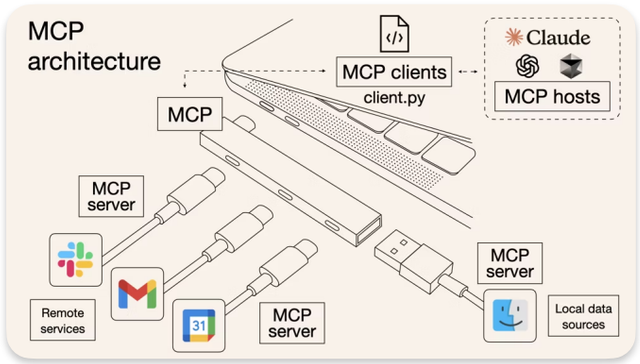
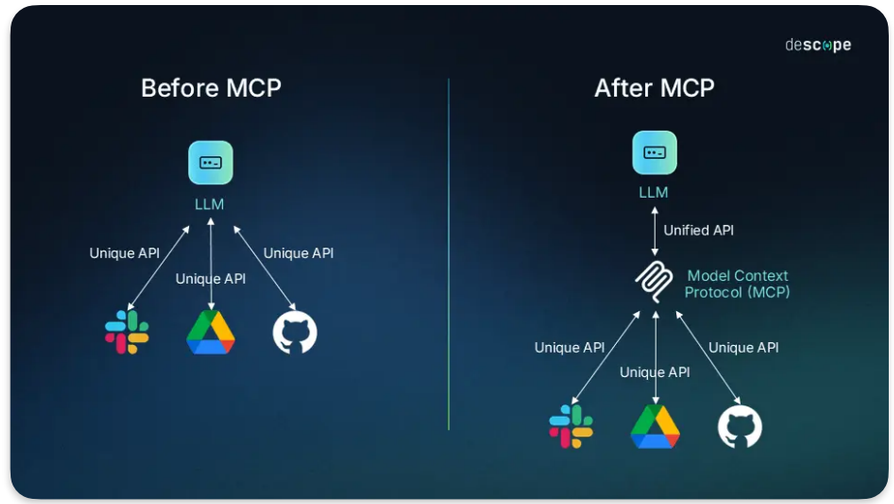


📌 What is MCP?

MCP (Model Context Protocol) is an **open protocol** that allows LLMs to connect to external data and tools in a standardized, safe way.
Instead of the LLM being "just a text predictor," MCP enables it to interact with:

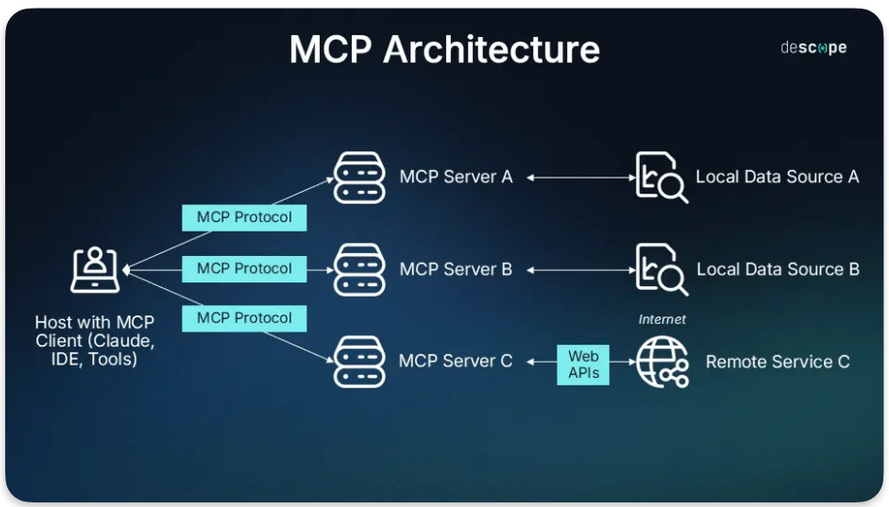
- **Databases**
- **File systems**
- **Web APIs**
- **Search engines**

and more — through a consistent interface.



📌 Why is MCP becoming popular?

1. **Standardization**
   - Until now, every project implemented LLM ↔ Tool integration differently.
   - MCP defines a common interface: "Here's how LLMs talk to tools."
2. **Reusability**
   - Example: once you build a `rag-mcp` server for PDF search, you can reuse it in Claude, Cursor, LangChain, etc.
   - One tool → multiple clients.
3. **Security & Isolation**
   - MCP servers run as isolated processes.
   - The LLM can only access external resources through defined MCP tools, preventing unrestricted file or system access.
4. **Extensibility**
   - Anything can be exposed as an MCP server: weather APIs, DB queries, Slack messages.
   - LLM clients automatically detect and surface them in the UI.
5. **Ecosystem Growth**
   - Big players like Anthropic (Claude), Cursor, and even OpenAI (experimental) are supporting MCP.
   - It's quickly becoming the "plugin standard" for connecting LLMs with external tools.



👉 In short: **MCP is a common language for connecting LLMs to the outside world safely and flexibly**, which is why it's gaining so much traction in the developer ecosystem