



MCP and Agents: Open-Source Foundations for Agent Trust, Safety, and Scale

TechXchange | October 6-7, 2025

Fred Arauju: IBM Research

Dean Wampler, Jeffrey Borek, Dave Nielsen: IBM and The AI Alliance

Outline



Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts

Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts

ContextForge MCP Gateway

Secure Open-Source Gateway, Proxy and Registry
for AI Agents and Tools

Unifying discovery, authentication, authorization, role-based access control, rate-limiting, observability, virtual servers, and protocol translation – with a security focus and configurable plugins

github.com/IBM/mcp-context-forge

Context Forge - Gateway Administration

AI Gateway and Registry supporting MCP, A2A and REST | [Docs](#) | [Star mcp-context-forge on GitHub](#) |

[All Teams](#) [admin@example.com](#) [Admin](#) [Logout](#)

[MCP Servers](#) [Virtual Servers](#) [Tools](#) [Prompts](#) [Resources](#) [Agents \(A2A\)](#) [Metrics](#) [Plugins](#) [MCP Registry](#) [Configuration](#) [Teams](#)

MCP Servers & Gateways

Gateways connect to external MCP servers (like GitHub, Notion, etc.) Once connected, their tools appear in the Tool Catalog automatically.

Show Inactive

Filter by Tags:
e.g., production,external (comma-separated) [Clear Filter](#)

S. NO.	NAME	URL	TAGS	STATUS	LAST SEEN	TEAM	VISIBILITY	ACTIONS
1	Find-A-Domain	https://api.findadomain.dev/mcp	domains dns search	Active	2025-10-02 18:37:52	N/A	Public	Test View Edit Deactivate Delete
2	DeepWiki	https://mcp.deepwiki.com/sse	rag wiki knowledge ai	Active	2025-10-02 18:38:03	N/A	Public	Test View Edit Deactivate Delete
3	LLM Text	https://mcp.llmtxt.dev/sse	ai nlm text-analysis	Active	2025-10-02 18:38:04	N/A	Public	Test View Edit Deactivate Delete
4	Cloudflare Docs	https://docs.mcp.cloudflare.com/sse	documentation cloudflare reference	Active	2025-10-02 18:38:09	N/A	Public	Test View Edit Deactivate Delete
5	Javadocs	https://www.javadoc.dev/mcp	java documentation api reference	Active	2025-10-02 18:38:16	N/A	Public	Test View Edit Deactivate Delete
6	OpenMesh	https://api.openmesh.dev/mcp	service-mesh discovery infrastructure	Active	2025-10-02 18:38:24	N/A	Public	Test View Edit Deactivate Delete



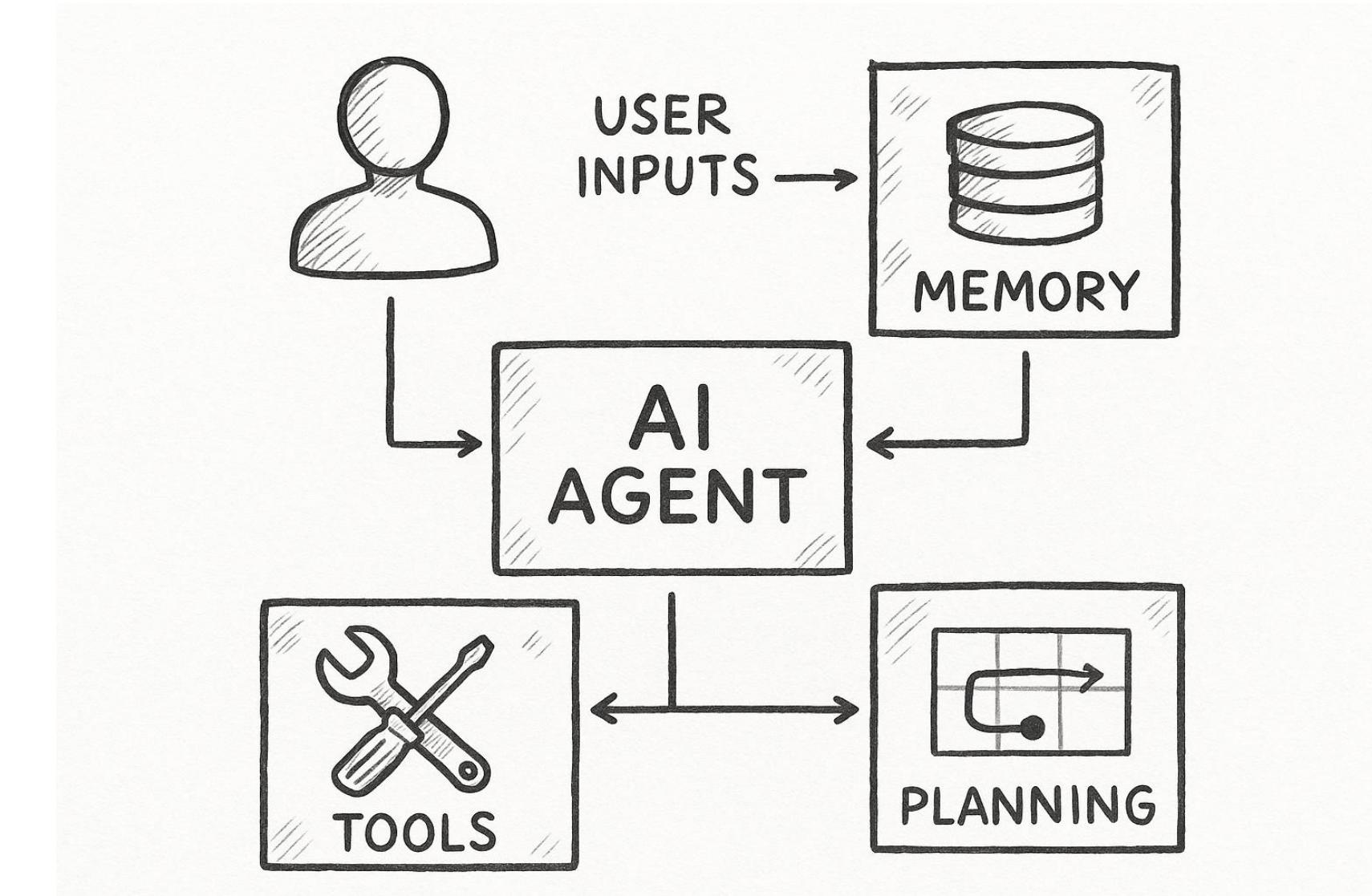
AI Agents use tools to accomplish complex tasks

AI Agent

A modular, goal-driven component that uses tools, memory, and reasoning to autonomously complete tasks via language models

These agents can plan, interact with APIs or other agents, and make decisions based on prompts, documents, or user input. They're often orchestrated in a multi-agent system to collaboratively solve complex problems

They typically use an agentic framework or orchestrator (e.g., langgraph, langchain, autogen, crew.ai) for tool execution



What can they do with tools?

Retrieve external information (e.g., web search, databases, RAG) as necessary, call other Agents or request user input

Generate artifacts (images, diagrams, word documents, excel files), interact with external APIs and systems using various Tools, run unit tests, etc.

Agents and tools turn “thoughts” into actions

Large Language Models call Tools through "Agentic Frameworks";
The LLM selects the right tool and parameters based on its
description, then processes the output.

