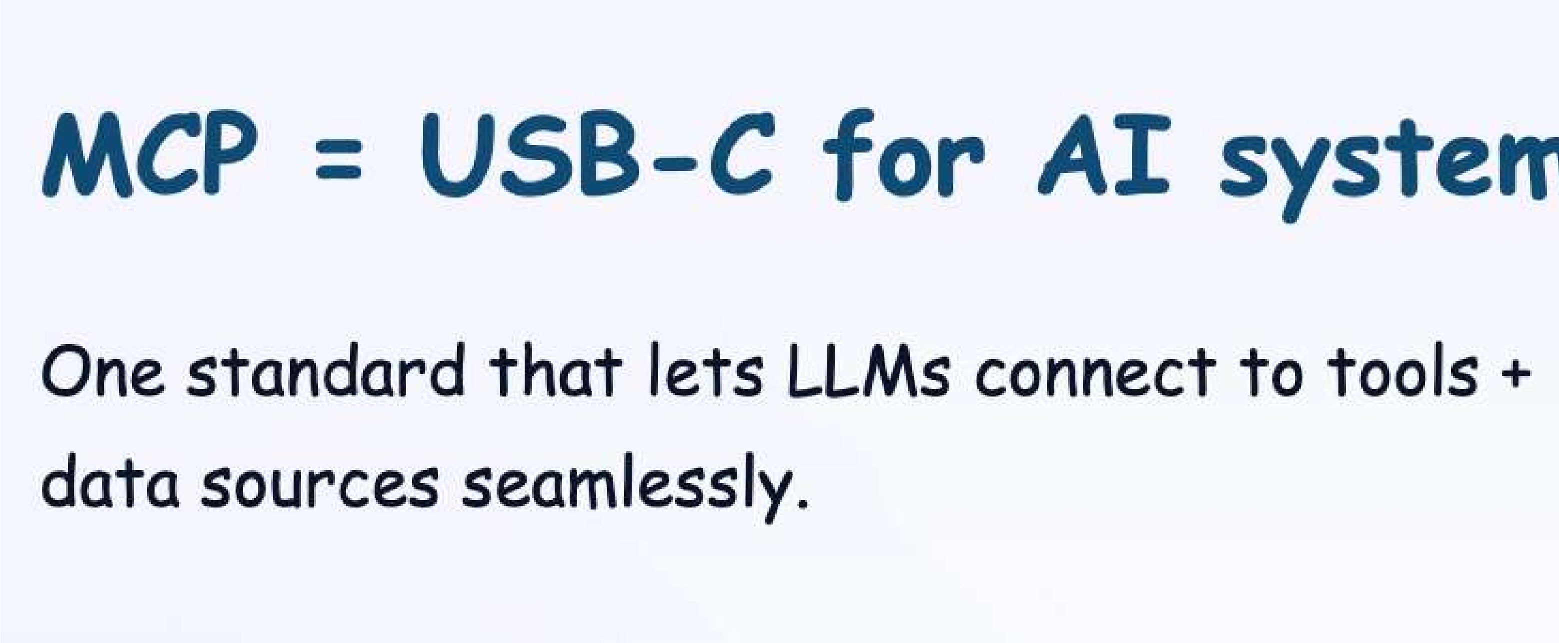
What is MCP?



