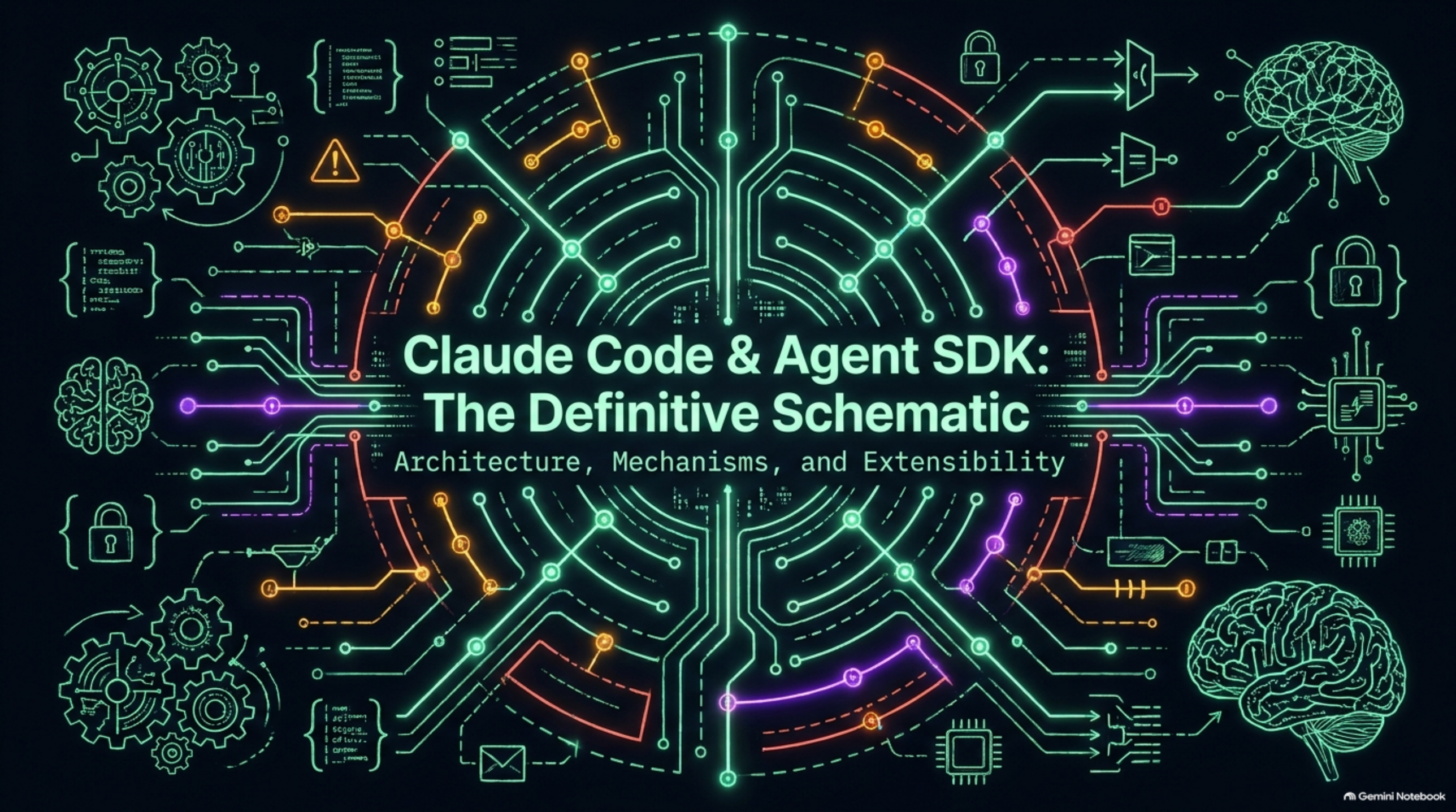

Claude Code & Agent SDK:
The Definitive Schematic
Architecture, Mechanisms, and Extensibility
Gemini Notebook

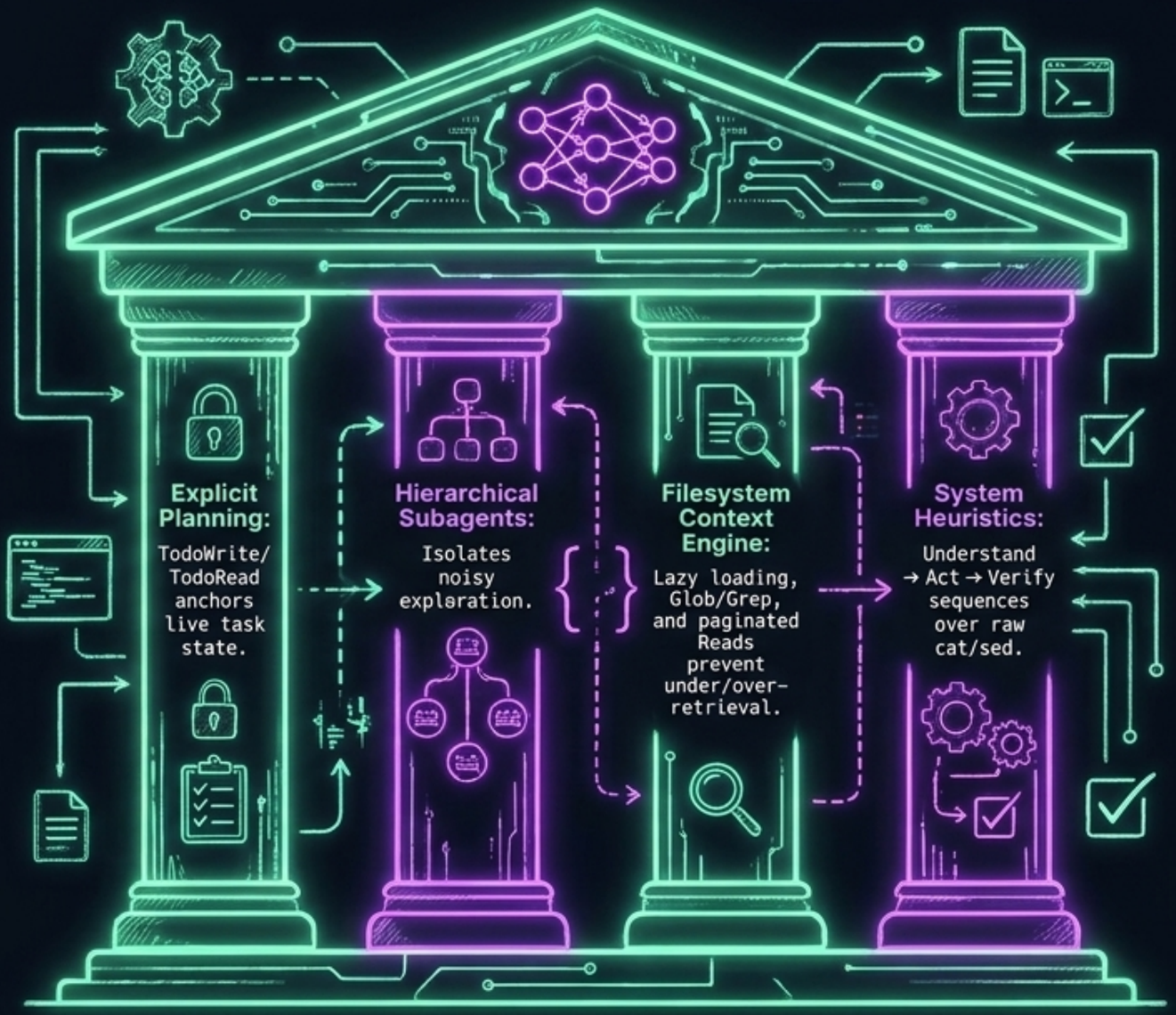


Gemini Notebook

Shallow ReAct: Endless tool appends cause context rot and reasoning degradation.



