



MCP
Dev Summit
North America

Patterns for Building MCP-powered Agent Systems

Jiquan Ngiam

Co-founder / CEO



About me



Jiquan Ngiam (JQ)

Stanford, advised by Andrew Ng
Coursera, Founding Team
Google Brain, Applied Research
MintMCP, Co-founder

Building an autonomous organization





Eric Monday at 5:29 PM

@Max what was the next steps discussed with [REDACTED].com after the call with Danie today



1



5 replies



Max APP Monday at 5:29 PM

✓ Looks like git operations are restricted by the environment. The progress.md and activity-log.csv up...

here's what was agreed on the [REDACTED].com call with danie today:

1. ****poc scoping call scheduled for tue apr 7**** at the same time (~16:30 utc). eric to send the invite. 45-60 min session to walk through pricing and align on what a successful poc looks like (which mcp servers to connect, which groups to pilot, etc.)
2. ****nda + security docs in parallel**** — danie is sending over their boilerplate nda, and their gic team will reach out for security info (soc 2, trust center). eric offered to send trust center links ahead of the call.
3. ****pricing preview**** — eric flagged it's user-based (no usage gates or sso tax). said based on their user count it shouldn't be an issue, but will go into scenarios on the apr 7 call.
4. ****poc timeline**** — eric mentioned typical pocs take 2-3 business weeks.



Peter APP Wednesday at 5:35 PM

☀️ wednesday evening wrap — march 25

█ active procurement tickets. 3 updated today. 2 new tickets.

🎉 big win: █ contract approved. █ confirmed both MSA + DPA accepted. Clean versions being created for signature.

2 replies



Peter APP Wednesday at █ Cursor

👤 @Bo Zhi See

🔴 RED

█

- Contract approved by █. Watch for signature request via Ironclad. DPA goes to you, MSA goes to @jngiam. Go-live target is TOMORROW (March 27).

█

- █ emailed today checking in on commercial terms. Respond to MSA redlines ASAP. Deep dive call TOMORROW with █

- Get DPA signed by Bo. █ is waiting.



jngiam Mar 6th at 7:52 AM

@Dan Loop hey the vscode quick install button does this npx remote thing, instead we should now switch the quick install to do http instead, can you fix?



1



7 replies



Dan Loop APP Mar 6th at 7:52 AM

✅ Main is protected - the workflow will auto-commit `progress.md` and `activity-log.csv` after the ses...

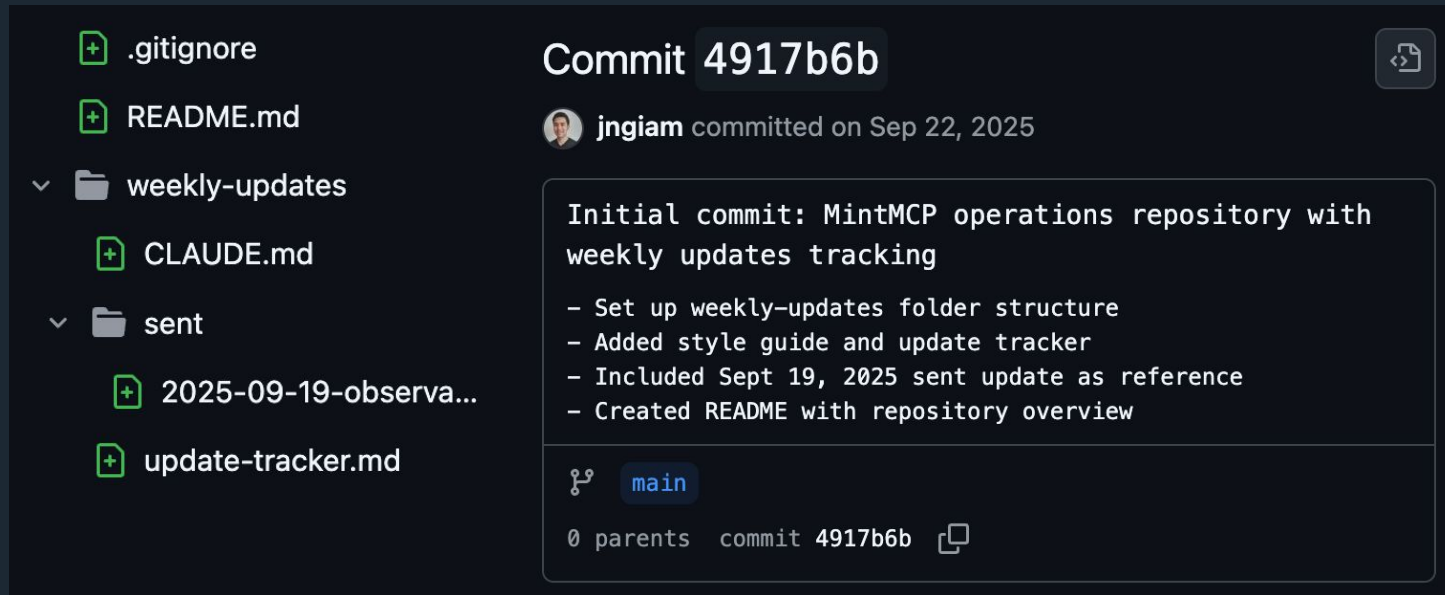
On it! Looking into the VS Code quick install button to switch it from npx to HTTP. Let me find the relevant code first.

