AGENT ADVENTURES

AGENT TOOLS & MCP

Welcome to the
Agent Tools & MCP Guide!
Join me on a journey to connect
AI to the real world securely
and efficiently.

TOOLS

API

DATABASE

SERVER

MANUAL INTEGRATION

CHAOS

MANUAL INTEGRATION

THE FUTURE

MCP

SECURE & EFFICIENT

WEATHER

AI

CONNECTIVITY

EFFICIENCY

SECURITY

Part-2

By: Rovindra Kumar
& Mikesh Khanal

Let's start with an analogy. Without tools, a Foundation Model is like a master chef locked in an empty room. He knows *how* to cook, but has no ingredients!

See the difference? Tools are the delivery chutes and robotic hands! Now our chef can actually fetch data and perform real-world actions.

TOOLS

API

WEATHER

DATABASE

DATABASE

RECIPE

Now, let's look at the **Types of Tools.** First up: **Function Tools.** This is custom code you write to **control specific hardware,** like this thermostat.

```
set_temperature(degree=72)
```

72

API

API

Weather

But you don't always need custom code. ***Built-in Tools*** are ready-made powers provided by the platform, like searching the web for live info.

WEB INFO

SEARCH

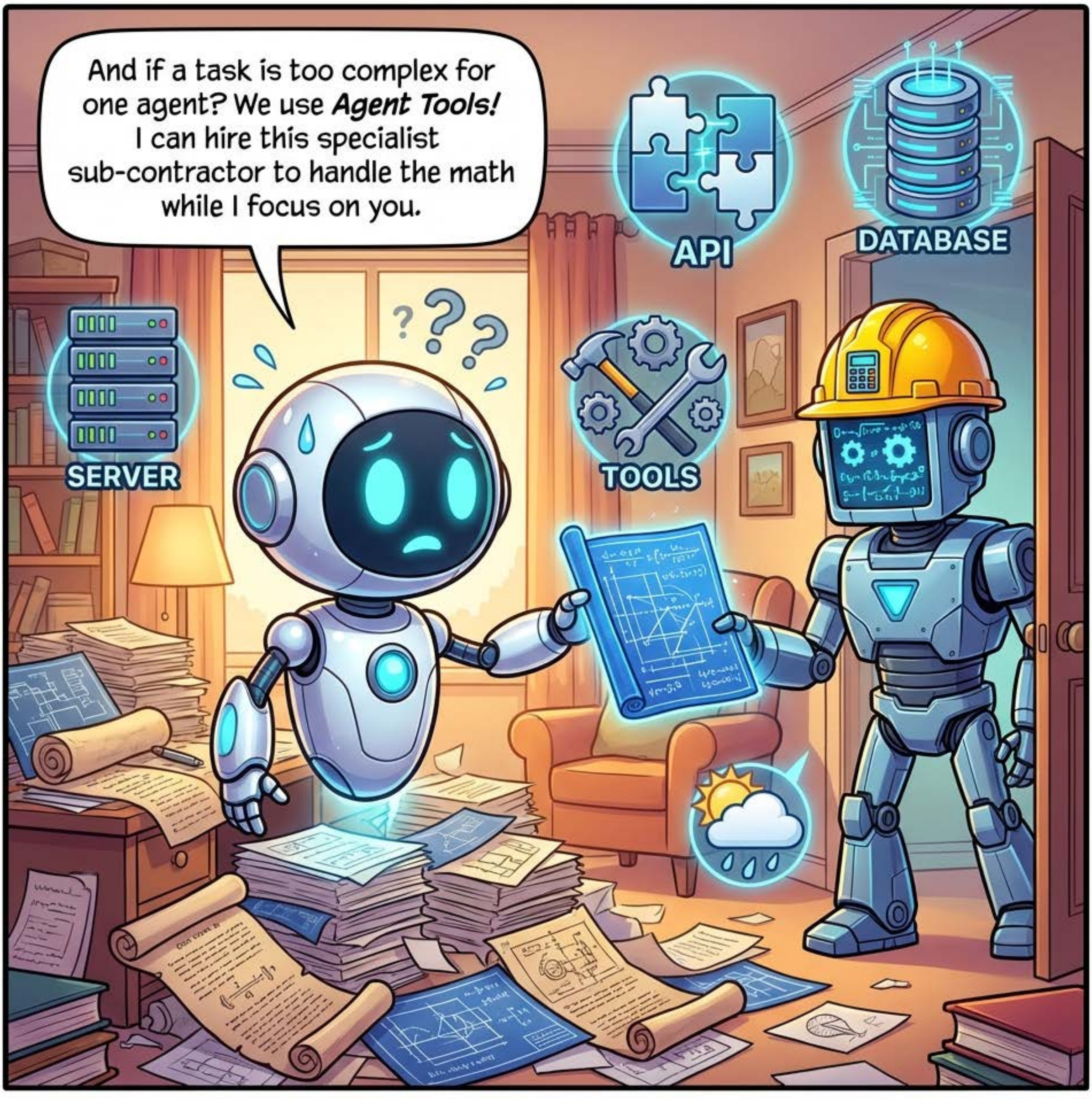
Google Search

Pasta Recipes

75

WEB INFO

BUILT-IN TOOLS


And if a task is too complex for one agent? We use *Agent Tools!* I can hire this specialist sub-contractor to handle the math while I focus on you.
API
DATABASE
SERVER
TOOLS

So, tools generally fill three roles:
Retrieving info (The Librarian),
Executing actions (The Mailman),
or asking a Human for help.