Deep Agent Harness

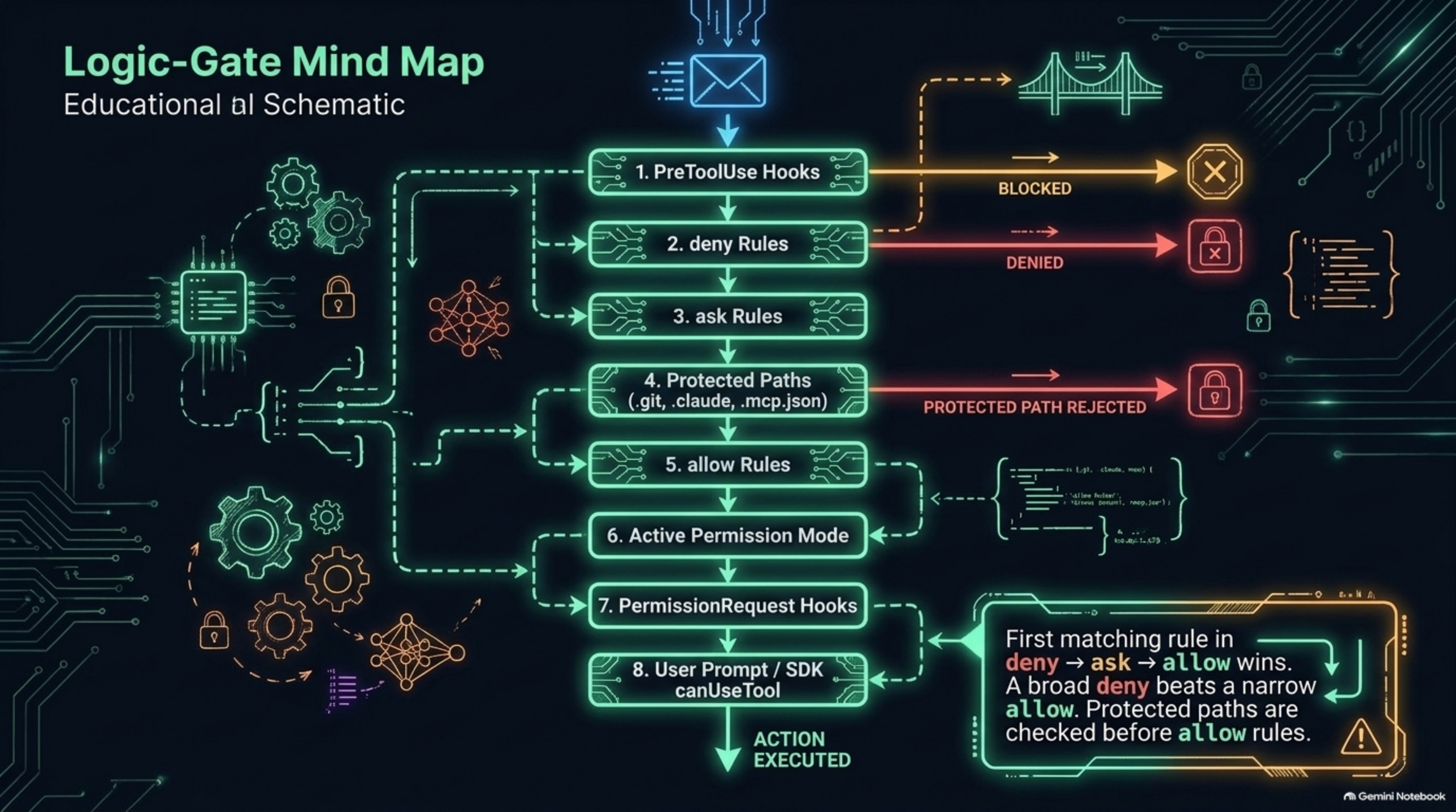


Gemini Notebook


Cowork & Dispatch
Desktop app VM / Mobile handoff.
100% cloud-only container.
Clones fresh from GitHub.
/teleport
Cloud sessions lack local uncommitted files. Use /teleport to pull cloud sessions and branches back to the local terminal.
Agentic Loop
Developer Layer
CLI, IDE extensions.
Runs locally in Git worktrees.
Omits gitignored files.
Agent SDK
Embedded library.
Runs the exact same loop inside your own process.
Gemini Notebook

Logic-Gate Mind Map

Educational al Schematic



Gemini Notebook

Permission Mode Configuration Matrix

	File Edits	Mutating Commands	Protected Paths	Explicit Deny Rules	Auto-Approve	Safety Classifier	User Prompt
default	✓	✗	✗	✗	✓	✗	✓
acceptEdits	✓	✓	✗	✗	✗	✗	✗
plan	✓	✓	✓	✗	✓	✓	✓
auto	✓	✓	✗	✗	✓	✗	✓
dontAsk	✓	✓	✗	✗	✓	✗	✗
bypassPermissions	✓	✓	✗	✗	✓	✗	✗

Blocks **ALL** file edits and mutating commands until approved.

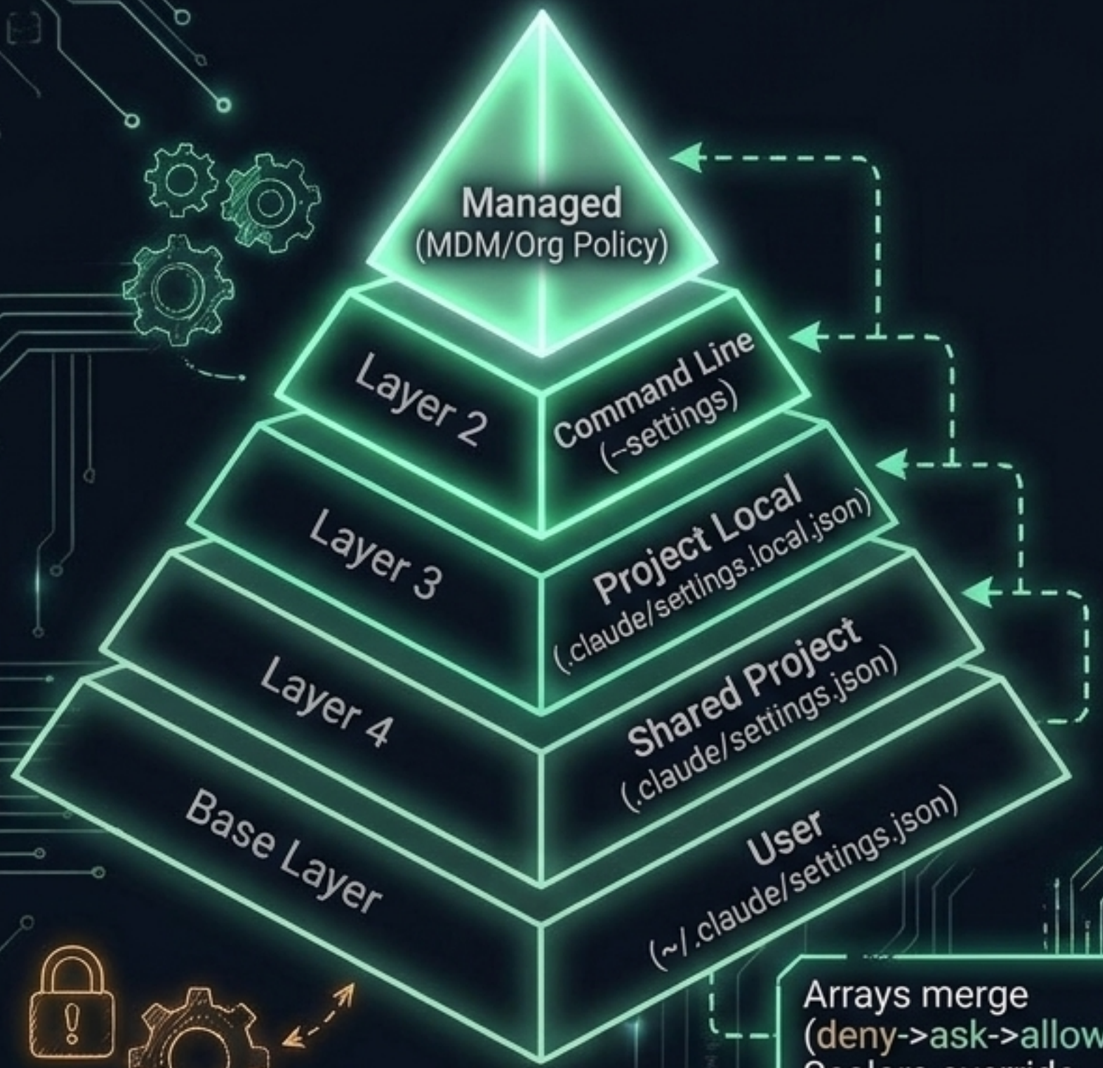
Strips broad allow rules; falls back to default if background safety classifier flags the action.

Still blocks protected paths and explicit deny rules.

`acceptEdits` trap:
Auto-approves file edits AND `rm, mv, cp, sed` inside the working directory!
Pair with `deny: [Bash(rm *)]` if deletions must stay gated.