Example

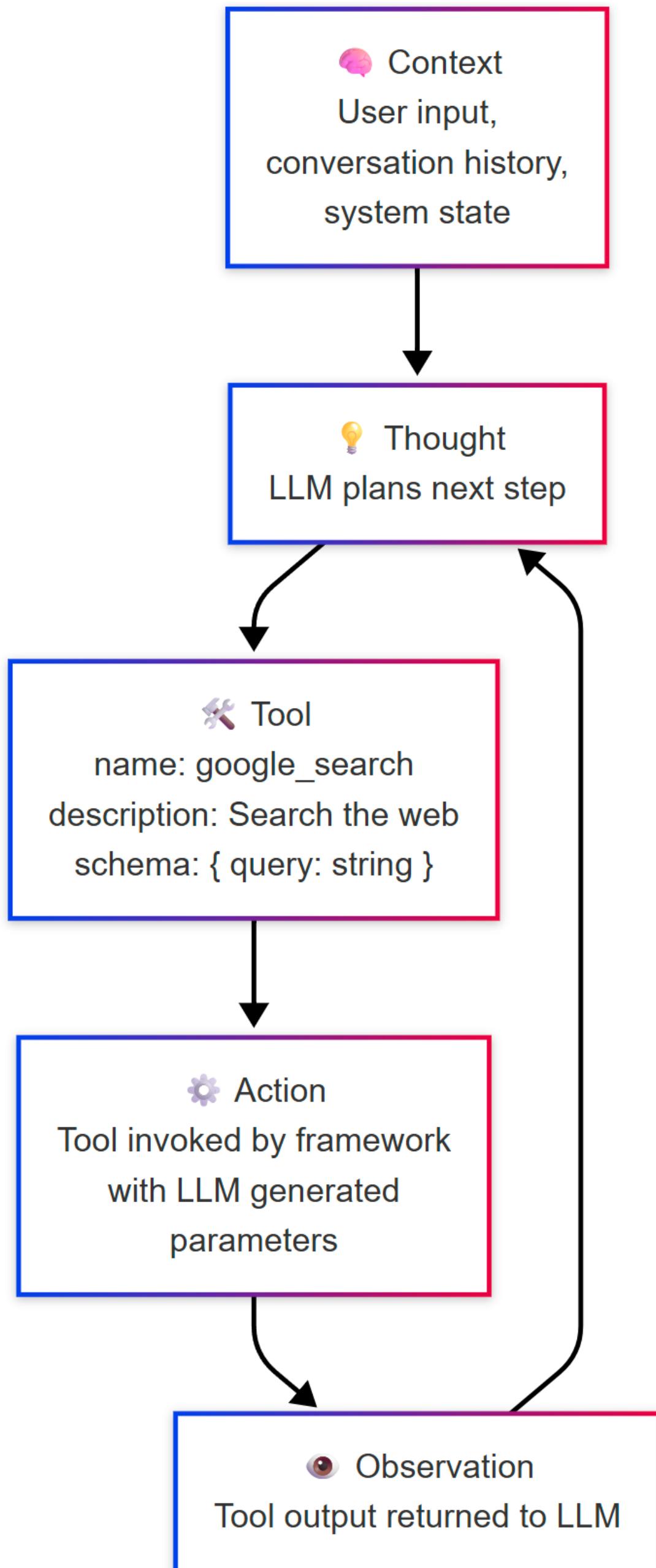
`name: google_search`

`description: Use this tool to search the internet,
providing an input prompt.`

`input schema: {"query": "Latest News"}`

MCP standardizes how AI Agents interact with Tools

- MCP de-couples AI Tools from the Agentic Platform
- Without MCP, each framework or AI tool would duplicate work,
and LLMs couldn't be 'fine tuned' for standardized tool calling.



Model Context Protocol (MCP) – "the USB-C for AI tools"

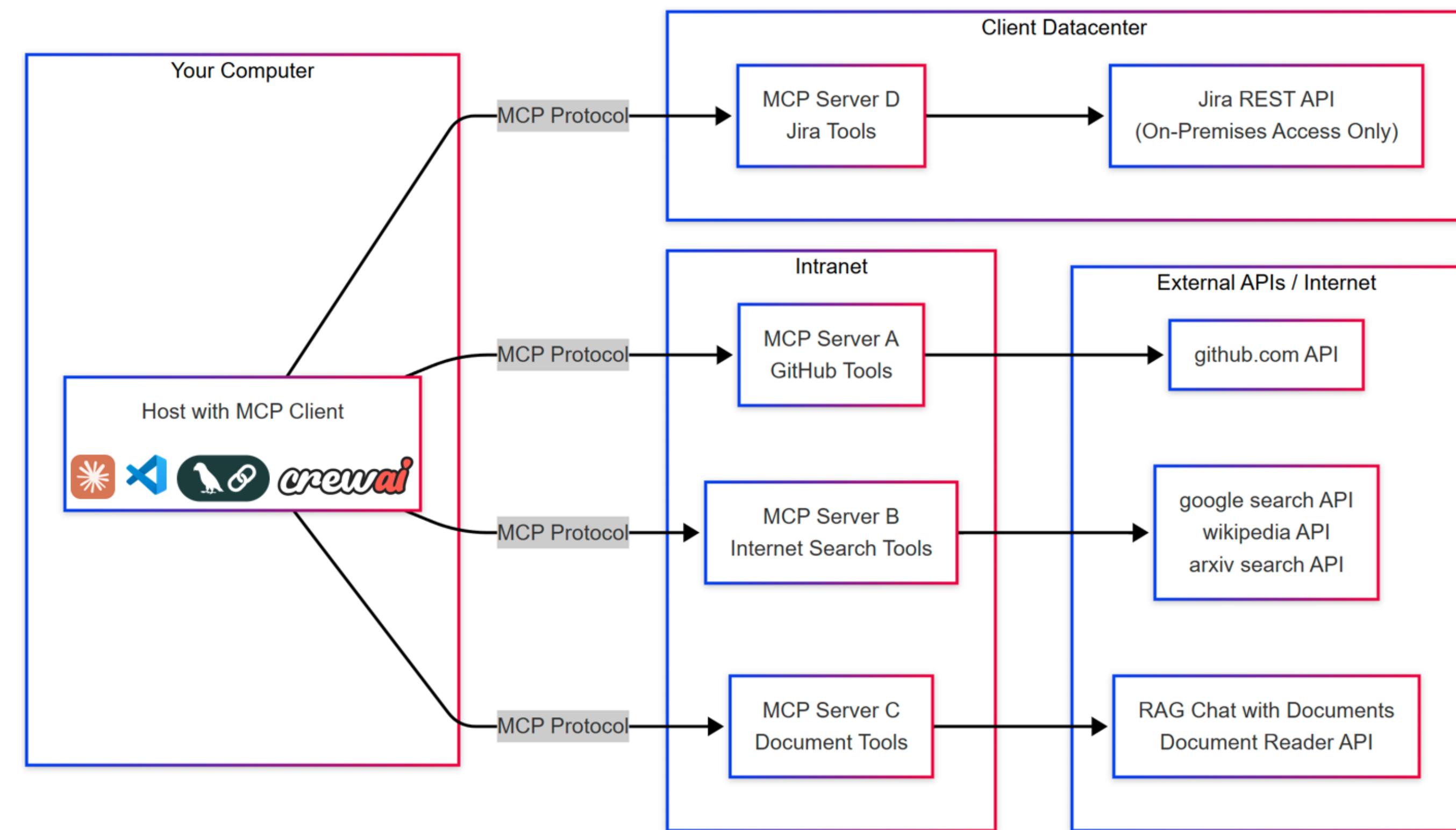
MCP Overview

- An open protocol introduced by Anthropic in November 2024 to standardize tool calling
- Enables a consistent interface to define how Agents and applications discover, invoke, and interact with tools and other context (prompts, resources)

Widely adopted: 15,000+ community servers developed since launch; wide adoption by major vendors

Still Evolving: the standard is rapidly evolving to resolve gaps in security, granular access controls, transparent tool usage, and user interaction, but many tools only implement a partial or older spec

ContextForge addresses these gaps



MCP Hosts: applications or AI tools that want to access data via MCP (VSCode+ Copilot/Cline/Continue, Langchain, Crew.AI, Claude Desktop)