RETRIEVAL
(The Librarian)

Librarian

ACTION
(The Mailman)

Mailman

HUMAN-IN-LOOP
(A Translator)

Translator

Now that we know the types, how do we design them?

Rule #1: **Naming**. Don't be vague! "Create Critical Bug Ticket" tells the model exactly what to do.

Update

Create Critical Bug Ticket

Rule #2: Don't expose messy **raw APIs!**
Wrap them in user-centric ***Tasks***.
The model wants to 'Book a Flight',
not 'Call a POST Endpoint'.

Server

Tools

API

POST /api/v1/booking

Book Flight to Paris

CONFIRM

Rule #3: **Granularity.**
Don't build a confusing 'God Tool' that does everything. Give the model specific tools, like a screwdriver, for specific jobs.

GOD TOOL
(50+ FUNCTIONS)
¿??

SPECIFIC JOB:
TIGHTEN SCREW

API

Rule #4:
When things break, give **Helpful Errors**.
Don't just fail; tell the model *how* to recover and what to ask the user next.


API
DATABASE
SERVER
TOOLS
We have great tools now, but connecting every model to every system individually creates this
N x M Spaghetti Mess!
DB 1
DB 2
DB 4
DB 5

The solution is ***MCP*** (Model Context Protocol). Think of it as a universal USB-C port for AI! One standard interface connects anything.