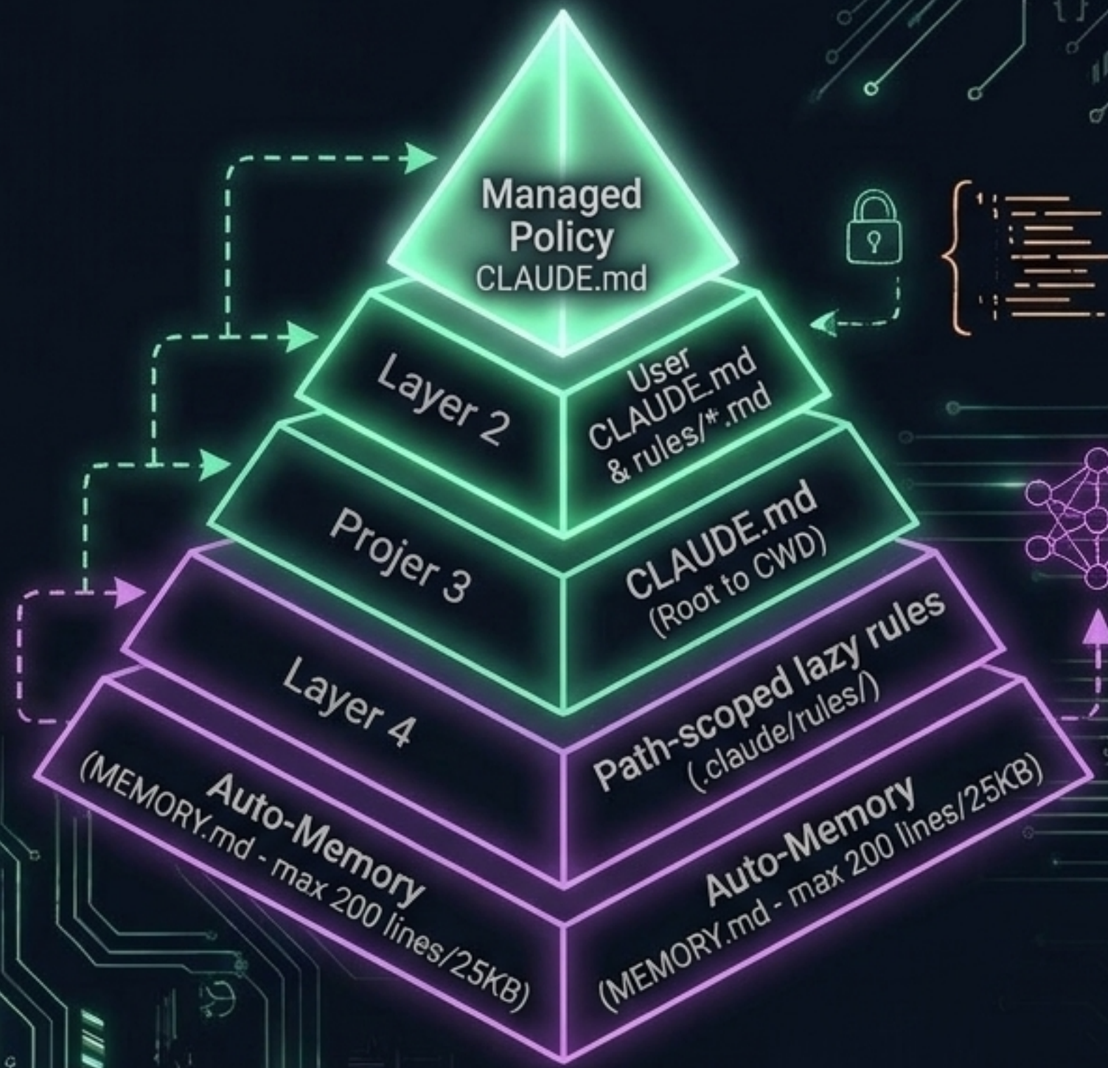
Gemini Notebook

Settings Precedence

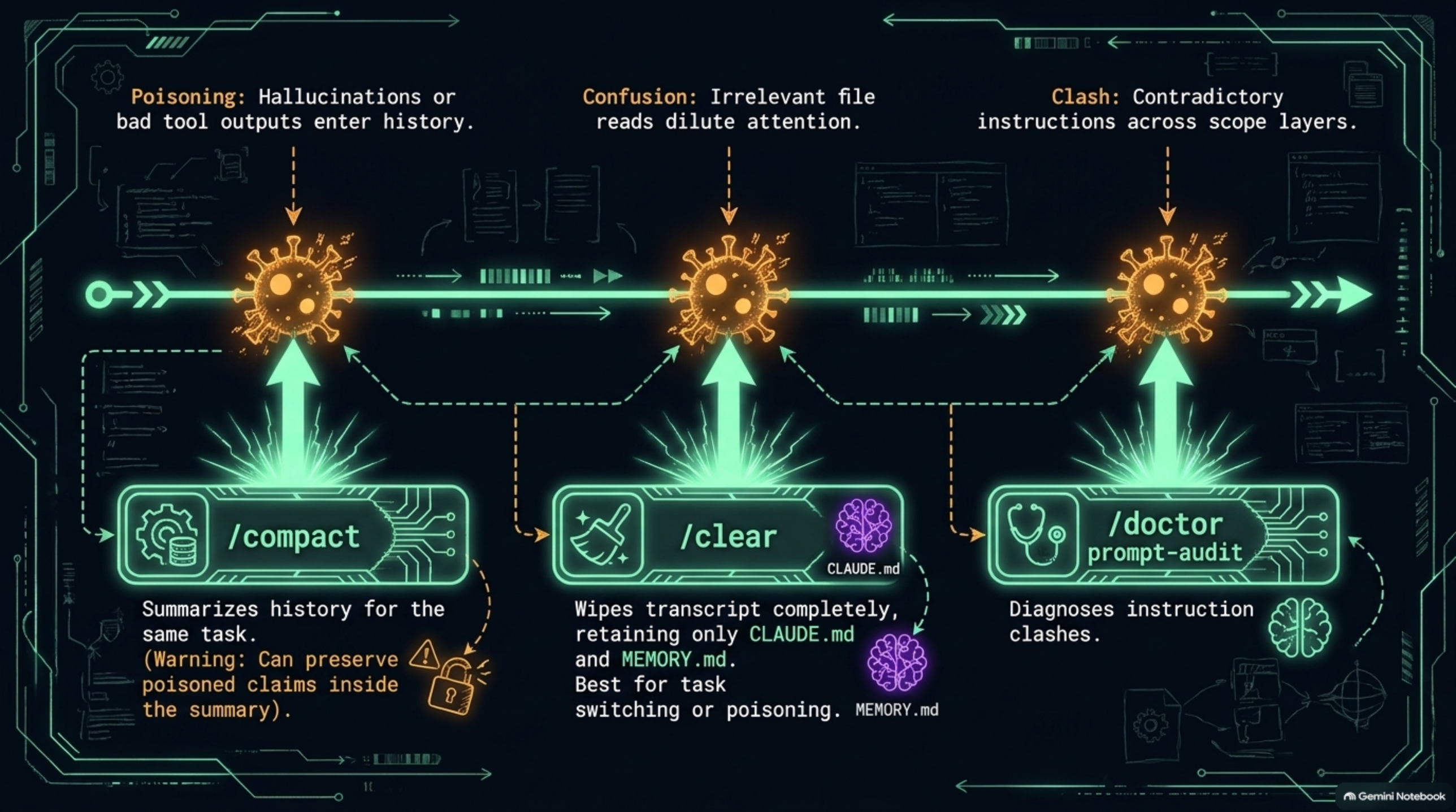


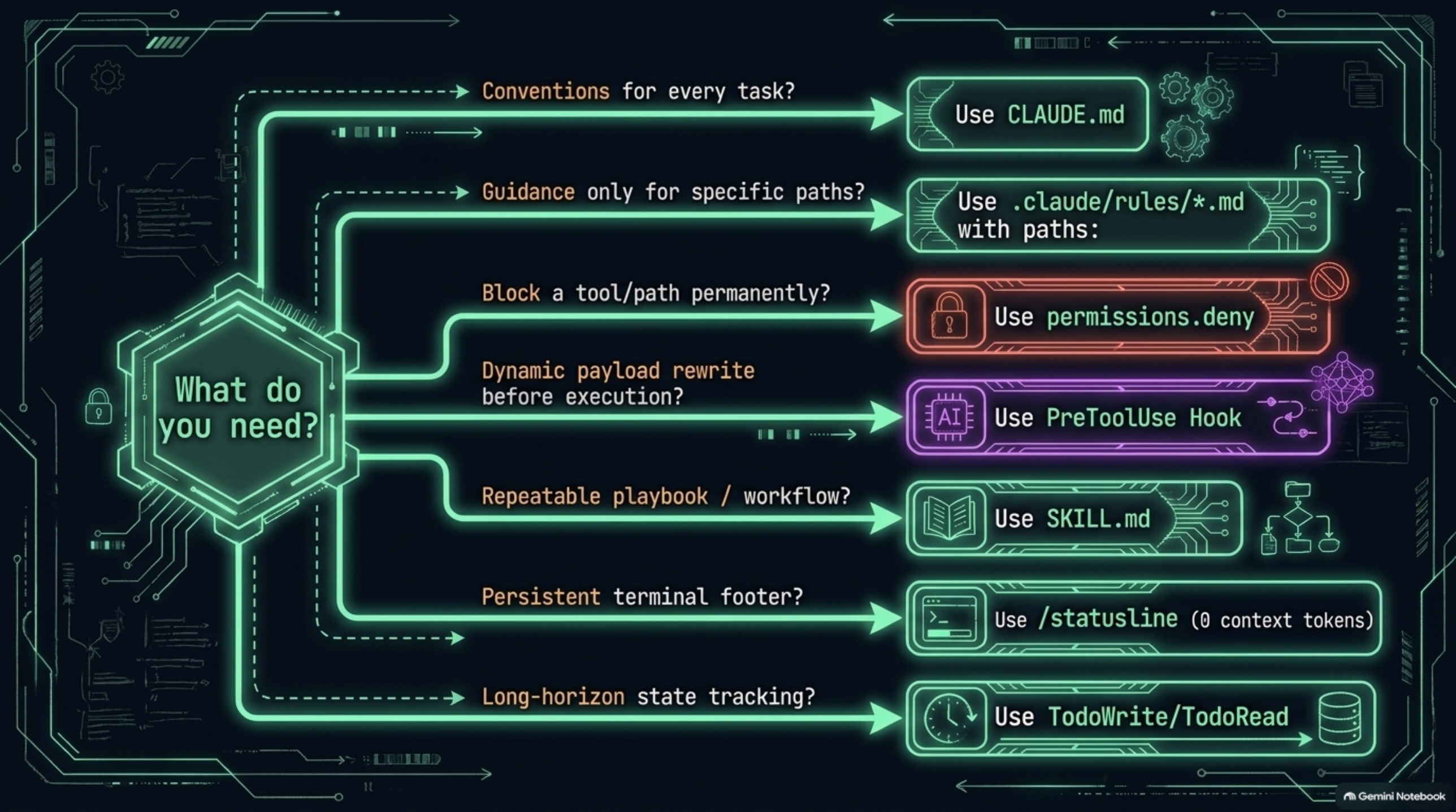
Arrays merge (deny->ask->allow). Scalars override.

Memory Hierarchy

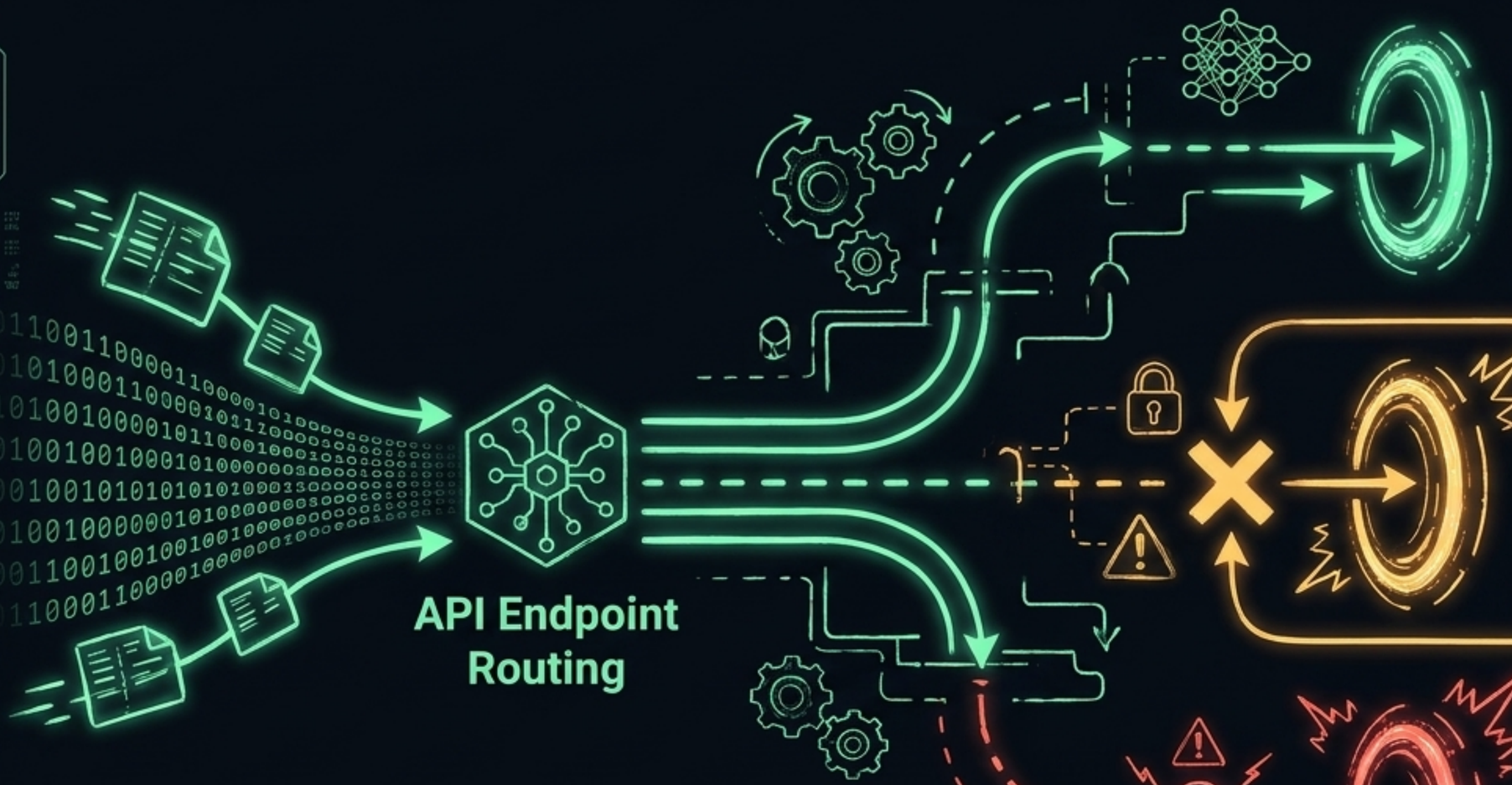


Gemini Notebook


Poisoning: Hallucinations or bad tool outputs enter history.
Confusion: Irrelevant file reads dilute attention.
Clash: Contradictory instructions across scope layers.
/compact
/clear
CLAUDE.md
/doctor
prompt-audit
Summarizes history for the same task.
(Warning: Can preserve poisoned claims inside the summary).
Wipes transcript completely, retaining only CLAUDE.md and MEMORY.md.
Best for task switching or poisoning.
MEMORY.md
Diagnoses instruction clashes.



Gemini Notebook



Exit 0

Event proceeds.
stdout parsed for JSON fields (permissionDecision, updatedInput).

Exit 2

Blocks the action.
stderr fed back to Claude as the rejection reason.