MCP = USB-C for AI system

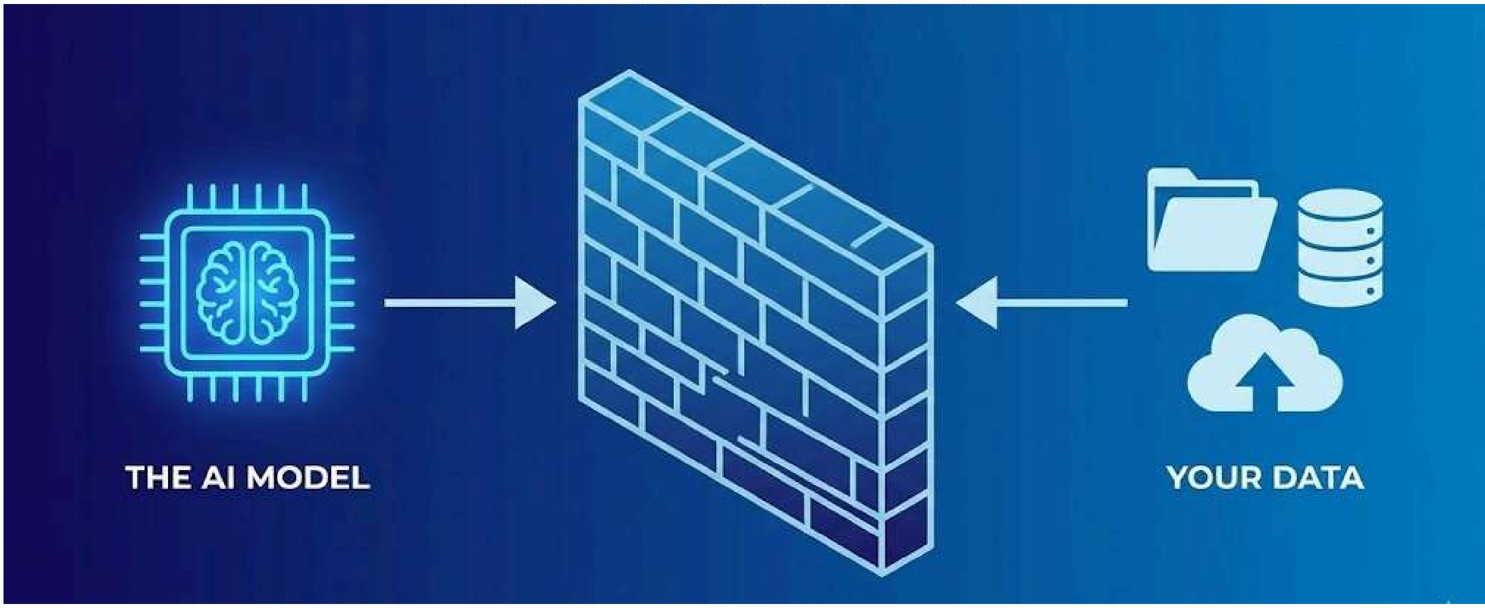
One standard that lets LLMs connect to tools + data sources seamlessly.

The Context Gap

LLMs are smart... but they can't access your:

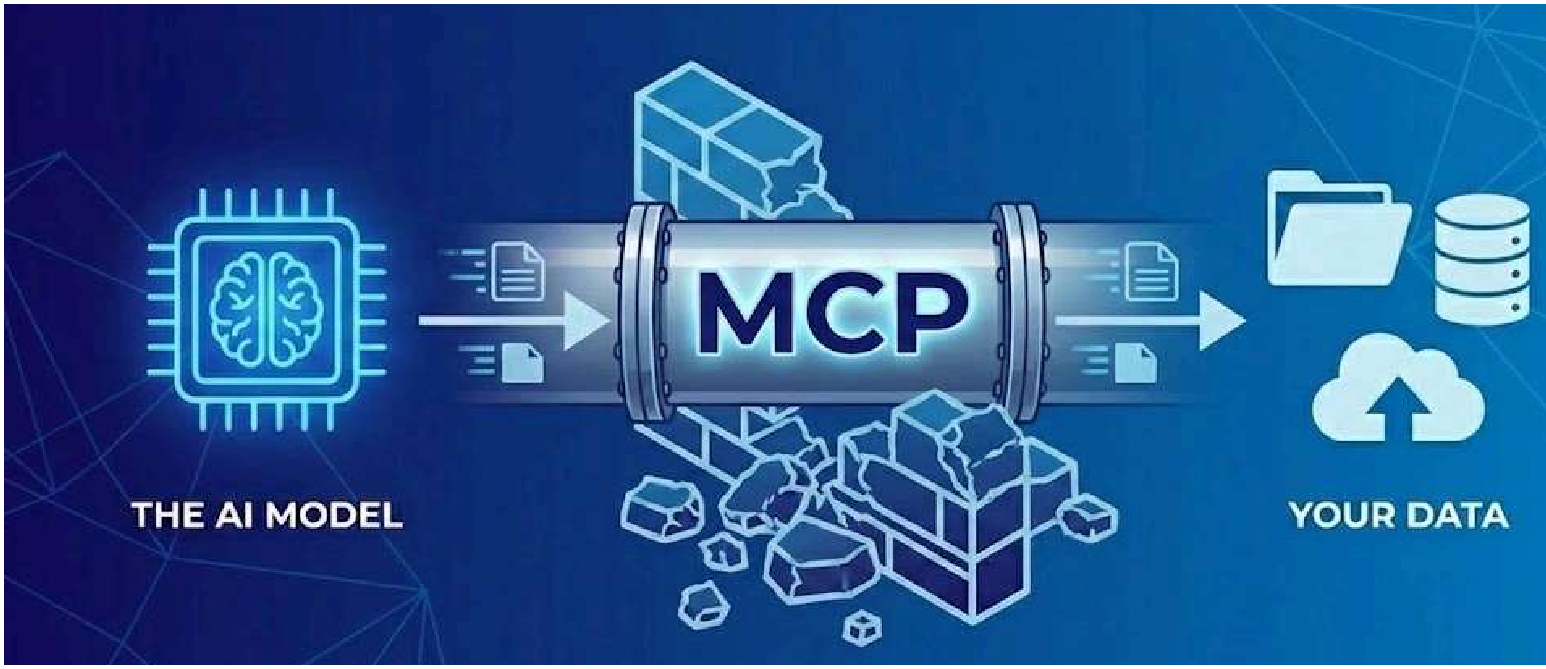
- Local files
- Internal APIs
- Live system data