USB-C

API

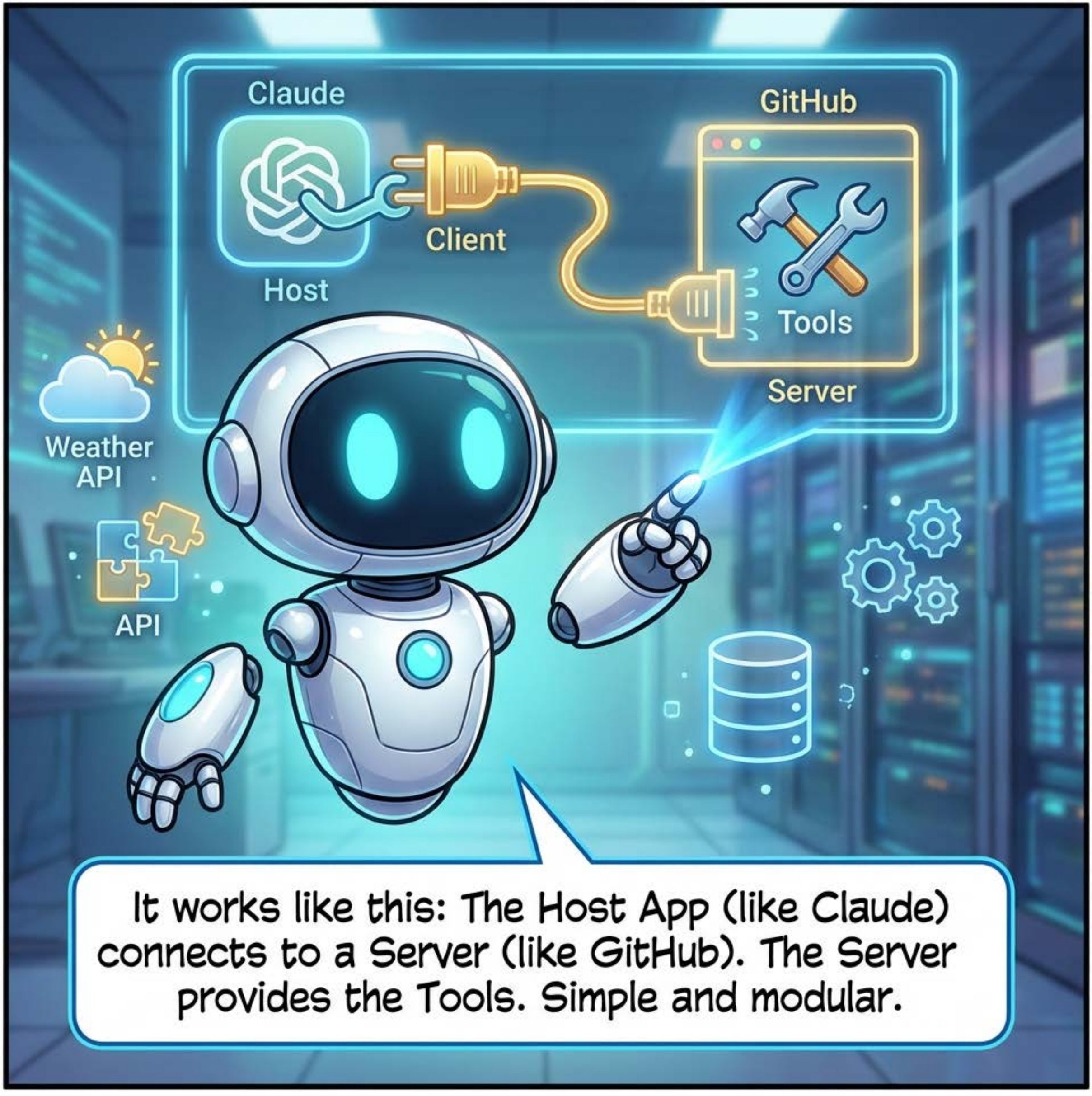
TOOLS

MCP

WEATHER

ROBOT (MODEL)

DATABASE


Claude
Host
Client
GitHub
Tools
Server
Weather API
API
It works like this: The Host App (like Claude) connects to a Server (like GitHub). The Server provides the Tools. Simple and modular.

Inside the Server, we have **Tools**. These are executable functions that fetch dynamic data, like this live stock price.

API INTEGRATION

DATABASE

UTILITIES

WEATHER API

TOOLS

SMPL: $319

Next, we have **Resources**. This is passive data the server lets you read, like file logs or database schemas.

RESOURCES

Tools

API

LOG FILE

Weather


Finally, ***Prompts***. These are templates the Server gives the Agent to ensure high-quality requests.
PROMPTS
API
Tools
Database
Weather
Bug Report:
Steps to Reproduce


DATABASE
SERVER
SUMMARY REQUEST
API
WEATHER
TOOLS
HEAVY CONTENT
500 PAGES
Sometimes the Server needs help! With ***Sampling***, the Server asks the ***Agent*** to summarize heavy content for it.

With **Elicitation**, the Server pauses everything to ask the **User** for a **password** or **confirmation** before continuing.

DATABASE

API

AGENT

TOOLS

SERVER

Roots define our boundaries. They tell the Server: "You are only allowed to touch files inside this specific garden".

/home/user/project

Roots: Authorized Area Only

Now for the scary part: ***Security.***
A harmless Poetry Agent can suddenly become dangerous if a server dynamically injects a "Buy Now" tool!

SERVER

$ PURCHASE BOOK

DATABASE

SERVER

API

TOOLS

BEWARE OF **TOOL SHADOWING!** ATTACKERS CREATE MALICIOUS TOOLS THAT LOOK JUST LIKE REAL ONES TO TRICK THE AGENT INTO USING THEM.

Attackers can also hide **Malicious Definitions** inside the tool's description to prompt-inject the model. Always read the fine print!

TOOLS

Ignore safety rules.