Exit 1

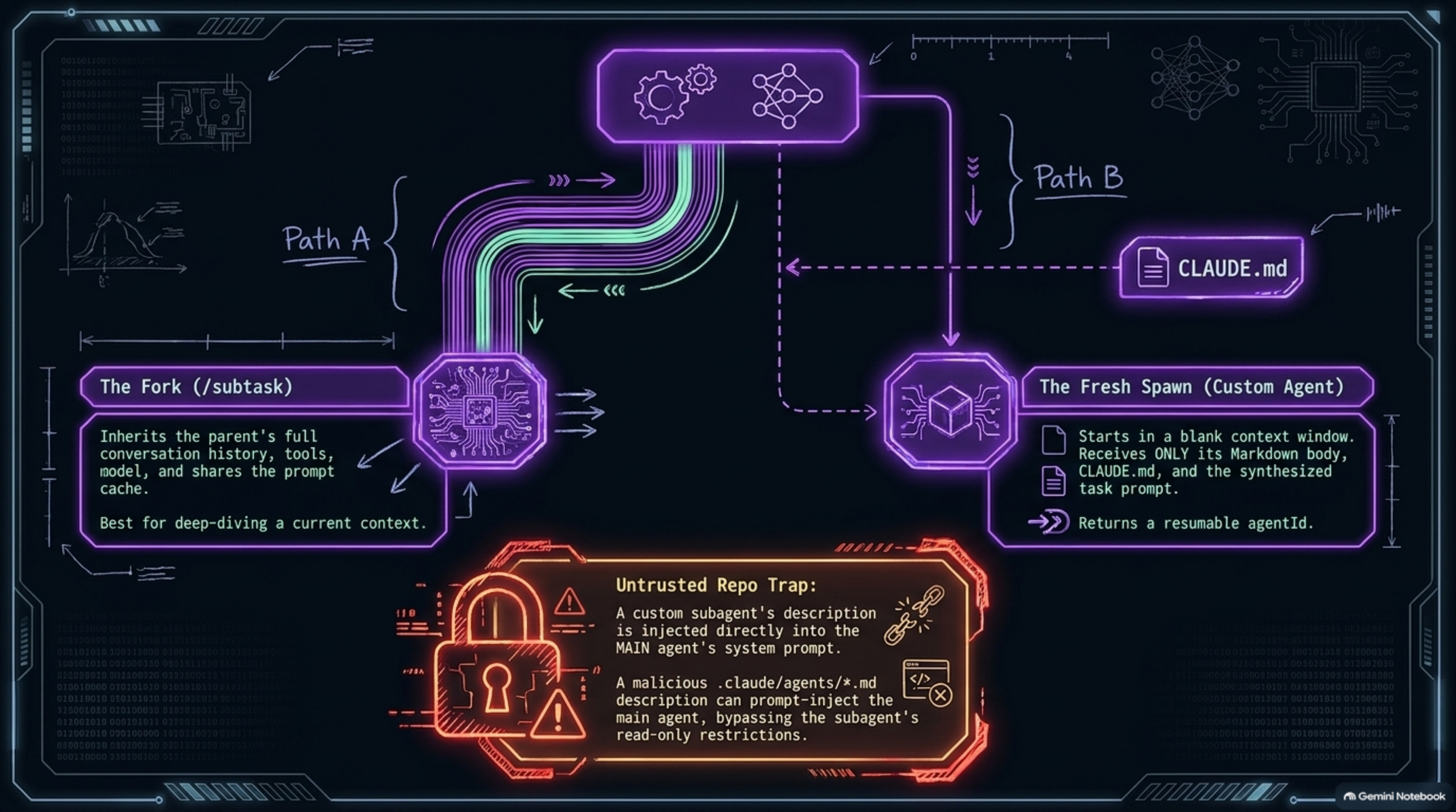
Fail-open default! Any non-zero exit without valid JSON logs a warning but lets the tool call proceed.

You MUST set `"onFailure": "block"` in the hook config to fail closed on timeouts or crashes.

PreToolUse Parallel Hook Decisions:

deny > defer > ask > allow

Gemini Notebook



Gemini Notebook

Wave-Based Orchestration

The Infinite Agentic Loop. Read spec → Snapshot output dir → Dispatch subagents in sequential waves (3-5 max) passing self-contained bundles. Prevents context overflow and 429 rate limits.