MCP Clients: Protocol clients that maintain 1:1 connections with servers

MCP Servers: Lightweight programs that each expose specific capabilities through Model Context Protocol

ContextForge addresses challenges with the MCP Ecosystem

MCP challenges

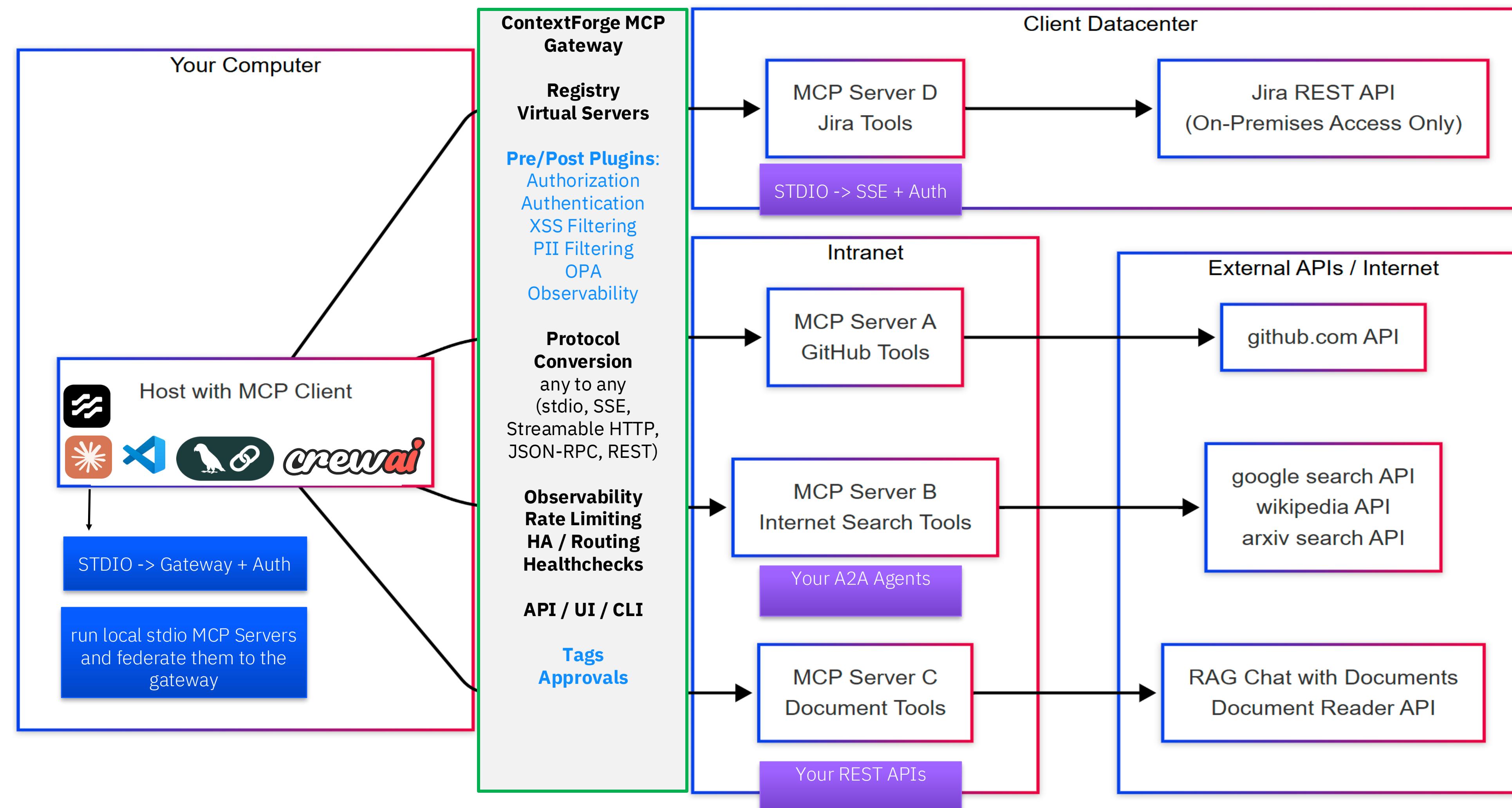
MCP gained rapid adoption – but the ecosystem evolved unevenly. Many tools only partially implement the spec, and integration challenges remain:

- Existing tools: REST endpoints must be rewritten to become MCP-compliant.
- Protocol and security inconsistency: some use JWT authentication, others OAuth2, many use nothing at all – while most servers are still developed to stdio / SSE transport (instead of the newer streamable HTTP).
- Integration complexity: tools are scattered across servers, each with its own config, retry logic, and monitoring gaps

MCP Gateway emerges as a mandatory pattern when deploying MCP in the enterprise

- Acts as a secure, unified proxy between AI agents and tool servers, easily deployable in remote environments.
- Convert between different transports, add authorization, security, observability, retry logic, and tool lifecycle controls – allowing you to quickly convert non-compliant MCP servers to the latest standard, and add security, observability, etc.
- Wrap any REST API and exposes it as a typed, discoverable MCP-compatible tool
- Reusable building block, easily embedded into other products and tools