Done! PR #1348: <https://github.com/d8e-ai/mintmcp/pull/1348>

Changed the VS Code "Add to VSCode" quick install button from `type: "studio"` with `npx -y mcp-remote` to `type: "http"` with the direct URL. Both occurrences in `setup-instructions.tsx` updated.

Our journey to
agentifying the business

Our first steps | September 2025



The screenshot displays a Git commit interface. On the left, a file tree shows the repository structure: `.gitignore`, `README.md`, a folder `weekly-updates` containing `CLAUDE.md`, a folder `sent` containing `2025-09-19-observa...`, and `update-tracker.md`. The right side shows the commit details for `Commit 4917b6b` by `jngiam`, committed on `Sep 22, 2025`. The commit message is: `Initial commit: MintMCP operations repository with weekly updates tracking`. The commit includes a list of changes: `- Set up weekly-updates folder structure`, `- Added style guide and update tracker`, `- Included Sept 19, 2025 sent update as reference`, and `- Created README with repository overview`. Below the message, the current branch is `main`, and the commit has `0 parents`.

Git Repository for all **Business Operations**

Our first steps | September 2025

MintMCP Weekly Updates Guide

Purpose

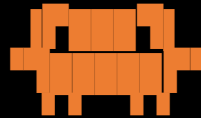
Weekly updates to MintMCP customers about new features, capabilities,

Tone & Format

- Direct and concise: Get to the point without unnecessary padding
- Feature-focused: Lead with the feature and explain the benefit

...

CLAUDE.md



Claude Code
Sonnet 4

~/mintmcp-ops/weekly-updates

› Let's write the update post for this week!

- Let me gather context on recent developments and any existing updates to inform this week's post.

...

Connects to **GitHub**, **Linear** via MCP ...



Our first steps | November 2025

```
● weekly-updates/ (Nov 2025)
├── CLAUDE.md
├── update-tracker.md
├── drafts/
│   ├── 2025-11-03-security-summit-vmcp.md
│   └── 2025-11-11-analytics-insights.md
├── sent/
│   ├── 2025-09-19-observability-gateway.md
│   ├── 2025-09-23-registry-performance.md
│   ├── 2025-09-30-docs-devsummit.md
│   ├── 2025-10-07-whitepaper-features.md
│   ├── 2025-10-14-cursor-bedrock.md
│   ├── 2025-10-21-compatibility-secrets.md
│   └── 2025-10-28-enterprise-controls.md
```