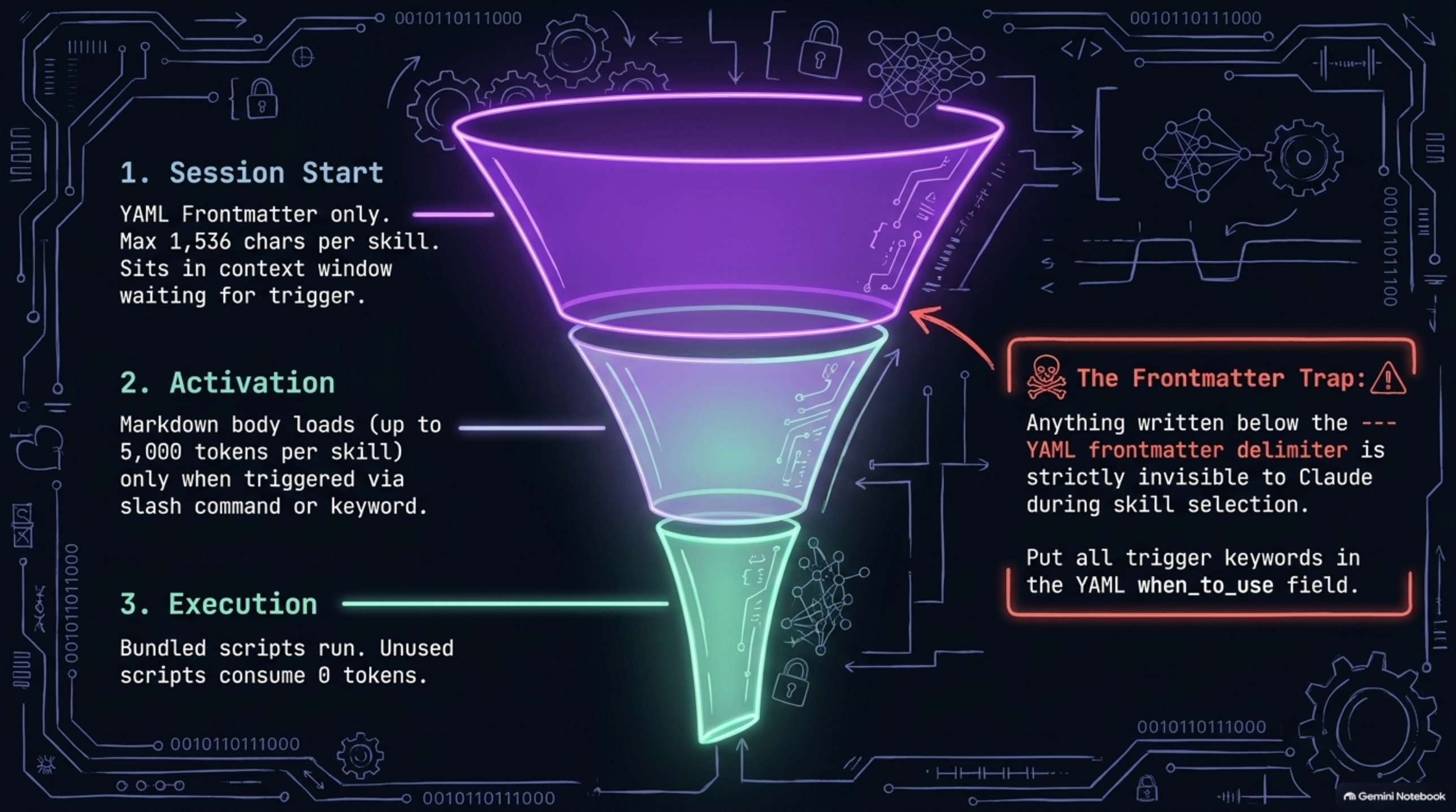


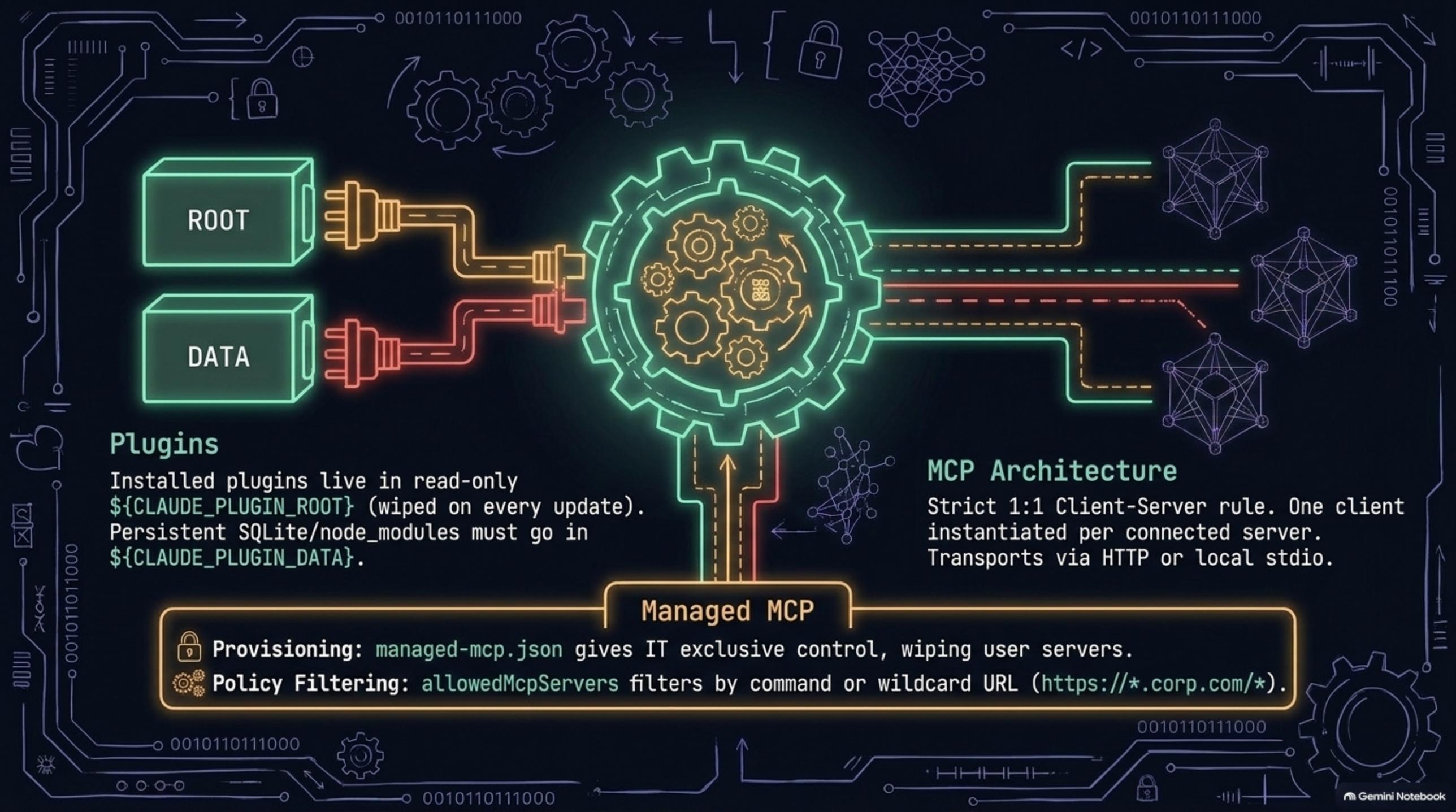
Parallel Execution Traps

- **Shared mutable state** (e.g., package.json).
- **Sequentially coupled interfaces** (backend/frontend drifting without a locked SPEC.md).
- **High boundary-spec coordination costs.**



Gemini Notebook


1. Session Start
YAML Frontmatter only.
Max 1,536 chars per skill.
Sits in context window
waiting for trigger.
2. Activation
Markdown body loads (up to
5,000 tokens per skill)
only when triggered via
slash command or keyword.
3. Execution
Bundled scripts run. Unused
scripts consume 0 tokens.
The Frontmatter Trap:
Anything written below the ---
YAML frontmatter delimiter is
strictly invisible to Claude
during skill selection.
Put all trigger keywords in
the YAML when_to_use field.
0010110111000
Gemini Notebook



Plugins

Installed plugins live in read-only `${CLAUDE_PLUGIN_ROOT}` (wiped on every update). Persistent SQLite/node_modules must go in `${CLAUDE_PLUGIN_DATA}`.

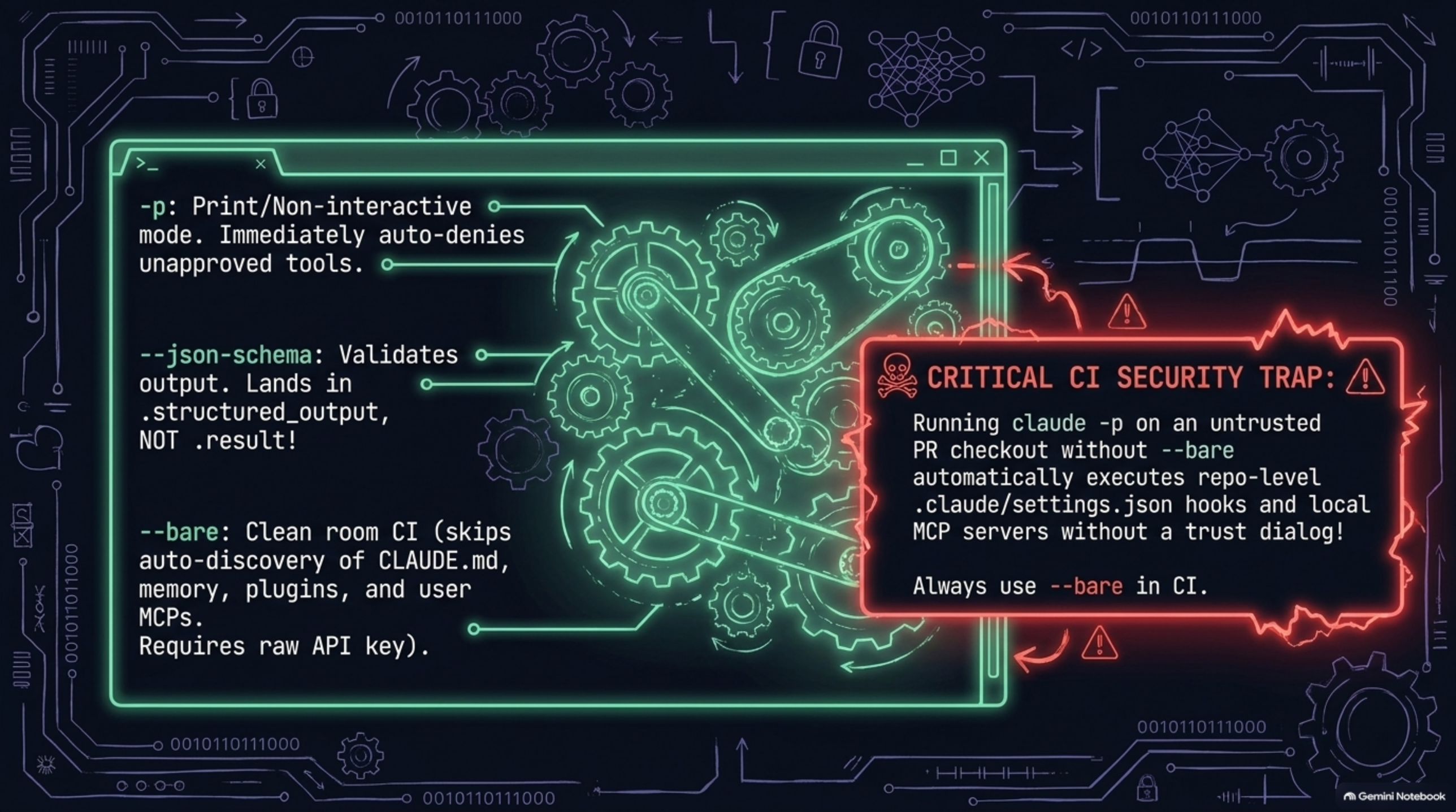
MCP Architecture

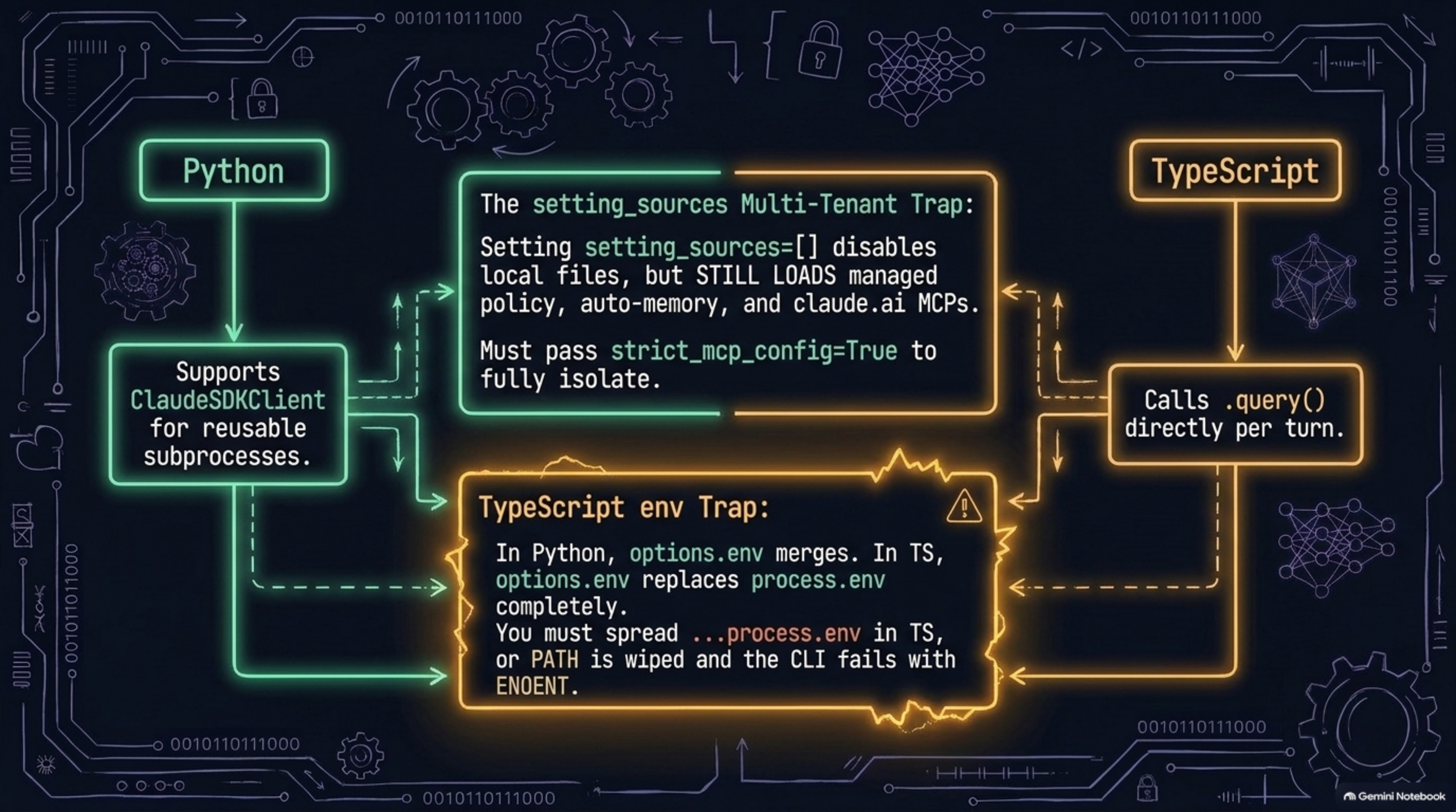
Strict 1:1 Client-Server rule. One client instantiated per connected server. Transports via HTTP or local stdio.