ContextForge: open source secure, modular proxy for MCP



Security-first design

Core Security Mission

Protect against untrusted MCP servers

Sanitize all inputs/outputs

Policy-based access control

Pluggable security middleware

Isolation Capabilities

Separate tool namespaces

Independent auth configs

Per-server rate limits

Custom security policies

Enterprise Security

Policy as Code with OPA

SSO Integration

(OAuth/SAML), JWT

RBAC, Multi-tenancy,

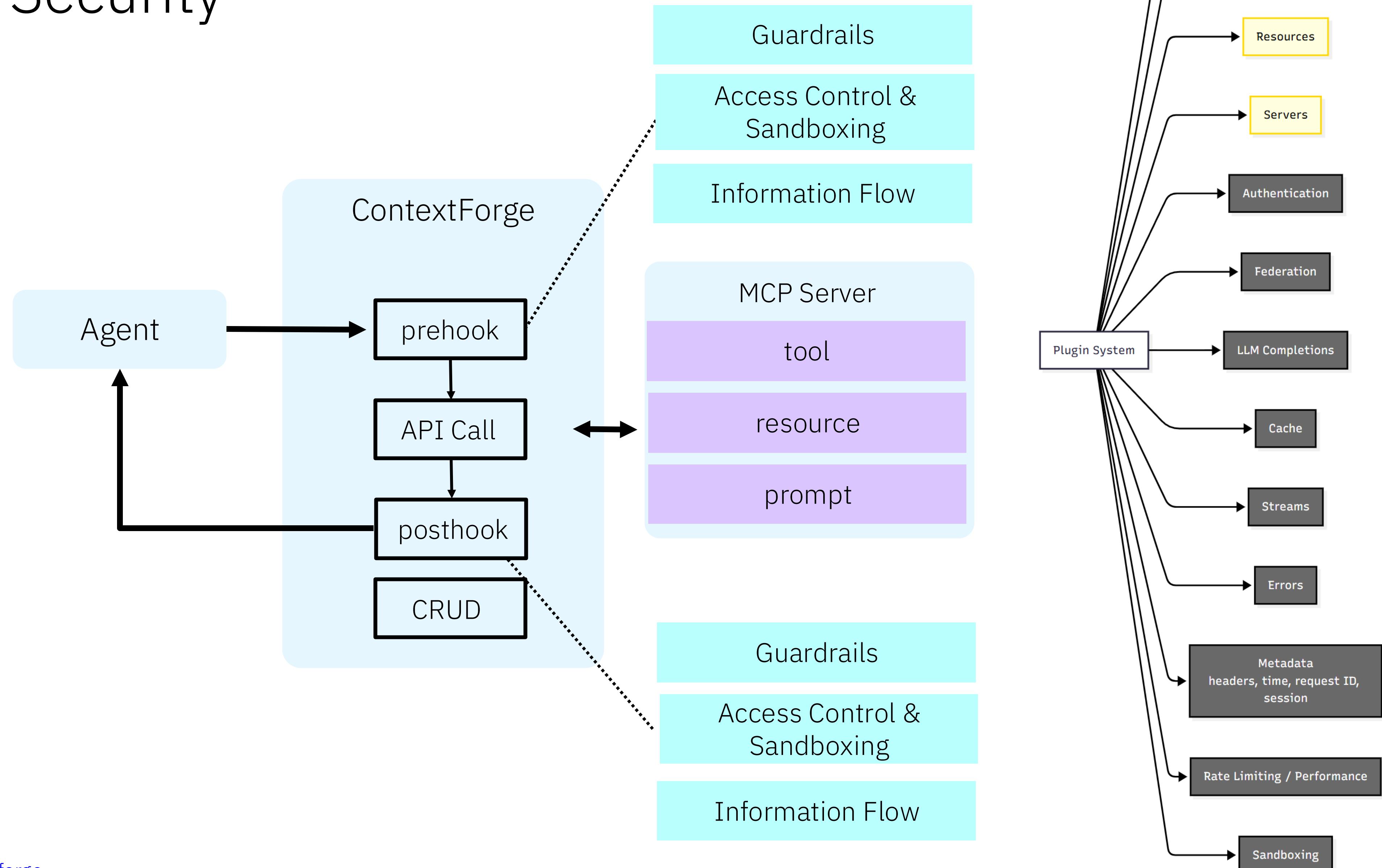
Database Encryption

Observability

(OpenTelemetry)

ContextForge with Pluggable Security

Security extensions
implemented as LSM-style
hooks to ContextForge



Community engagement and growth



2.6k+ stars

319 forks

57 contributors

The most popular MCP Gateway!
– with highest number of
features and a security focus

Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts

Trends in Artificial Intelligence - Closed or Open?

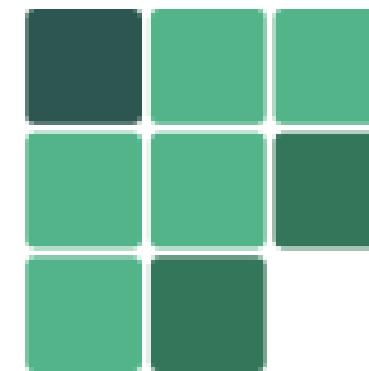
ANNALS OF TECHNOLOGY

THE INSIDE STORY OF MICROSOFT'S PARTNERSHIP WITH OPENAI

The companies had honed a protocol for releasing artificial intelligence ambitiously but safely. Then OpenAI's board exploded all their carefully laid plans.

By Charles Duhigg

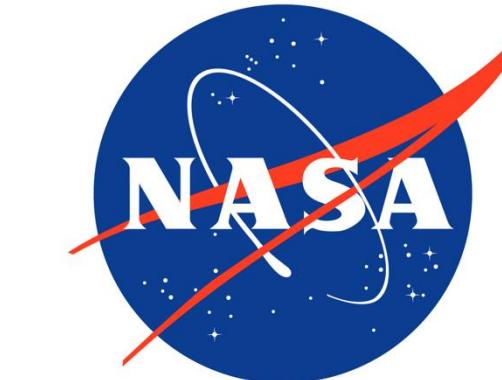
December 1, 2023



FRONTIER MODEL FORUM

“The future of AI is open — no matter what some say.”

Dario Gill, SVP and Director of Research, IBM



AI Alliance

Meta and IBM form open-source alliance to counter big AI players

NASA, Intel, Yale University and more related bodies are involved.



Sarah Fielding

Tue, Dec 5, 2023 · 2 min read



1



aialliance.org

The AI Alliance brings together organizations, people, and resources to accelerate *open innovation, technology development* and *adoption*.

Launched December 5, 2023



linkedin.com/company/the-aialliance/



bsky.app/profile/aialliance.bsky.social

Map of Members

Member organizations in the AI Alliance comprise academia, commercial, research and non-profits and span the globe.

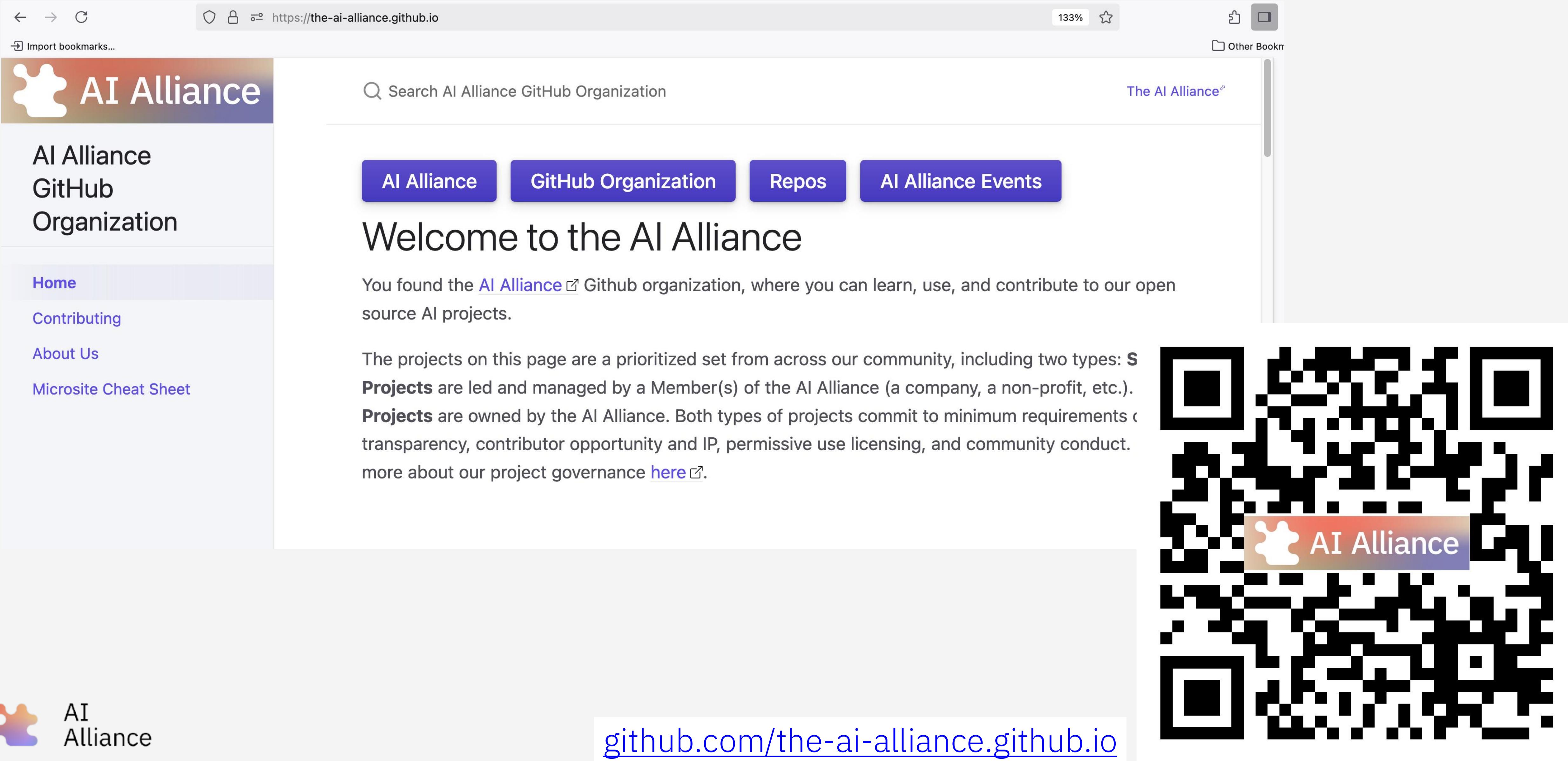
Our core beliefs in AI
that is open is the tie
that binds us, despite
our differences.