They only know what you type.



Enter MCP

- MCP is an open standard that lets AI models t to your systems securely.
- Think of it as an API specifically designed for AI Assistants.
- The Goal: Give the AI tools to fetch its own data.



MCP Security Risks

Common risks you must plan for:

⚠️ Prompt Injection

⚠️ Tool Poisoning

⚠️ Sensitive Data Exposure

⚠️ Authentication Bypass

Latest MCP Advancements

What's improving fast:

🚀 Secure login support (OAuth-style)

🚀 Critical security fix released (update!)

🚀 Windows supports MCP natively

🐍

Build Your Own MCP

Python Implementation Guide

Let's Build Our Own MCP Server

Build your own MCP server in Python

🚀

Fast Setup

💻

Code Examples

🔧

Real Tools

✨

Production Ready

⚡ **Because MCP isn't just theory — you can implement**

1 Setup

Install modules (Python 3.9+)

We'll use FastMCP to keep it simple.

CODE

```
pip install fastmcp
```

2 Create the Server

Create a minimal MCP server

Start small: define a server name + initialize the MCP app.

CODE

```
from fastmcp import FastMCP
```

3 Create a Tool

Turn a Python function into an AI skill

Use @mcp.tool() → now your function becomes callable by the AI.

CODE

```python
@mcp.tool()
def get_weather(location: str):
    """Get weather for a location"""
    # Your logic here
    return f"Weather in {location}"
```

4 Connect to the Real World

Example idea: live weather using requests

Now AI isn't guessing weather... it's fetching it.

CODE

```python
import requests

@mcp.tool()
def get_weather(location: str):
    url = f"https://api.weather.com/{location}"
    response = requests.get(url)
    return response.json()
```

5 Run the Server

Run using SSE (Server-Sent Events)

The server listens to AI requests and streams back results.

CODE

```python
if __name__ == "__main__":
    mcp.run(transport="sse")
```

6 Test Your Tools

Run from terminal → connect via an MCP-compatible client

Run from terminal → connect via an MCP-compatible client → tools appear → call them with args.

