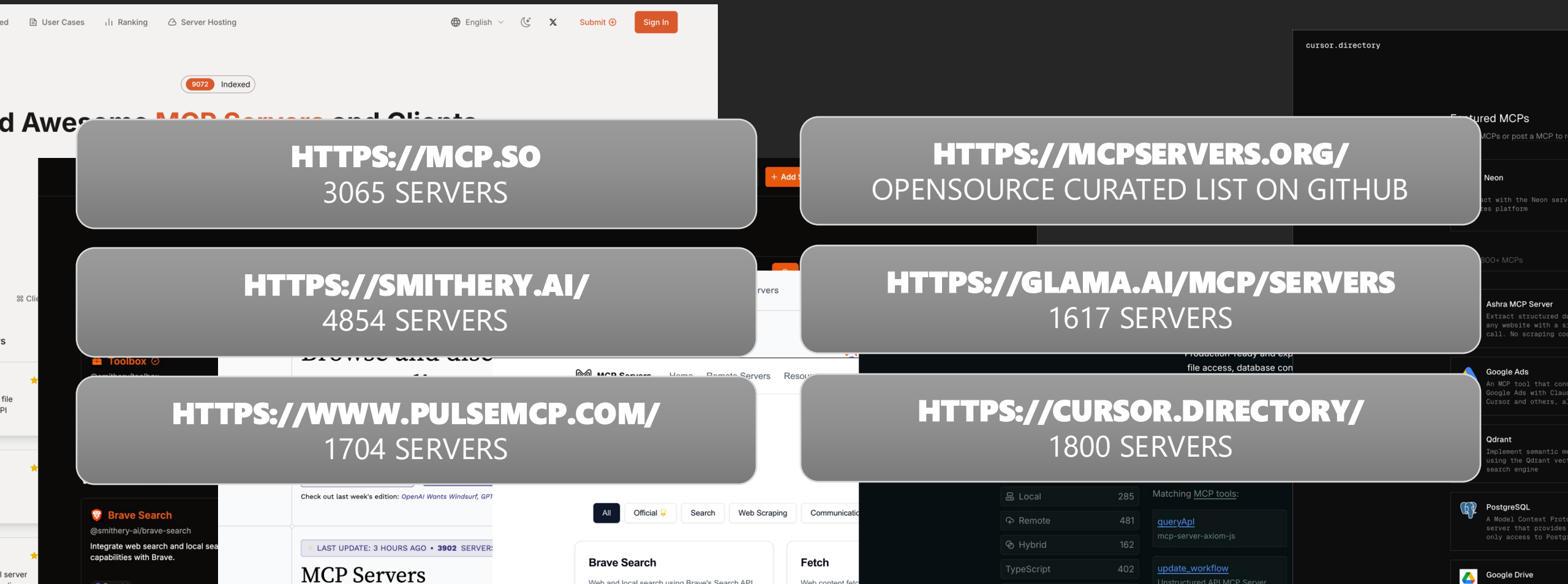
EXPLORATORY TESTING

UNSCRIPTED SCENARIOS

CREATING A MCP SERVER
FOR EVERY WEB APP?
AINT NOBODY GOT TIME FOR THAT
ZURE

MCP

EXPLOSION OF MCP SERVERS



HTTPS://MCP.SO
3065 SERVERS

HTTPS://MCPSERVERS.ORG/
OPENSOURCE CURATED LIST ON GITHUB

HTTPS://SMITHERY.AI/
4854 SERVERS

HTTPS://GLAMA.AI/MCP/SERVERS
1617 SERVERS

HTTPS://WWW.PULSEMCP.COM/
1704 SERVERS

HTTPS://CURSOR.DIRECTORY/
1800 SERVERS

CREATING MCP SERVERS

MAKE YOUR BUSINESS APP AI READY

.NET APIS

`MCPDOTNET`

https://www.nuget.org/packages/mcpdotnet

AZURE FUNCTIONS

`[MCPToolTrigger]`

EXPERIMENTAL ATTRIBUTE

CREATING MCP SERVERS

MAKE YOUR BUSINESS APP AI READY

COPILOT STUDIO

MCP CUSTOM CONNECTORS (PREVIEW!)

https://learn.microsoft.com/en-us/microsoft-copilot-studio/agent-extend-action-mcp

MCP

ALL THE THINGS!

ZURE

USING 3RD PARTY MCP SERVERS

MCP RISKS

TREAT THEM AS 3RD PARTY CODE PACKAGES

USING 3RD PARTY MCP SERVERS

MCP RISKS

TREAT THEM AS 3RD PARTY CODE PACKAGES

THEY ARE EXECUTING CODE ON YOUR MACHINE

WITH ACCESS TO ALL YOUR THINGS

YOU GET A MCP!
EVERYONE GETS A MCP!
ZURE

THANK YOU!
GEERT VAN DER CRUIJSEN
CEO ZURE NL
GEERT@ZURE.COM
Let's chat afterwards!
Or connect on LinkedIn
BUILD IT
RUN IT
BREAK IT
ZURE