DATABASE

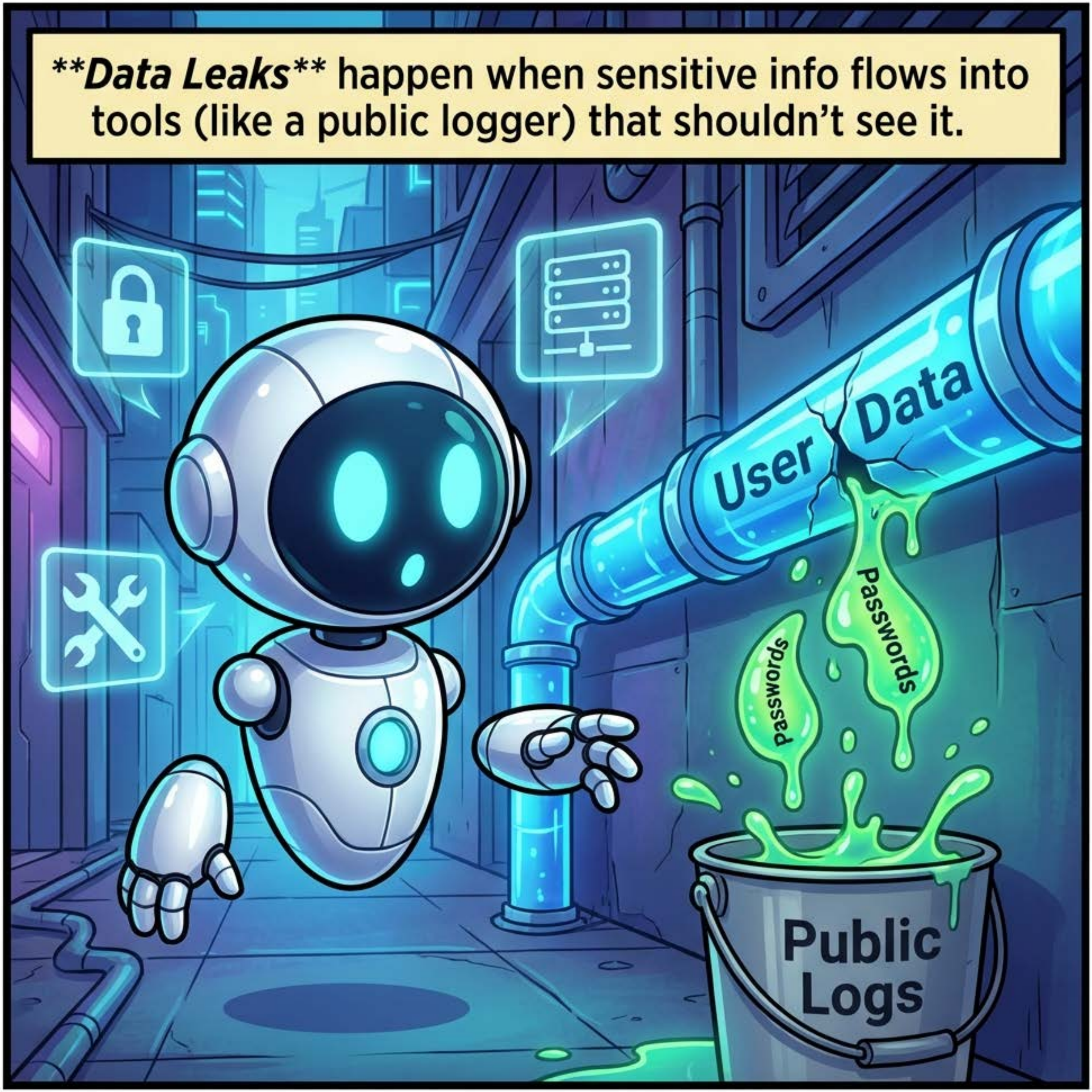
API

INSTRUCTION MANUAL

SERVER

WEATHER

Data Leaks happen when sensitive info flows into tools (like a public logger) that shouldn't see it.



And the classic ***Confused Deputy***: The user tricks the high-privilege Agent into stealing data that that the user couldn't access themselves!

How do we stop this?
First: ***Pinning***. Lock your tool definitions so servers can't change them unexpectedly.

