## **🔌 What is MCP?**

* **MCP (Model Context Protocol)** is an **open protocol** that standardizes how applications provide **context to LLMs**.
* Think of it like **USB-C** for AI: a universal port to connect LLMs to tools and data.

## **🤖 Why MCP?**

* 🧩 **Plug & Play Integrations**: Use pre-built tools your LLM can connect to immediately.
* 🔁 **LLM Agnostic**: Switch between models/providers (Claude, GPT, etc.) easily.
* 🔐 **Secure by Design**: Keep data within your infrastructure, follow best practices for security.
* 🧠 **Agent-Ready**: Ideal for building multi-step agents and complex workflows.

## **🧱 Architecture Overview**

* **MCP follows a client-server model**:  
  + **MCP Host**: Tools like Claude Desktop, IDEs, or AI apps that want to access external context.
  + **MCP Client**: Maintains 1:1 protocol connections with servers.
  + **MCP Server**: Lightweight program exposing one or more capabilities through MCP.

## **🗂️ Server Capabilities**

* 🔍 Connects to **Local Data Sources** (files, databases)
* 🌐 Connects to **Remote Services** (web APIs, cloud tools)
* 🧩 Each server can be swapped or added like a module – enabling scalable, composable workflows.