The AI Alliance is made up of ~200 organizations in 24+ countries, and growing



Numerous Projects:



The screenshot shows the homepage of the AI Alliance GitHub organization. The URL in the browser bar is <https://the-ai-alliance.github.io>. The page features a header with the AI Alliance logo and a search bar. Below the header are four navigation buttons: "AI Alliance", "GitHub Organization", "Repos", and "AI Alliance Events". The main content area has a large heading "Welcome to the AI Alliance" and a paragraph explaining the organization's purpose. To the right of the text is a QR code with the AI Alliance logo in the center.

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

AI Alliance GitHub Organization Repos AI Alliance Events

Welcome to the AI Alliance

You found the [AI Alliance](#) GitHub organization, where you can learn, use, and contribute to our open source AI projects.

The projects on this page are a prioritized set from across our community, including two types: **Projects** are led and managed by a Member(s) of the AI Alliance (a company, a non-profit, etc.). **Projects** are owned by the AI Alliance. Both types of projects commit to minimum requirements of transparency, contributor opportunity and IP, permissive use licensing, and community conduct. Learn more about our project governance [here](#).

github.com/the-ai-alliance.github.io

Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts

Open Agent Lab

AI ALLIANCE

About Agents Components Use Cases Research Q Log In

Open Agent Lab

Innovators, researchers, and engineers uniting to craft the next generation of domain-specific AI —powered by open source and tested in real-world enterprises.

All Agents Components Use Cases Research Newest

 AFerretti @AFerretti · September 17, 2025 Components

NextGem Catalog

NextGem is an innovative tool designed to transform the open data landscape by focusing on transparency and usability. Imagine a world where...

[View external link](#)

0 likes 0 comments Bookmark Share

 Tim Bonnemann @tbonnema · September 16, 2025 Components

DANA

Domain-Aware Neurosymbolic Agent (Dana), an agent-native programming language

[View external link](#)

0 likes 0 comments Bookmark Share

 Tim Bonnemann @tbonnema · September 16, 2025 Components

Docling

Docling simplifies document processing, parsing diverse formats — including advanced PDF understanding — and providing seamless...

[View external link](#)

0 likes 0 comments Bookmark Share

 Tim Bonnemann @tbonnema · September 16, 2025 Components

Llama Stack

Composable building blocks to build Llama Apps

[View external link](#)

0 likes 0 comments Bookmark Share

 Tim Bonnemann @tbonnema · September 16, 2025 Components

SEMIKONG

First Open-Source Industry-Specific Model for Semiconductors

[View external link](#)

0 likes 0 comments Bookmark Share

 Tim Bonnemann @tbonnema · September 16, 2025 Agent

Deep Research Agent for Finance

This app is an example application of a deep research agent designed to collect comprehensive information about publicly-traded companies an...

[View external link](#)

0 likes 0 comments Bookmark Share

github.com/the-ai-alliance.github.io



AI Alliance

MCP Projects

AI Alliance GitHub Organization

Home Home Contributing About Us Microsite Cheat Sheet

AI Alliance

<https://the-ai-alliance.github.io> 133% Import bookmarks... Other Bookmarks

Model Context Protocol (MCP) Ecosystem and Related Projects

The [Model Context Protocol](#) (MCP) from [Anthropic](#) is quickly becoming an industry standard for communications between models, agents, data repositories, and other tools. The AI Alliance seeks to advance this protocol and foster a robust suite of tools around it to enable broad, trusted, and high-value use in production.

Links	Description
MCP in the Enterprise: A User Guide	<p>MCP has enormous potential to accelerate AI adoption in enterprises. This "living" user guide features chapters written by experts on various aspects of deploying, managing, and using MCP successfully in enterprise settings. It contains the first two chapters with many more planned. Contributions are welcome!</p> <ul style="list-style-type: none">repodashboardissuesdiscussions
Deep Research Agent for Finance	<p>The Deep Research Agent for Finance project demonstrates MCP in action for a common design pattern, <i>Deep Research Agent</i>. This example shows how a financial analyst can use a deep research agent to find, aggregate, and analyze information about a public company (or other potential investment). There are many other applications possible. The app is built on MCP Agent, developed by LastMile AI, discussed next.</p> <ul style="list-style-type: none">repodashboardissuesdiscussions
LastMile AI MCP Agent	<p>Build effective agents using Model Context Protocol and simple to sophisticated workflow patterns. See the Deep Research Agent for Finance, discussed in the previous row, which is</p> <ul style="list-style-type: none">repo...

AI Alliance



User Guide: MCP in the Enterprise

The screenshot shows a web browser displaying the AI Alliance User Guide at <https://the-ai-alliance.github.io/enterprise-MCP/developing-mcp-servers/>. The page title is "MCP in the Enterprise: A User Guide". The main content is titled "Developing MCP Servers: Tools, Techniques, and Design Patterns". A large blue button labeled "Demo" is visible on the left. The navigation menu includes "Home", "Developing MCP Servers" (which is expanded to show "Building a Deep Research Agent Using MCP-Agent"), "Getting to Know MCP and Its Ecosystem", "Contributing", and "About Us". On the right, there are buttons for "Join This Project", "GitHub Repo", and "Discuss This Guide". The footer features the AI Alliance logo and a copyright notice.

MCP in the Enterprise: A User Guide

Join This Project GitHub Repo Discuss This Guide

Developing MCP Servers: Tools, Techniques, and Design Patterns

This section contains chapters about how to write effective MCP servers, including experience reports, tools to consider, and other guidance. Here is a summary of these chapters.

Building a Deep Research Agent Using MCP-Agent

In [Building a Deep Research Agent Using MCP-Agent](#), Sarmad Qadri , Co-founder and CEO at LastMile AI, and creator of [mcp-agent](#)  documents the journey of building a **Deep Research Agent** with mcp-agent, highlighting the evolution from an initial *Orchestrator* design, to an over-engineered *Adaptive Workflow*, and finally to the streamlined [Deep Orchestrator](#)  now supported in mcp-agent. Sarmad emphasizes his view that “MCP is all you need,” and shows how connecting LLMs to MCP servers with simple design patterns enables agents to perform complex, multi-step research tasks. Key lessons include the importance of simplicity over complexity, leveraging deterministic, code-based verification alongside LLM reasoning, external memory for efficiency, and structured prompting for clarity. The resulting Deep Orchestrator balances performance, scalability, and adaptability, proving effective across domains like finance research. Future directions include remote execution, intelligent tool and model selection, and treating memory and knowledge as MCP resources. The open-source project, available on [GitHub](#) , offers developers a powerful foundation for creating general-purpose, AI research agents.

MCP + Agents

AI Alliance GitHub Organization

Home Home Contributing About Us Microsite Cheat Sheet

AI Alliance

https://the-ai-alliance.github.io 133% Import bookmarks... Other Bookmarks

Model Context Protocol (MCP) Ecosystem and Related Projects

The [Model Context Protocol](#) (MCP) from [Anthropic](#) is quickly becoming an industry standard for communications between models, agents, data repositories, and other tools. The AI Alliance seeks to advance this protocol and foster a robust suite of tools around it to enable broad, trusted, and high-value use in production.