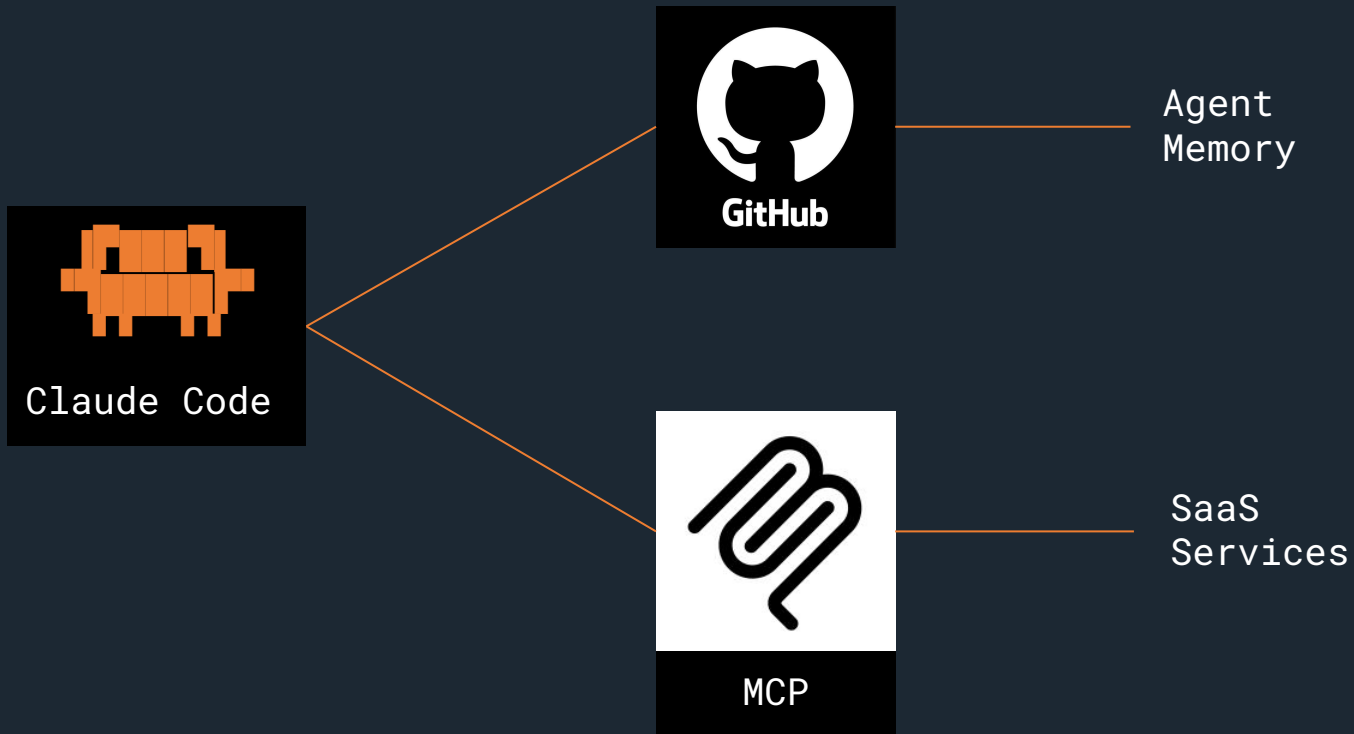
Progress Tracker
(Markdown)

Files as “Memory” in Git

Claude Code could pull up the files as needed to figure out context.

(e.g., don't re-send updates)