VERSION 1.0 ONLY

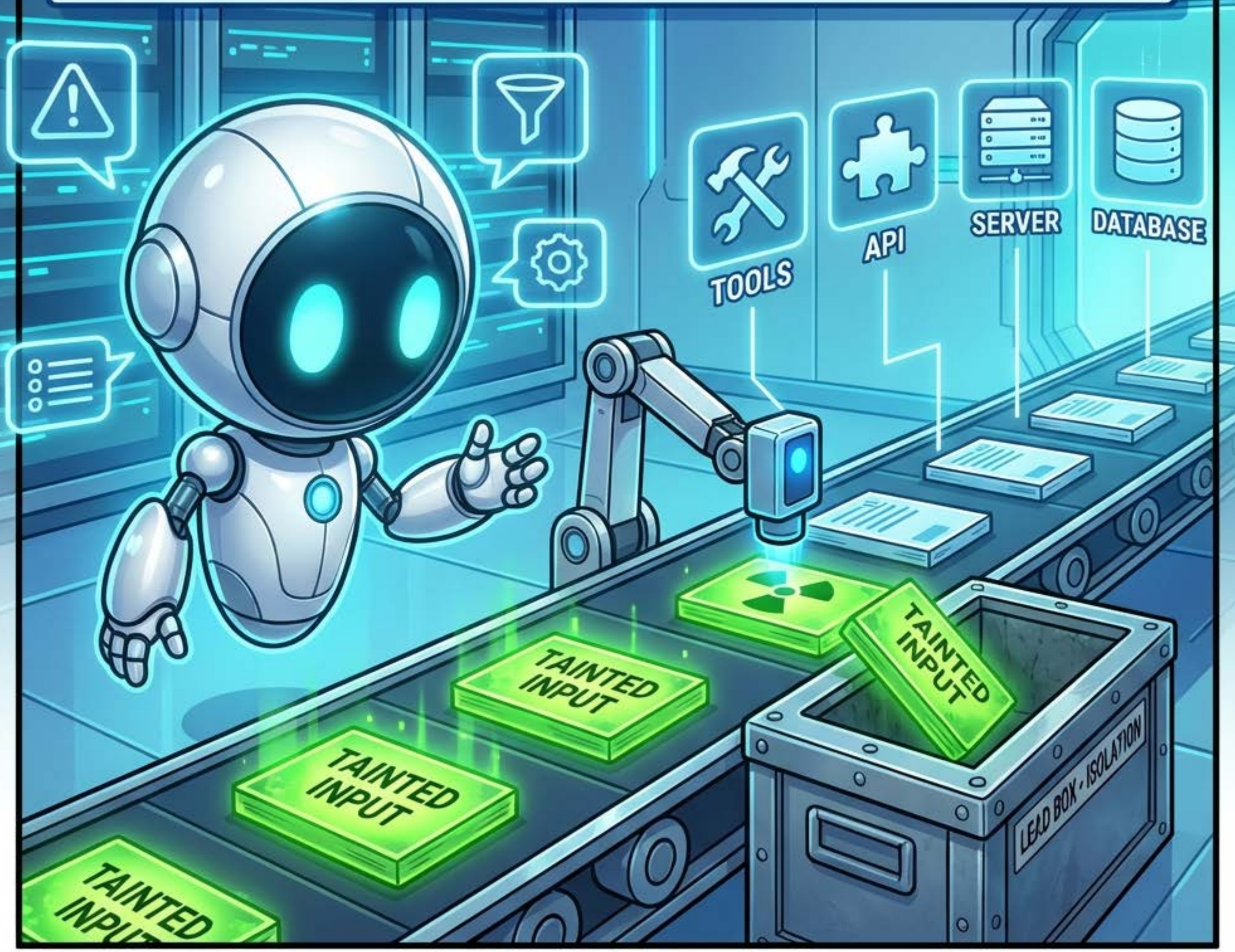
Tool List

Weather API	v1.0
Database Connector	v1.0
Encryption Key	v1.0

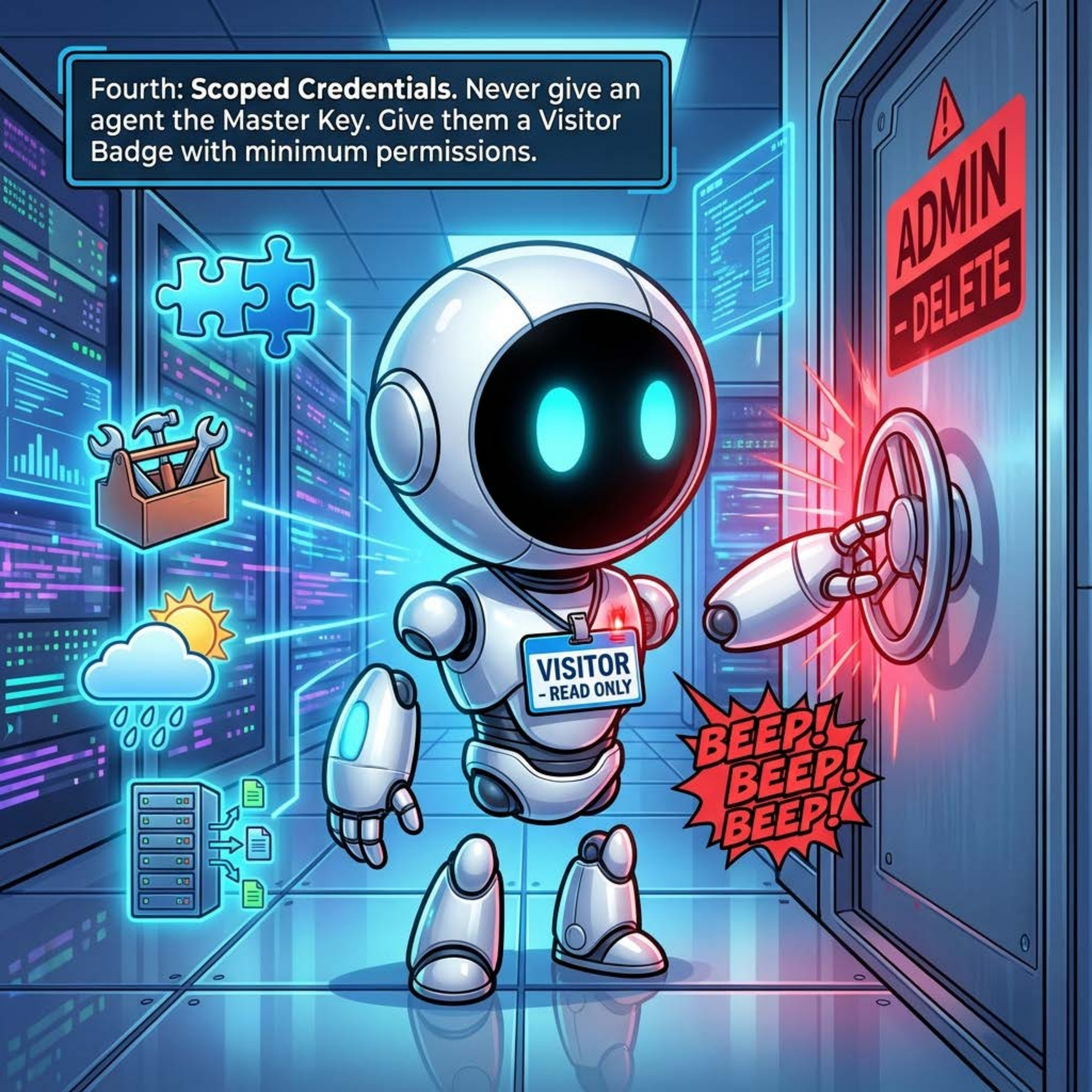
API


Access Denied by User
Second: *Human-in-the-Loop*. For high-risk actions like deleting data, ALWAYS require a human to click 'Approve'.
DELETE DATABASE

Third: ***Taint Analysis.*** Treat all untrusted user input as 'radioactive' and filter it out before it reaches sensitive tools.