Links	Description
repo	MCP has enormous potential to accelerate AI adoption in enterprises. This "living" user guide features chapters written by experts on various aspects of deploying, managing, and using MCP successfully in enterprise settings. It contains the first two chapters with many more planned. Contributions are welcome!
repo	The Deep Research Agent for Finance project demonstrates MCP in action for a common design pattern, <i>Deep Research Agent</i> . This example shows how a financial analyst can use a deep research agent to find, aggregate, and analyze information about a public company (or other potential investment). There are many other applications possible. The app is built on MCP Agent , developed by LastMile AI , discussed next.
repo	Build effective agents using Model Context Protocol and simple to sophisticated workflow patterns. See the Deep Research Agent for Finance , discussed in the previous row, which is

Deep Research Agent for Finance

The [Deep Research Agent for Finance](#) project demonstrates MCP in action for a common design pattern, *Deep Research Agent*. This example shows how a financial analyst can use a deep research agent to find, aggregate, and analyze information about a public company (or other potential investment). There are many other applications possible. The app is built on [MCP Agent](#), developed by [LastMile AI](#), discussed next.

LastMile AI MCP Agent

Build effective agents using Model Context Protocol and simple to sophisticated workflow patterns. See the [Deep Research Agent for Finance](#), discussed in the previous row, which is



MCP + Agents: Deep Research App

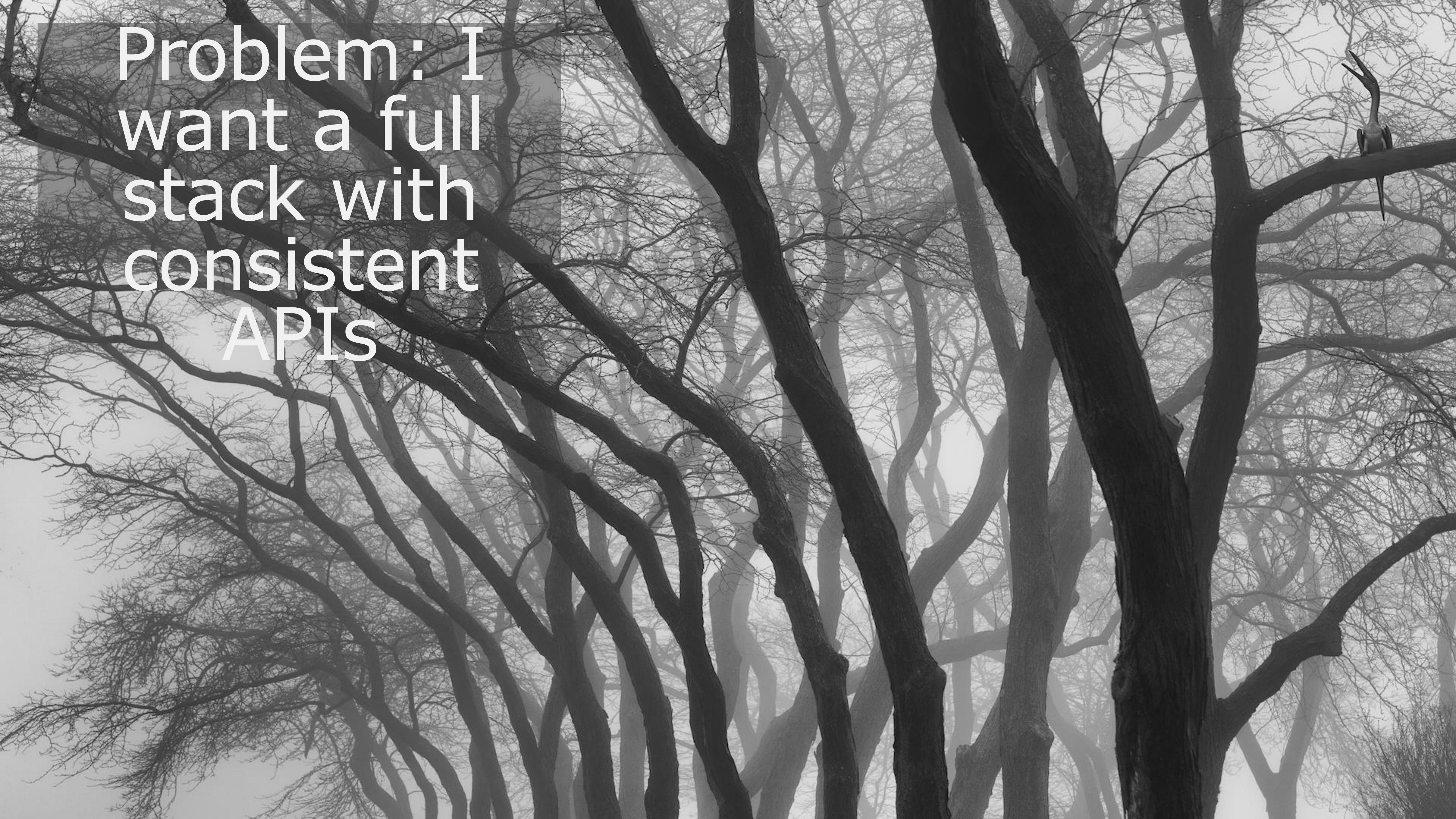
The screenshot shows a GitHub repository page for 'The-AI-Alliance/deep-research-agent-for-finance'. The page includes a navigation bar with links for Code, Issues (4), Pull requests, Discussions, Actions, Projects (1), Wiki, and Security. Below the navigation is a header with the repository name, a search bar, and user profile icons. The main content area displays the repository's details: 'deep-research-agent-for-finance' (Public), Edit Pins, Watch (0), Fork (4), and Star (19). A note indicates it was generated from [The-AI-Alliance/microsite-template](#). On the left, there's a sidebar with a 'main' dropdown, file navigation icons, and a 'Go to file' button. The right sidebar contains an 'About' section with a description of the app as an example of building production-quality AI applications, along with links to Readme, Contributing, Activity, Custom properties, 19 stars, and 0 watching. A large blue button with the word 'Demo' is overlaid on the commit history. The commit history lists several recent changes:

- andrew-lastmile Merge pull request #16 from andrew-la... (last week)
- .github Forgot to add the "use case" label. (3 months ago)
- docs merge (2 weeks ago)
- Added a title. (3 months ago)
- deep finance research (2 months ago)
- Delete src/finance_deep_search/fina... (last week)
- .gitignore integrating deep orchestrator (2 months ago)
- GITHUB_PAGES.md Typo! (3 weeks ago)

At the bottom left, there's an 'AI Alliance' logo.

Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts



Problem: I
want a full
stack with
consistent
APIs

Solution: Llama Stack

The screenshot shows a web browser window with the URL <https://the-ai-alliance.github.io>. The page is titled "Llama Stack and Llama Stack Agents". On the left, there's a sidebar with the "AI Alliance GitHub Organization" logo and links to "Home", "Contributing", "About Us", and "Microsite Cheat Sheet". The main content area describes the Llama Stack project, mentioning its goal of standardizing building blocks for AI application development, integrating with other tools, and providing APIs for inference, evaluation, agents, and deployment. It also mentions the "llama-stack-examples" project, which includes two initial example applications: a chatbot app and a deep research app. A QR code is visible on the right side of the page.

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

Llama Stack and Llama Stack Agents

The [Llama Stack](#) project standardizes the core building blocks that simplify AI application development. It codifies best practices across the Llama ecosystem, integrates with other open-source tools and managed services, and provides APIs for inference, evaluation, agents, [MCP](#), and deployment requirements like observability. It is designed to support both on-premise and cloud deployments. The ecosystem provides many example applications to help developers build and deploy AI applications quickly and effectively.