Early Core Pattern



Pattern 1: Git as Memory

- **Fully auditable**

`git blame`

- **Easily reversible**

`git revert`

- **Multi-agent ready**

`git merge`

- **Human-in-the-loop**

`git pull request`

- **Auto learning**

self-updates CLAUDE.md and configurations

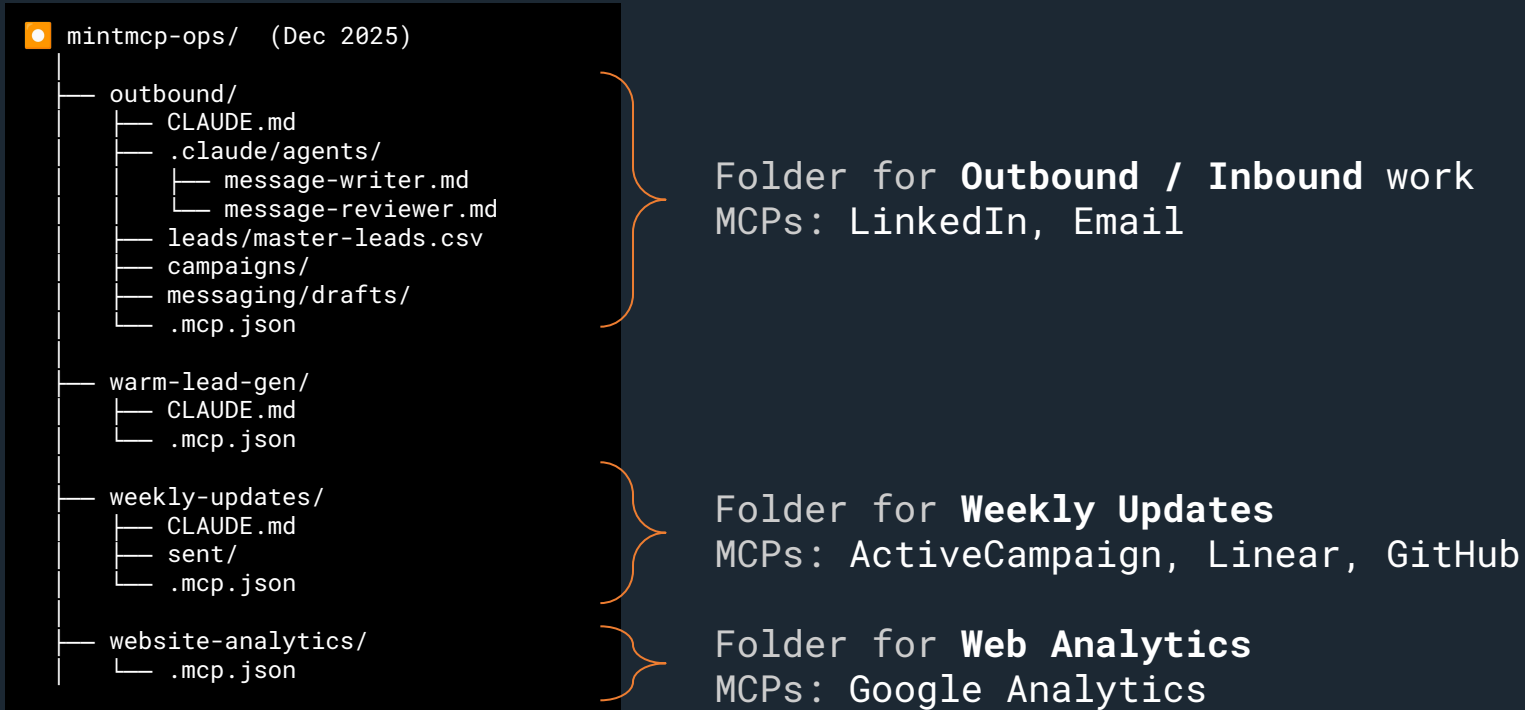


Agent
Memory

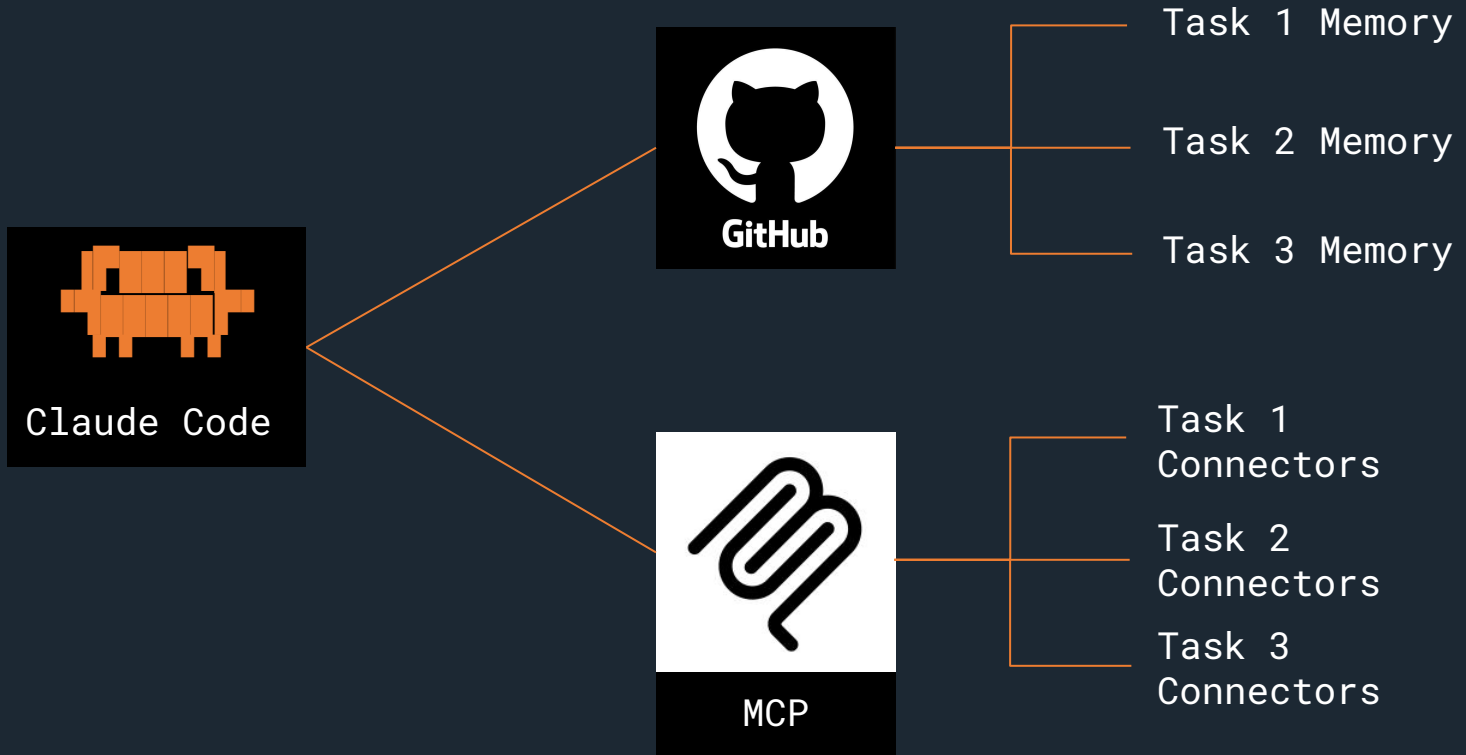
If a coding agent can handle a **huge code repository**, it can handle a **huge memory repository**.