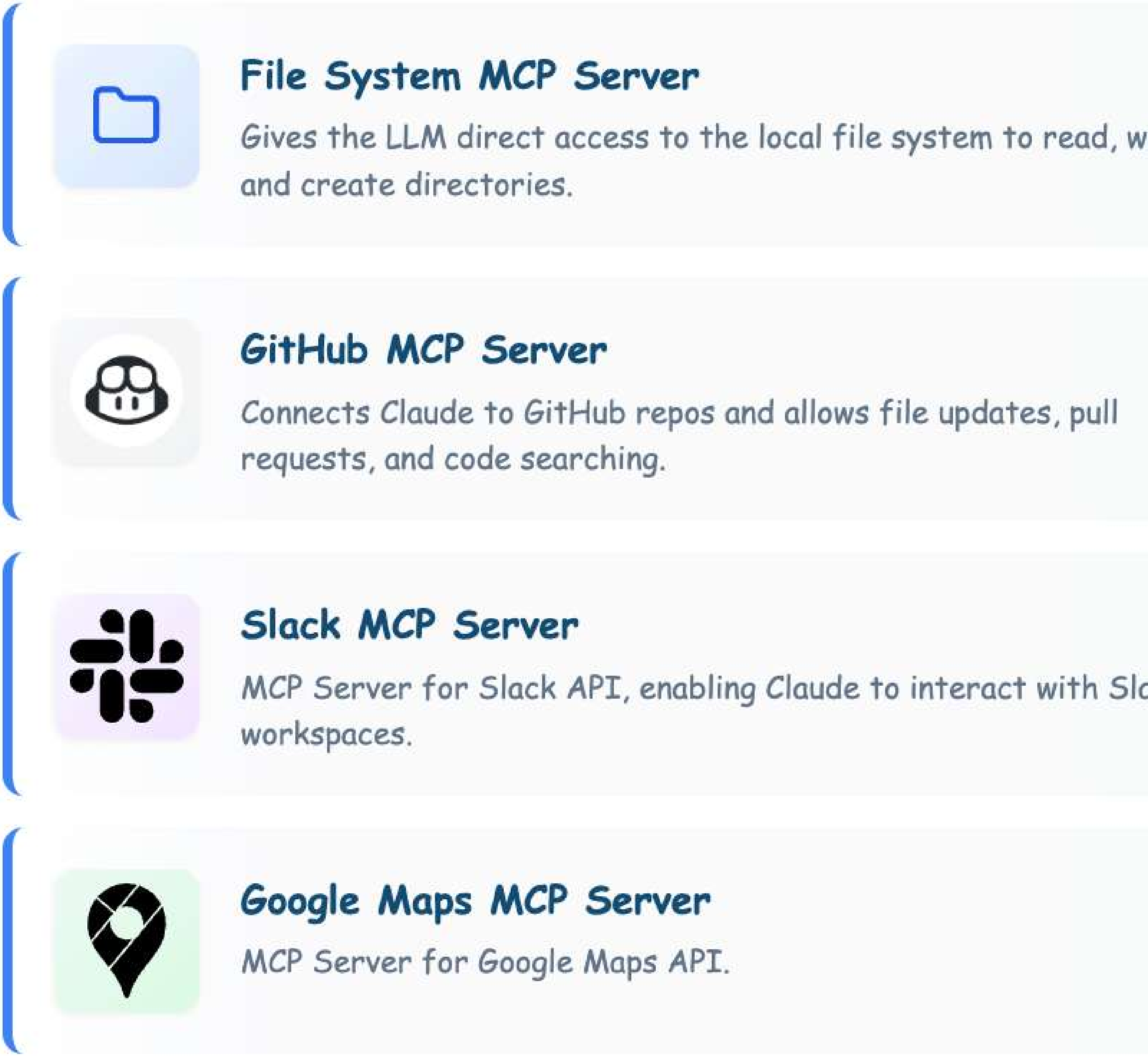
CODE

Popular MCP Servers You Can Use

Connect your AI to files, APIs, databases, a
more

Let's explore! 🚀

Popular MCP Servers



File System MCP Server

Gives the LLM direct access to the local file system to read, w

and create directories.

GitHub MCP Server

Connects Claude to GitHub repos and allows file updates, pull requests, and code searching.