AI Alliance members are [contributing directly](#) to Llama Stack development, as well as building example applications that illustrate its use in various enterprise scenarios. The `llama-stack-examples` project has two initial example applications, described in the table below. The first app is a simple getting-started chatbot that shows you the basics of creating an app with Llama Stack and how to run it. The second app (in development) is a *deep research* application, a popular class of AI applications, which will demonstrate Llama Stack support for technologies like agents and [MCP](#). Other examples under consideration will be chosen to cover other common application patterns seen in several industries. [Please join us!](#)

Links	Description
AI Alliance Llama Stack Example Apps	<p>A growing suite of example applications for Llama Stack that demonstrate various stack features and common application patterns:</p> <ul style="list-style-type: none">repoissuesdiscussions <p>1 A getting-started chatbot app, which shows how to build and deploy Llama Stack applications. It includes two different UI options and inference with an ollama-hosted Llama 3 model.</p> <p>2 A <i>deep research</i> app (under development), which illustrates an emerging, common application pattern for AI. The user asks for detailed information about a topic, for example</p>





Problem: I
need open,
trusted
datasets

Solution: Open Trusted Data Initiative

← → ⌂ https://the-ai-alliance.github.io 133% ⭐

Import bookmarks... Other Bookmarks

AI Alliance

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

Open Trusted Data and Tooling

Good datasets are essential for building good models and applications. The AI Alliance is cataloging datasets, and in some cases building them, that have clear licenses for open use, backed by unambiguous provenance and governance constraints.

Links	Description
The Open, Trusted Data Initiative	<p>Open data has clear licence for use, across a wide range of topic areas, with clear provenance and governance. OTDI seeks to clarify the criteria for openness and catalog the world's datasets that meet the criteria. Our projects:</p> <ul style="list-style-type: none">repo ↗dashboard ↗issues ↗discussions ↗Open Dataset Catalog: details ↗, current work ↗Define Openness Criteria: details ↗, current work ↗Find Diverse Datasets: details ↗, current work ↗Data Pipelines to Validate Datasets: details ↗, current work ↗
Docling	<p>Docling simplifies document processing, parsing diverse formats — including advanced PDF understanding — and providing seamless integrations with the gen AI ecosystem. Docling is a key tool for the project <i>Parsing PDFs to Build AI Datasets for Science</i>, discussed above. (Principal developer: IBM Research ↗)</p>

AI Alliance



Solution: Open Trusted Data Initiative

The screenshot shows a web browser displaying the AI Alliance website at <https://the-ai-alliance.github.io/open-trusted-data-initiative/>. The page features a header with the AI Alliance logo and navigation links for 'Join Our Initiative', 'Browse the Datasets', and 'Contribute a New Dataset'. A large section titled 'Open Trusted Data Initiative (OTDI)' contains a yellow callout box with the text: 'We are building the world's largest, most diverse catalog of open and transparently sourced datasets for AI. [Join us!](#)'.

AI Alliance

Open Trusted Data Initiative

Start Here!

Trustworthiness

Dataset Catalog

Dataset Specification

How We Process Datasets

How to Contribute

About Us

References

Demo

Search Open Trusted Data Initiative

Join Our Initiative Browse the Datasets Contribute a New Dataset

Open Trusted Data Initiative (OTDI)

We are building the world's largest, most diverse [catalog](#) of open and transparently sourced datasets for AI. [Join us!](#)

Datasets for Languages

Datasets with different human languages.

Subcategories

African Languages Languages in the Americas Asian Languages

European Languages Languages in the Middle East

Languages of the Pacific Islands and Nations



Problem: I don't
know how to
test AI-enabled
apps!

Solution: Evaluation and Safety

← → ⌂ https://the-ai-alliance.github.io 133% ⭐

Import bookmarks... Other Bookmarks

AI Alliance

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

Governance, Evaluation, and Safety

Safety, accuracy, red-teaming, security, compliance, and more are required for successful AI applications. How do we know that AI applications are *trustworthy*, that they are *safe*, meaning free of harmful outputs, that they correctly implement the required behaviors? The following projects address these concerns.

Links	Description
The AI Trust and Safety User Guide	An introduction to trust and safety concepts from diverse experts, followed by recommendations for how to meet your application's needs. Start here if you are new to trust and safety, then leverage the projects discussed next to implement what you need.
Achieving Confidence in Enterprise AI Applications	Are you an enterprise developer? How should you test AI applications? You know how to write <i>deterministic</i> tests for your "pre-AI" applications. What should you do when you add generative AI models, which aren't deterministic? This project adapts existing evaluation techniques for the "last mile" of AI evaluation; verifying that an AI application correctly implements its requirements and use cases, going beyond the general concerns of evaluation for safety, security, etc. We are building nontrivial, reusable examples and instructional materials, so you can use these techniques effectively in combination with the traditional tools you already know. See also the companion Evaluation Reference Stack and Evaluation Is for Everyone projects. This project is part of the Trust and Safety Evaluation Initiative (TSEI).



Evaluation Is for Everyone



Solution: Evaluation and Safety

The screenshot shows a web browser displaying the AI Alliance website at <https://the-ai-alliance.github.io/ai-application-testing/>. The page title is "Achieving Confidence in Enterprise AI Applications". A large blue button labeled "Demo" is prominent on the left. The main content area features a search bar, two purple buttons ("Join This Project" and "GitHub Repo"), and a large heading. A sidebar on the left lists navigation links.

AI Alliance

Achieving Confidence in Enterprise AI Applications

Home
Testing Problems
Architecture and Design for Testing
Testing Strategies and Techniques
A Working Example
Glossary of Terms

Demo

Search Achieving Confidence in Enterprise AI Applications

Join This Project GitHub Repo

Achieving Confidence in Enterprise AI Applications

(Previous Title: *AI Application Testing for Developers*)

I am an Enterprise Developer: How Do I Test My AI Applications??

I know how to test my traditional software, which is **deterministic** (more or less...), but I don't know how to test my AI applications, which are uniquely **nondeterministic**.

Welcome to the **The AI Alliance** project to advance the state of the art for **Enterprise Testing of Generative AI Applications**. We are building the knowledge and tools you need to achieve the same testing confidence for your AI applications that you have for your traditional applications.

Tips:

- 1 Use the search box at the top of this page to find specific content.
- 2 [Capitalized Terms](#) link to glossary definitions.
- 3 Most chapters have a **Highlights** section at the top that summarizes the key takeaways from that chapter.

Outline

- ContextForge
- What Is the AI Alliance... and Why?
- Building AI-empowered Applications:
Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA
Projects
- Final Thoughts

Final Thoughts



ContextForge - Meets many requirements for enterprise deployments of MCP.



The AI Alliance - Strives to make all users able to safely and successfully use AI.



ContextForge - Many requirements for enterprise deployments of AI

Fill out our Trust and Safety survey! What are you doing? What concerns do you have?