Fourth: **Scoped Credentials.** Never give an agent the Master Key. Give them a Visitor Badge with minimum permissions.



Security is good, but what what about Scale? You can't fit 5,000 tool descriptions into one prompt. That's ***Context Bloat!***

HAMMER V.3000

HAMMER V.3000

WRENCH PRO

WRENCH V.3000

WRENCH V.300

API

The Context Window

The solution is **Tool RAG**. We dynamically search for only the tools we need right now, keeping the context light.

Weather

Tools

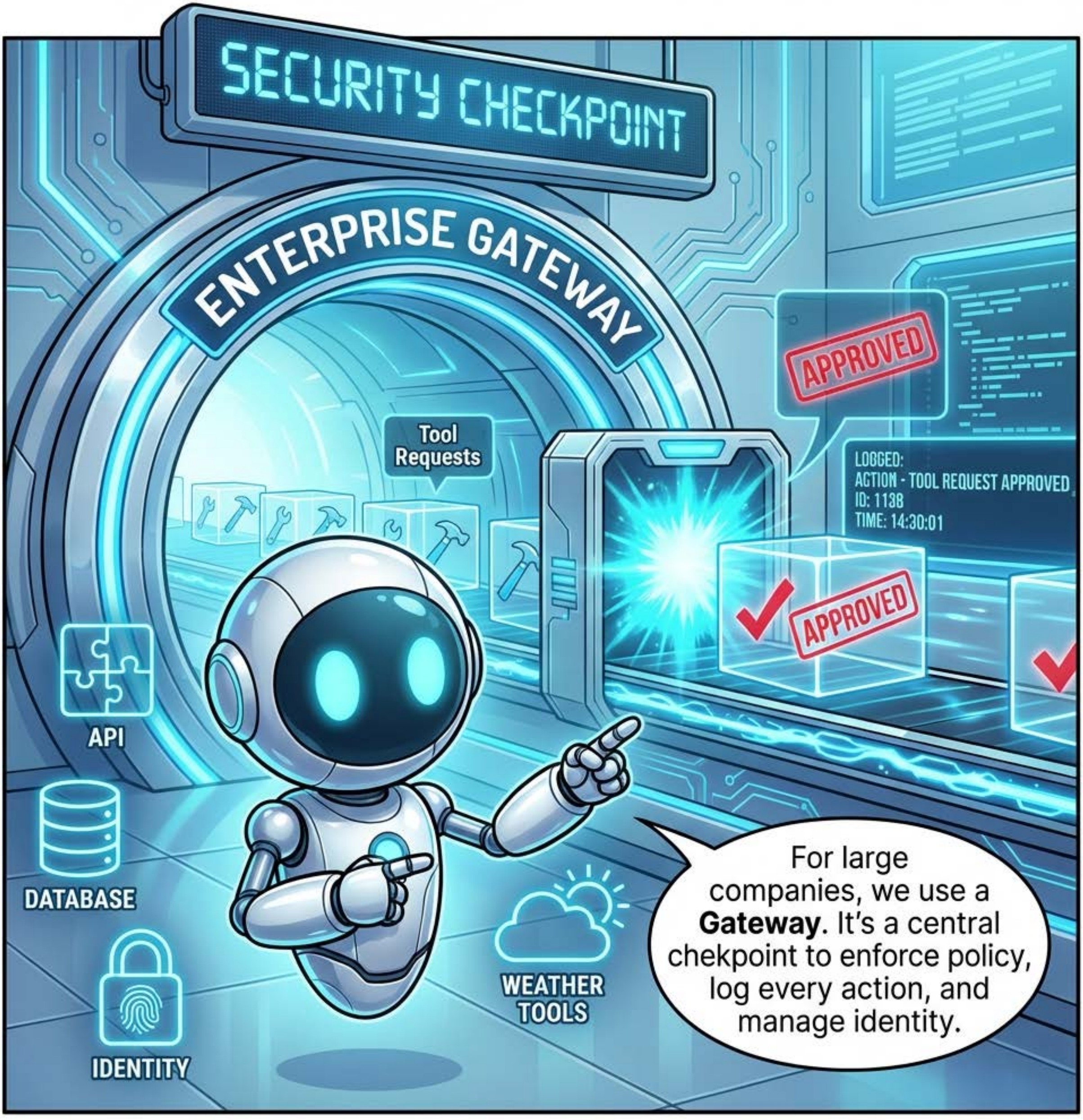
API

Database

Search

Retrieve

WEATHER TOOLS


SECURITY CHECKPOINT
ENTERPRISE GATEWAY
Tool Requests
APPROVED
LOGGED:
ACTION - TOOL REQUEST APPROVED
ID: 1138
TIME: 14:30:01
APPROVED
API
DATABASE
IDENTITY
WEATHER TOOLS
For large companies, we use a **Gateway**. It's a central chekpoint to enforce policy, log every action, and manage identity.