Slack MCP Server

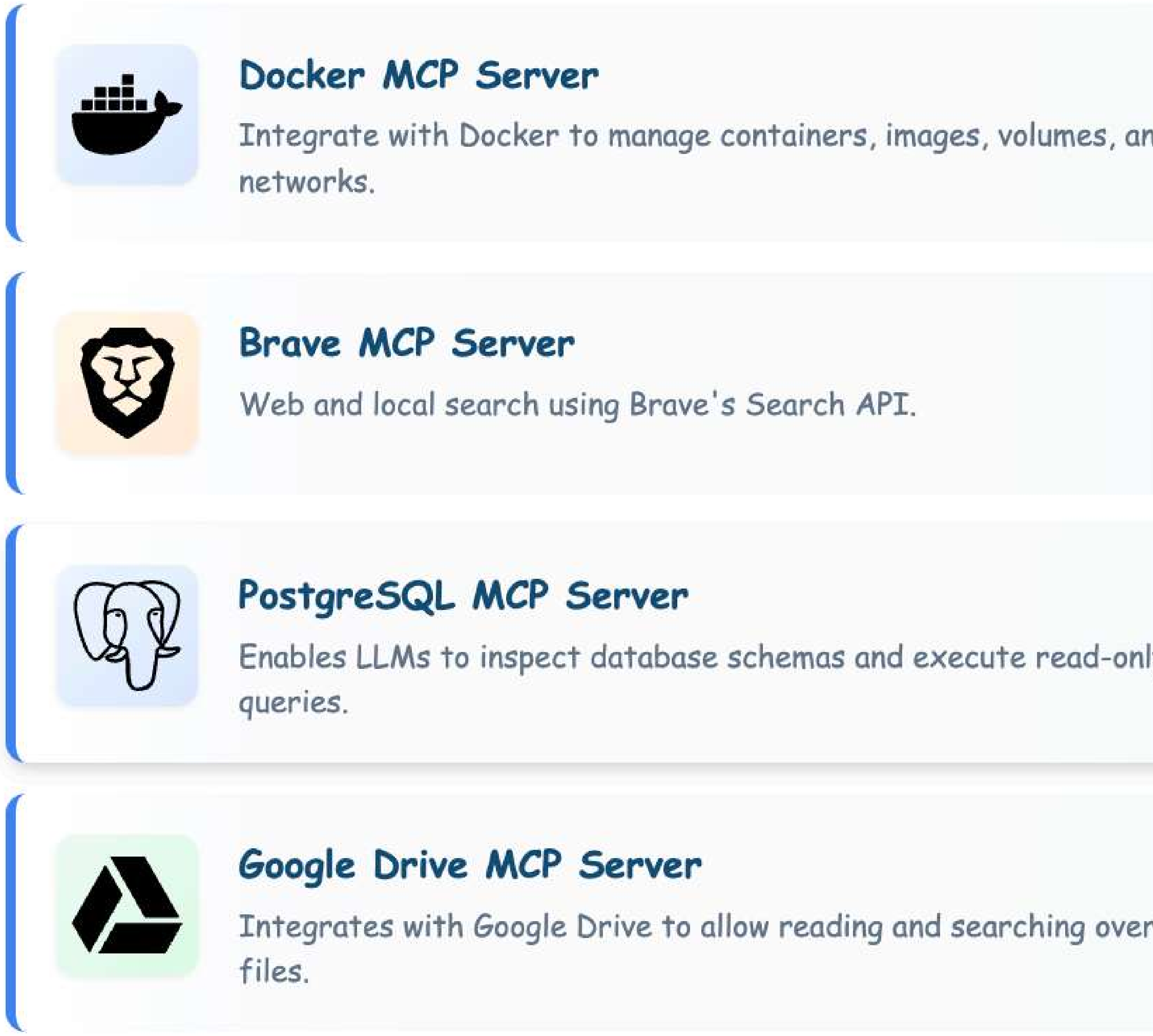
MCP Server for Slack API, enabling Claude to interact with Sl

workspaces.

Google Maps MCP Server

MCP Server for Google Maps API.

Popular MCP Servers



Docker MCP Server

Integrate with Docker to manage containers, images, volumes, an networks.

Brave MCP Server

Web and local search using Brave's Search API.