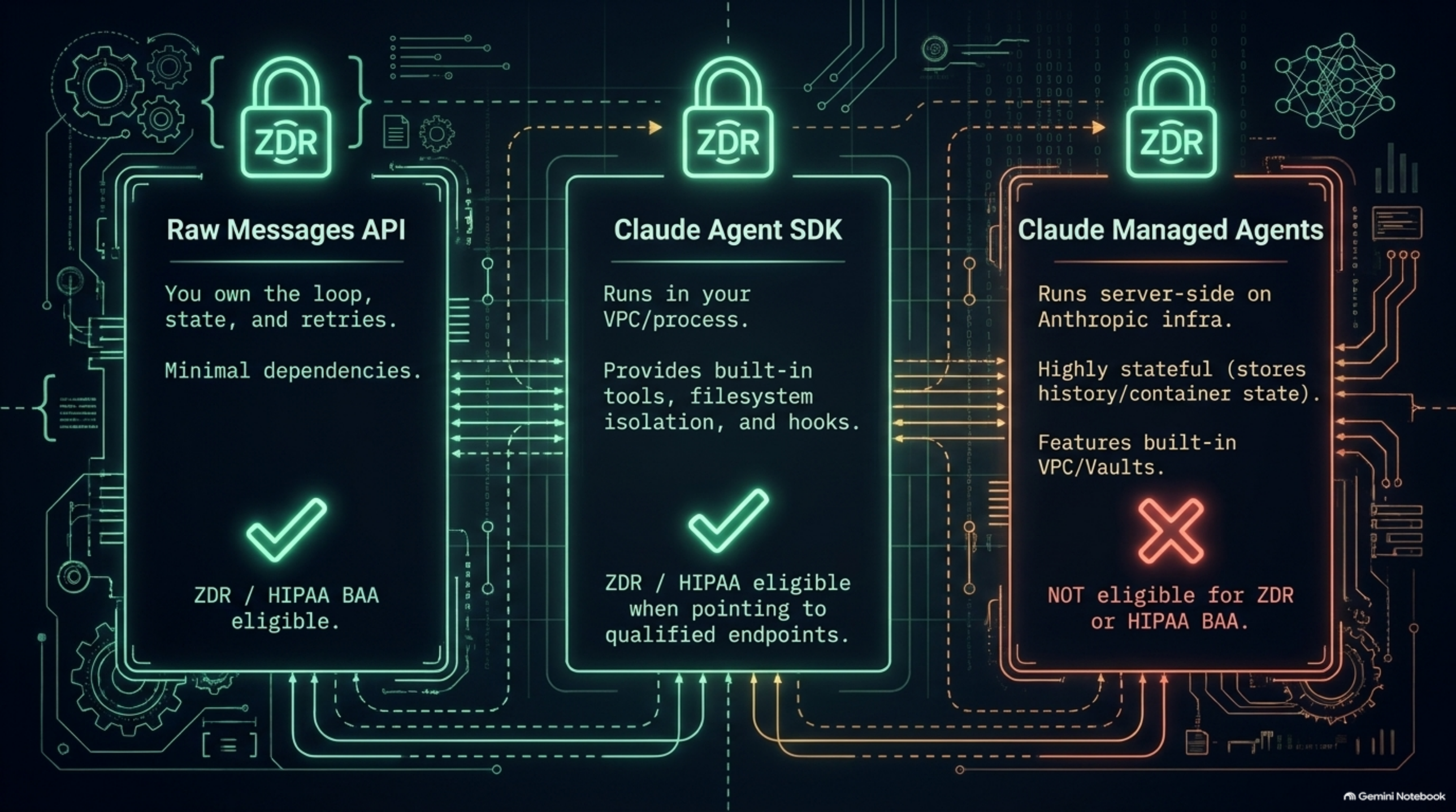
Managed MCP

- **Provisioning:** `managed-mcp.json` gives IT exclusive control, wiping user servers.
- **Policy Filtering:** `allowedMcpServers` filters by command or wildcard URL (`https://*.corp.com/*`).