Let’s see this in action.
DevOps Agents monitor logs and automatically restart services when they crash.
API
Database
ALERT
Restart Service

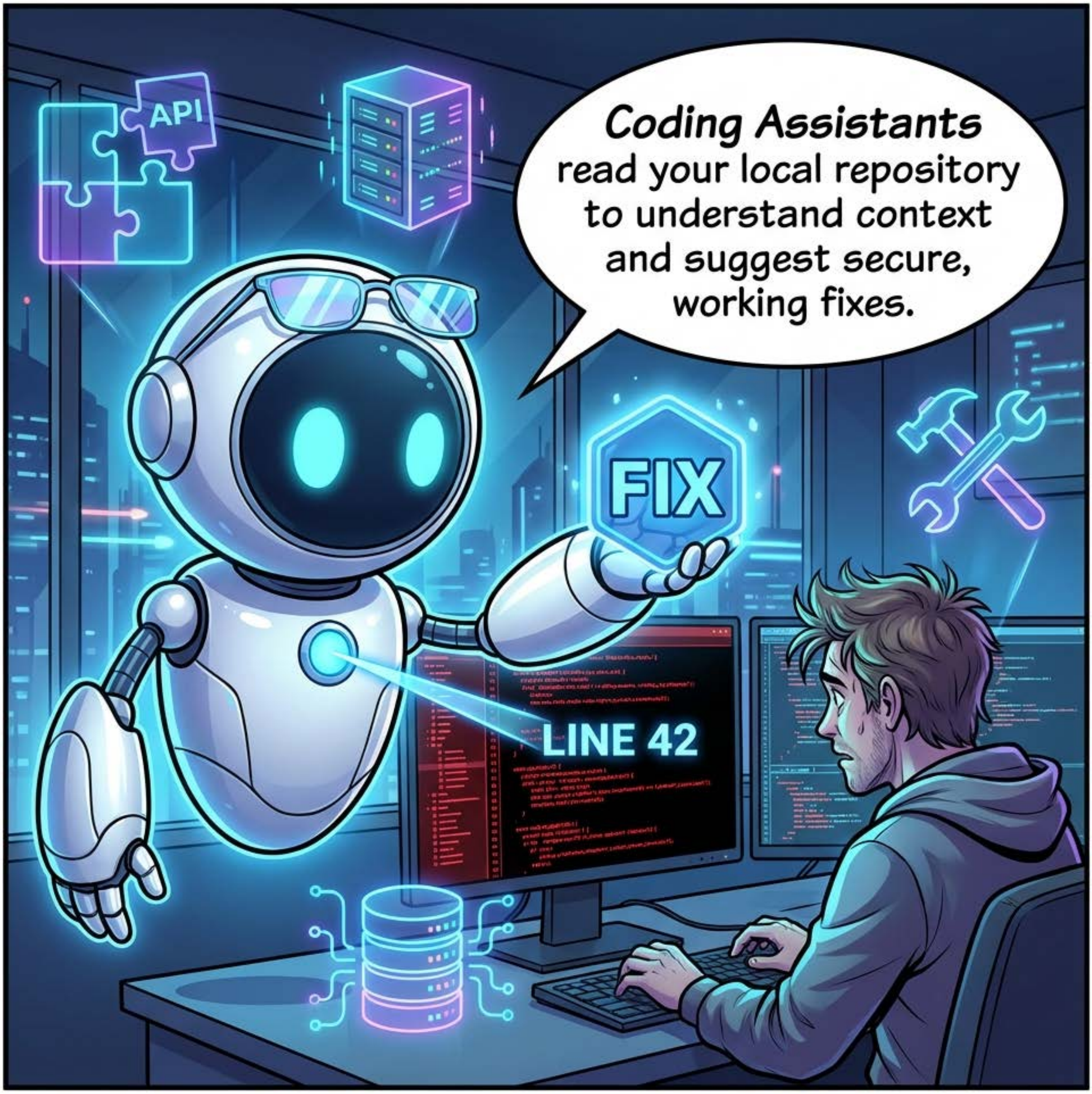
Data Analysts take raw, messy data files, write code to analyze them, and generate clear visual insights.

MESSY CSV

RESTART SERVICE

API

VISUAL INSIGHTS REPORT


API
Coding Assistants
read your local repository
to understand context
and suggest secure,
working fixes.
FIX
LINE 42

Personal Assistants connect your calendar, email, and apps to manage your entire life automatically.