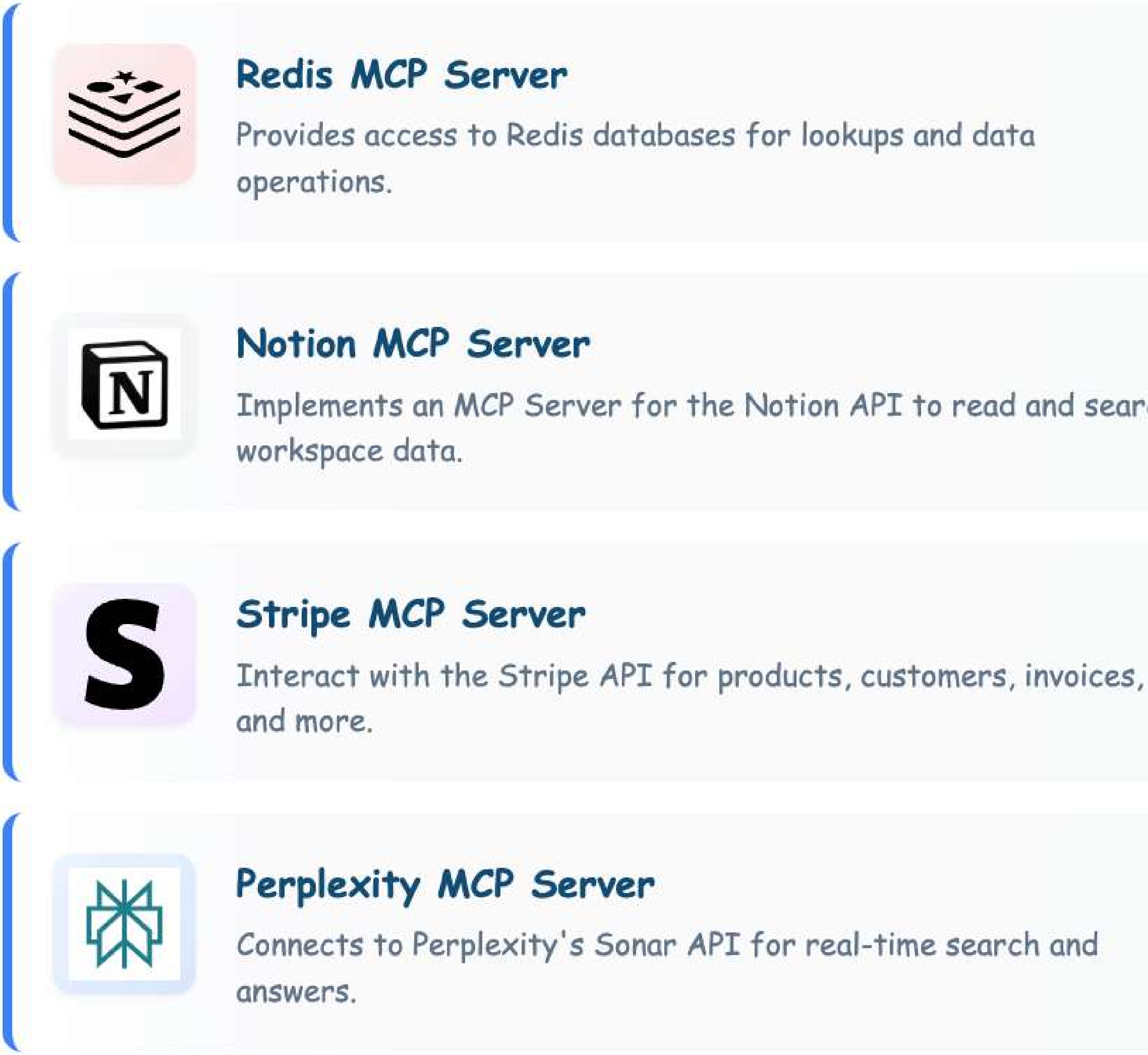
PostgreSQL MCP Server

Enables LLMs to inspect database schemas and execute read-onl queries.

Google Drive MCP Server

Integrates with Google Drive to allow reading and searching over files.

Popular MCP Servers



Redis MCP Server

Provides access to Redis databases for lookups and data operations.

Notion MCP Server

Implements an MCP Server for the Notion API to read and sear workspace data.

Stripe MCP Server

Interact with the Stripe API for products, customers, invoices, and more.

Perplexity MCP Server

Connects to Perplexity's Sonar API for real-time search and answers.