AI Alliance -
is to make all
able to safely
successfully use



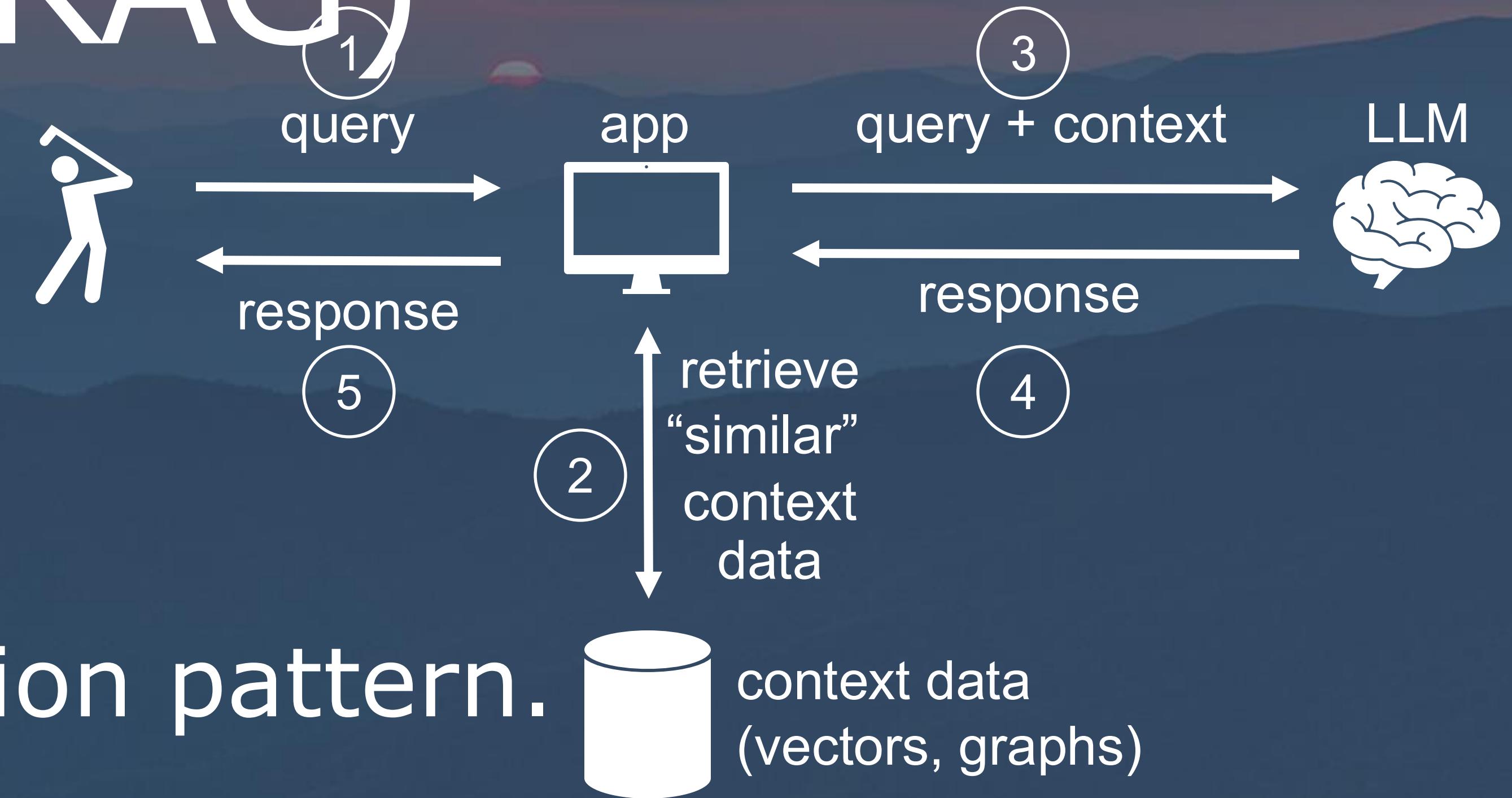
Extra Slides



Extra Slides

Retrieval-augmented
Generation (RAG)

Retrieval-Augmented Generation (RAG)



The first GenAI application pattern.

- Improves alignment.
- Incorporates new knowledge after training was done.
- Incorporates proprietary domain or use-case knowledge.

AllyCat

README Apache-2.0 license



license Apache-2.0 issues 16 open Stars 56

AllyCat

AllyCat is full stack, open source chatbot that uses GenAI LLMs to answer questions about your website. It is simple by design and will run on your laptop or server.

Why?

AllyCat is purposefully simple so it can be used by developers to learn how RAG-based GenAI works. Yet it is powerful enough to use with your website. You may also extend it for your own purposes.

★ Found this tool helpful? Give it a star on GitHub to support the project and help others discover it!

📢 [Allycat news](#) - releases and new features!

How does it work?

AllyCat uses your choice of LLM and vector database to implement a chatbot written in Python using [RAG](#) architecture. AllyCat also includes web scraping tools that extract data from your website (or any website).

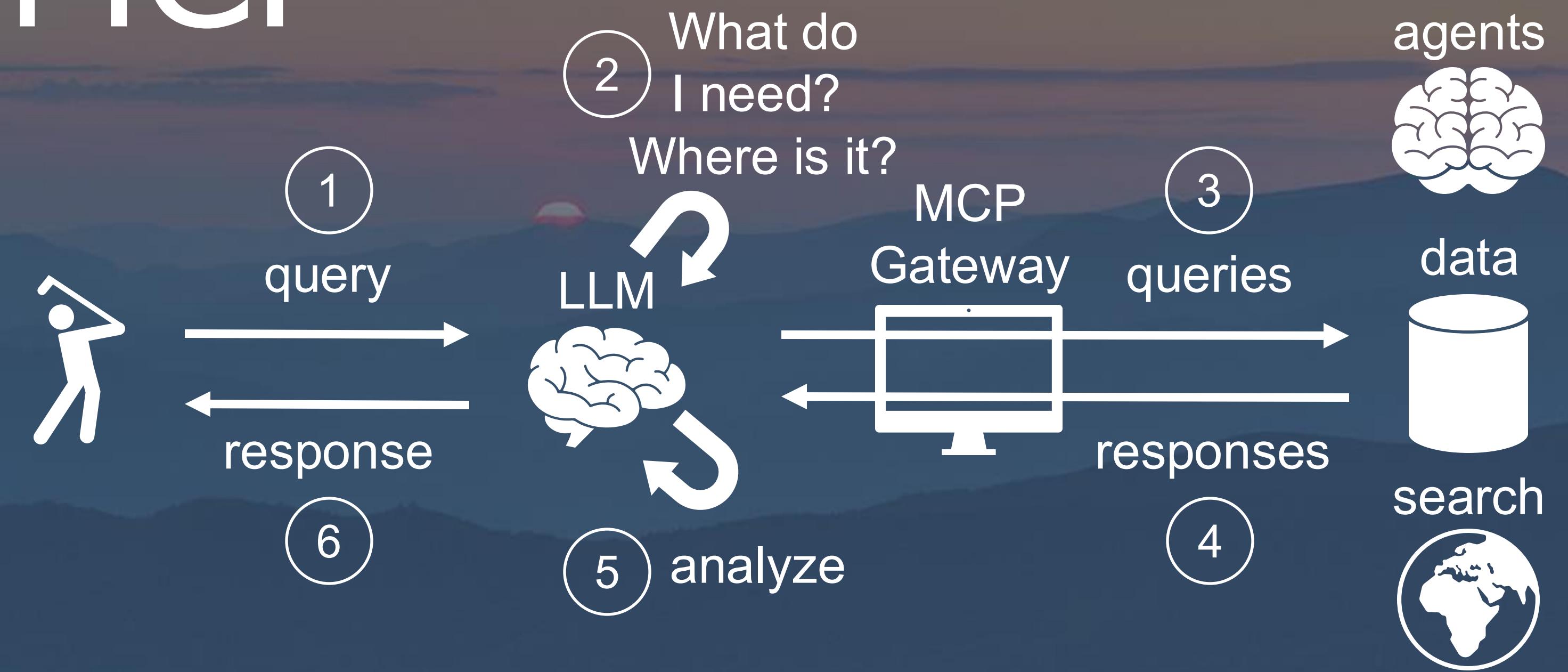
github.com/The-AI-Alliance/AllyCat/

Extra Slides

A wide-angle photograph of a mountain range at sunset. The sky is a vibrant orange and yellow, transitioning into darker blues and purples. In the foreground, a grassy hillside slopes down towards a winding path. A bright light source, possibly a headlamp or a camera flash, is visible on the path, creating a glowing trail. The mountains in the background are silhouetted against the bright sky, with their peaks gradually fading into the distance.

Agents and Model
Context Protocol
(MCP)

Agents and MCP



The second+ GenAI application pattern(s).

- LLMs do what they do best. Other tools do what they do best, orchestrated together.
- Flexible for very diverse use cases.