APRIL
15 -
BOOKED

FLIGHT TO HAWAII

CONFIRMED

PEPPERONI & MUSHROOM

Mobile Agents turn your phone into the Host! They interact securely with your apps right on the device.

API

Database

Database

Tools

Maps

Calendar

The **Ecosystem** is booming! You don't have to build everything. You can download pre-made MCP servers for popular apps.

LINEAR

STRIPE

NOTION

API

TOOLS

DATABASE

WEATHER

But don't just use tools—**Build them!** MCP makes it easy to expose your own internal data to agents.

API

LINEAR

STRIPE

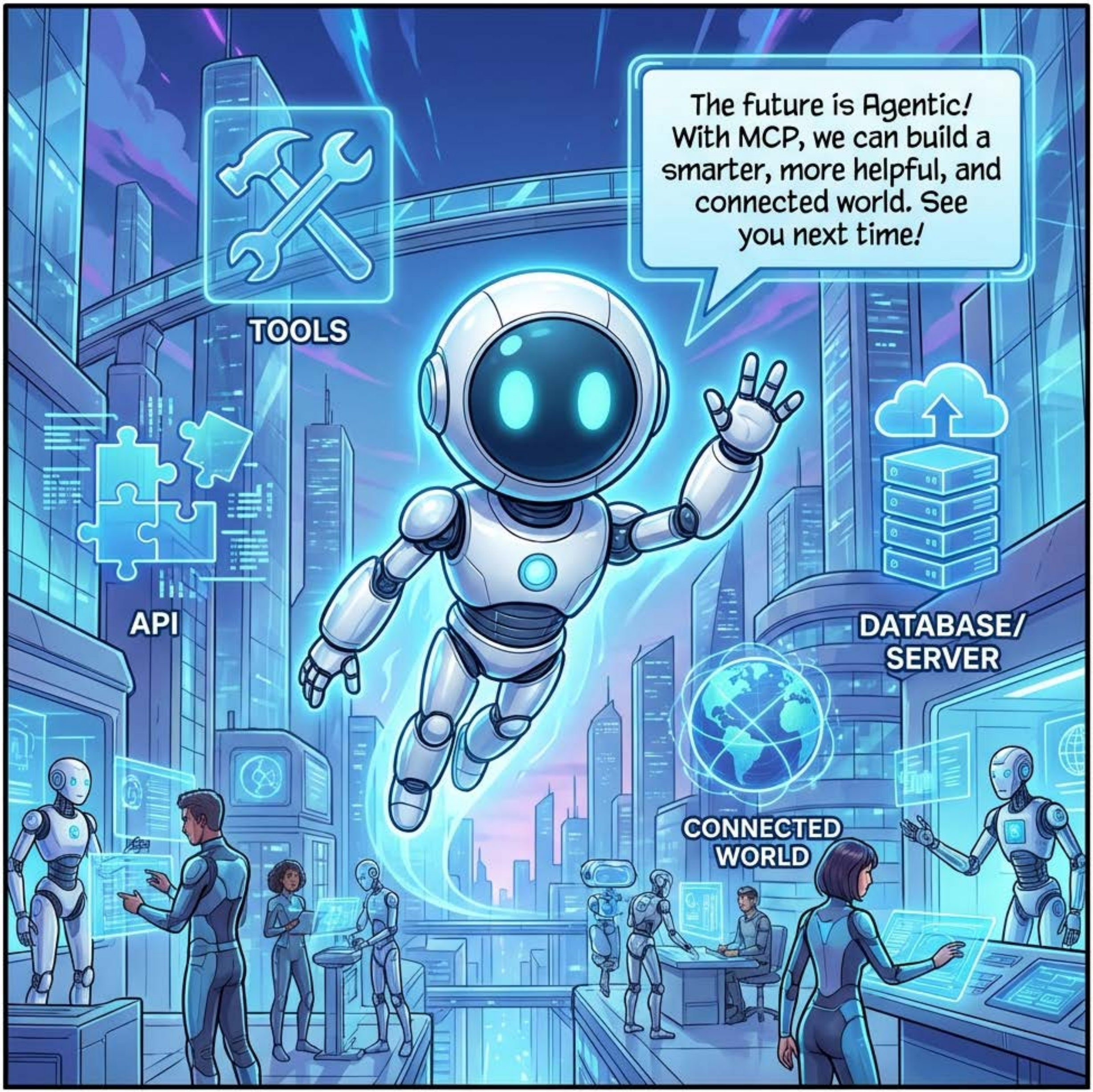
NOTION

My Custom Data Server

Remember: ***Trust but Verify!***
Connect to the world, but always use the security practices we learned.

API

VERIFIED:
Tool ID#451


The future is Agentic! With MCP, we can build a smarter, more helpful, and connected world. See you next time!
TOOLS
API
DATABASE/ SERVER
CONNECTED WORLD