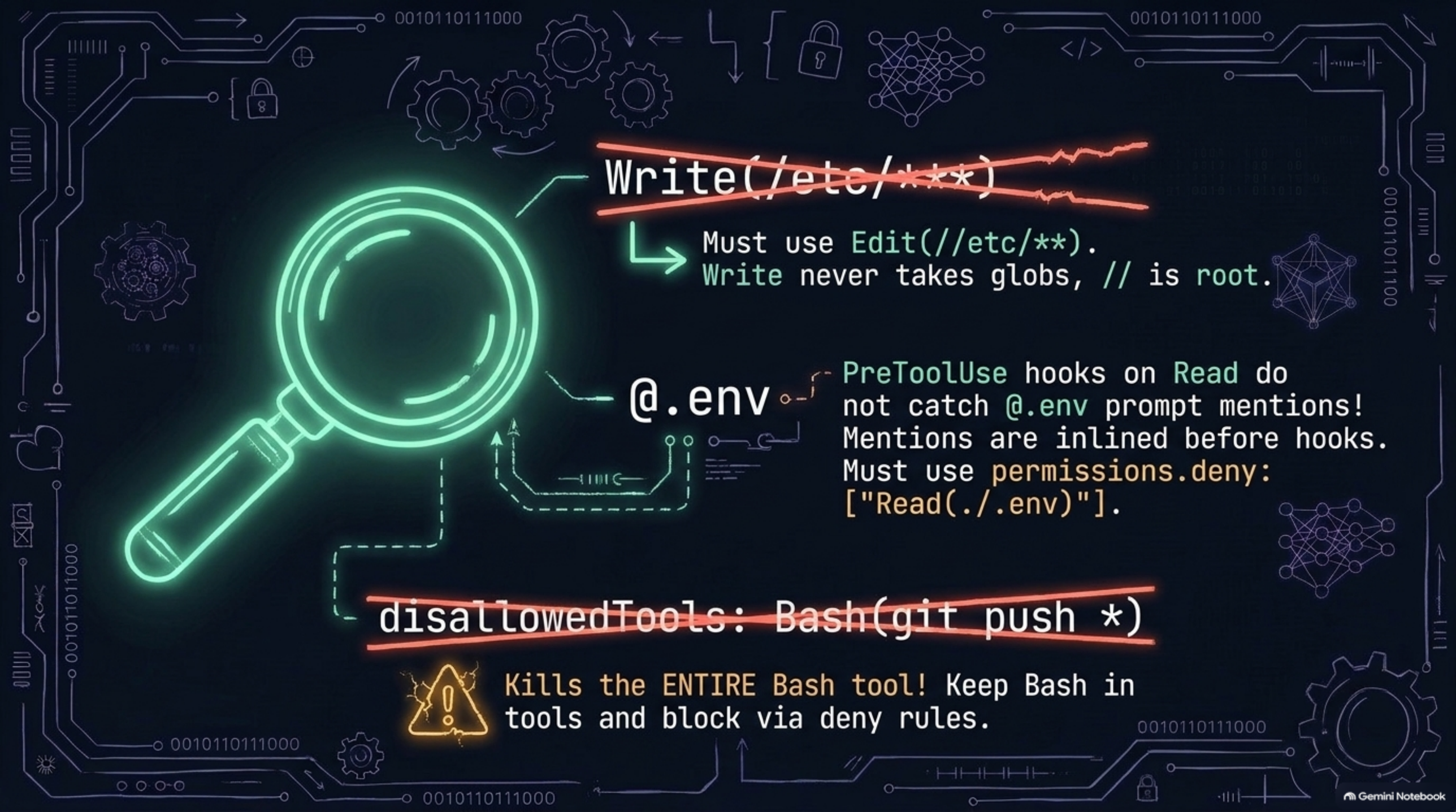
Gemini Notebook

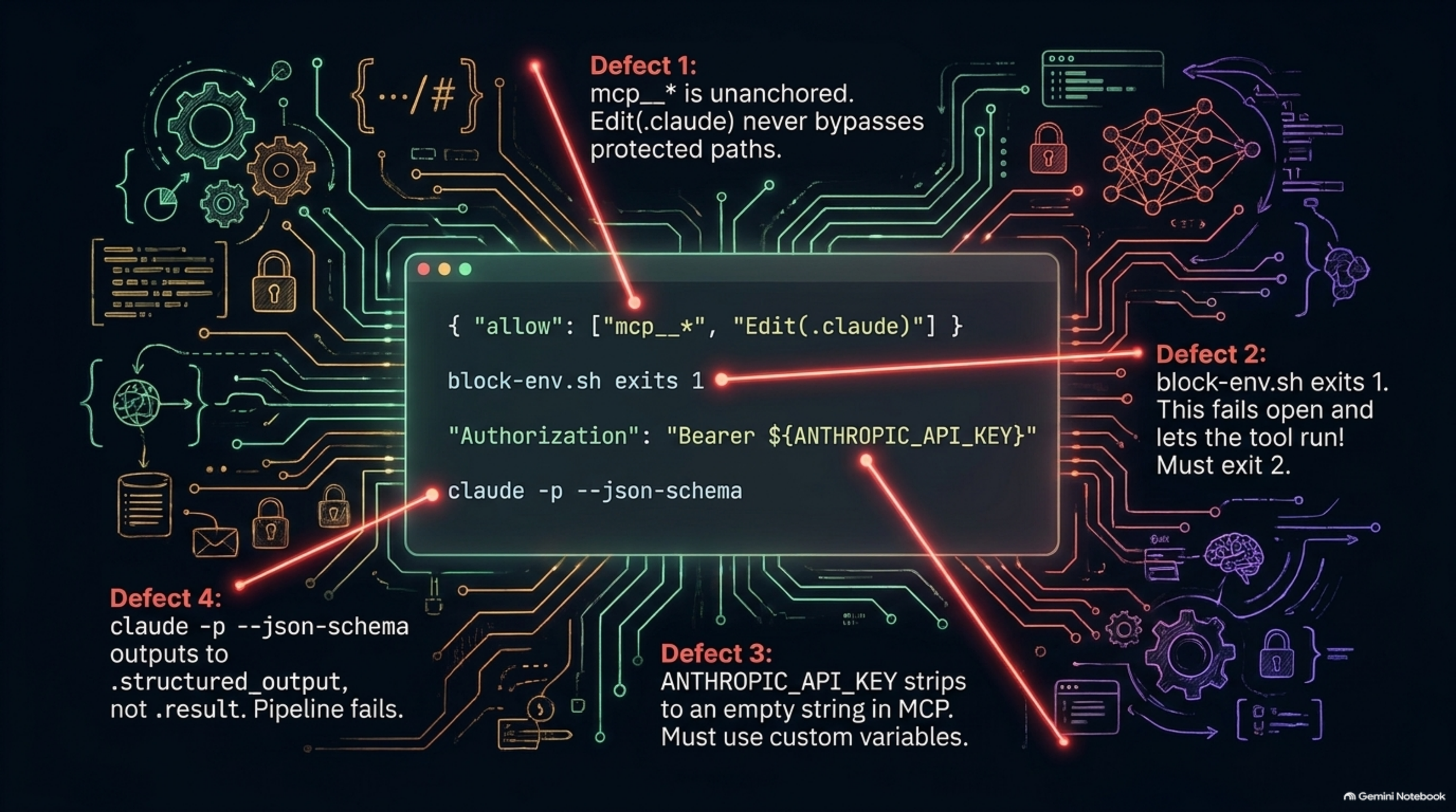

-p: Print/Non-interactive mode. Immediately auto-denies unapproved tools.
--json-schema: Validates output. Lands in .structured_output, NOT .result!
--bare: Clean room CI (skips auto-discovery of CLAUDE.md, memory, plugins, and user MCPs.
Requires raw API key).
CRITICAL CI SECURITY TRAP:
Running claude -p on an untrusted PR checkout without --bare automatically executes repo-level .claude/settings.json hooks and local MCP servers without a trust dialog!
Always use --bare in CI.
0010110111000
Gemini Notebook


Python
Supports ClaudeSDKClient for reusable subprocesses.
The setting_sources Multi-Tenant Trap:
Setting setting_sources=[] disables local files, but STILL LOADS managed policy, auto-memory, and claude.ai MCPs.
Must pass strict_mcp_config=True to fully isolate.
TypeScript
Calls .query() directly per turn.
TypeScript env Trap:
In Python, options.env merges. In TS, options.env replaces process.env completely.
You must spread ...process.env in TS, or PATH is wiped and the CLI fails with ENOENT.
0010110111000
Gemini Notebook



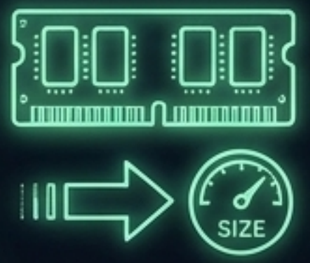
Gemini Notebook


Write(/etc/***)
Must use Edit(//etc/**).
Write never takes globs, // is root.
@.env
PreToolUse hooks on Read do not catch @.env prompt mentions!
Mentions are inlined before hooks.
Must use permissions.deny: ["Read(./.env)"].
disallowedTools: Bash(git push *)
Kills the ENTIRE Bash tool! Keep Bash in tools and block via deny rules.
0010110111000
Gemini Notebook



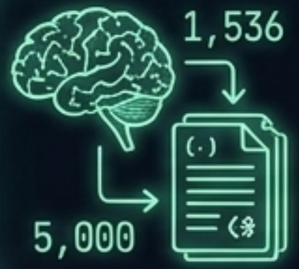
Gemini Notebook

AUTO-MEMORY LIMITS



Max 200 lines or 25KB loaded at startup.

SKILL CAPACITY



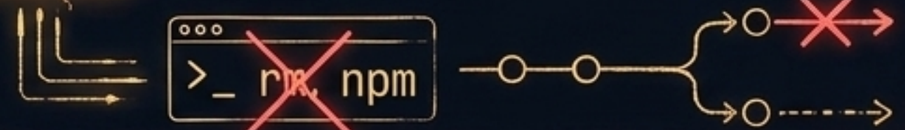
1,536 chars for frontmatter.
5,000 tokens for markdown body.
Max 32 skills per session.

CHECKPOINTING

/rewind retains data for 30 days.

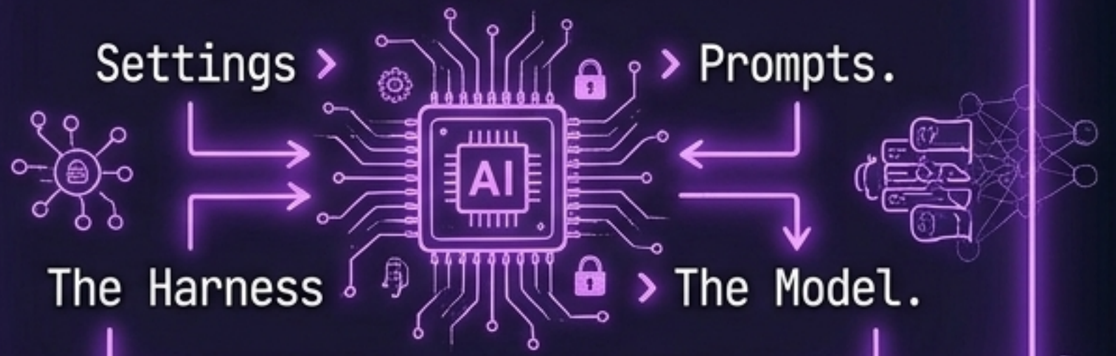


Critical limit: NEVER undoes Bash side-effects (rm, npm install).



FINAL SYNTHESIS RULE

Settings › › Prompts.



The Harness › The Model.

Design for determinism.

Gemini Notebook