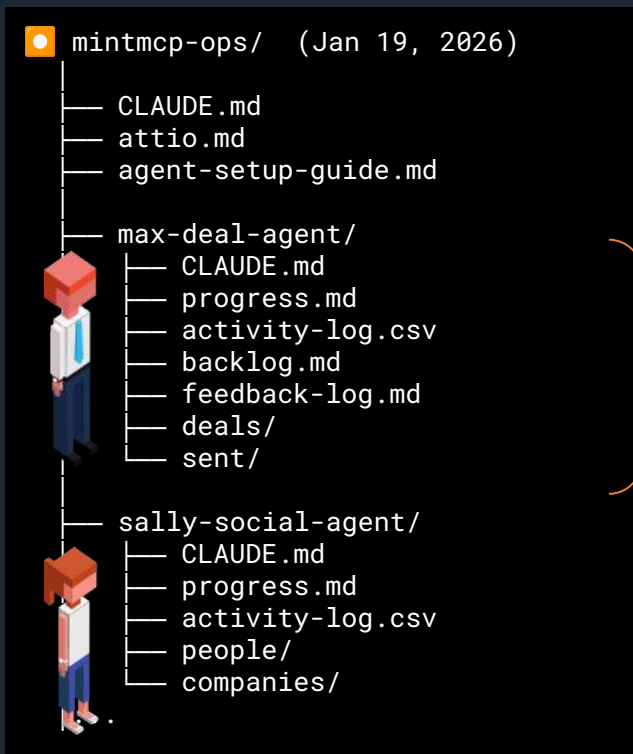
Toddler steps | Dec 2025



Early Core Pattern



Toddler steps | Jan 2026



More structure in each folder.

activity-log.csv

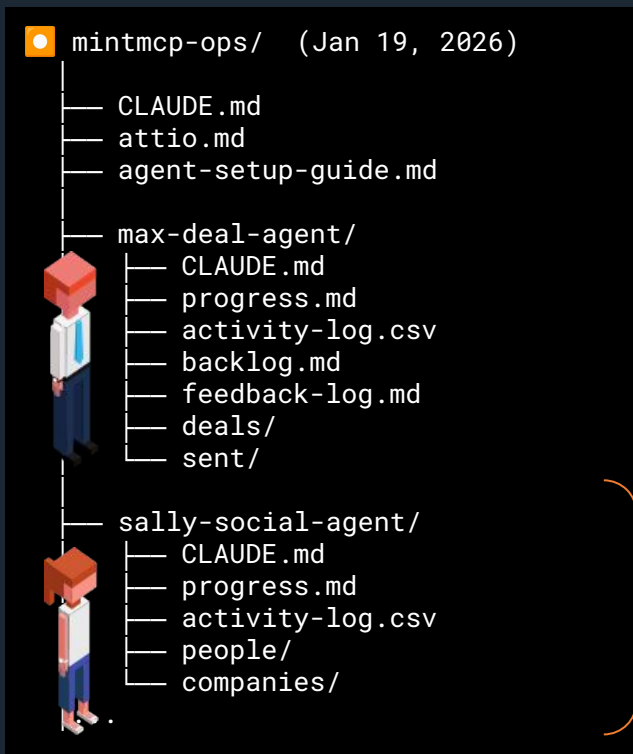
- Append only csv log of activity.
- Agent reads on session start to understand where they left off

Also, specialized sub-folders per agent.

Pattern 2: CLAUDE.md instructions + progress files

- **Auto-update tracking files**
progress.md, activity-log.csv
- **Always load progress files on startup**
Read most recent lines in
progress.md, activity-log.csv
- **Always run Bash(date) on startup**
Models are still [!] terrible at dates,
and day of the week.
- **Each agent maintains its own folder structure**
Sub-folders and files.

Agent beginnings | Jan 2026

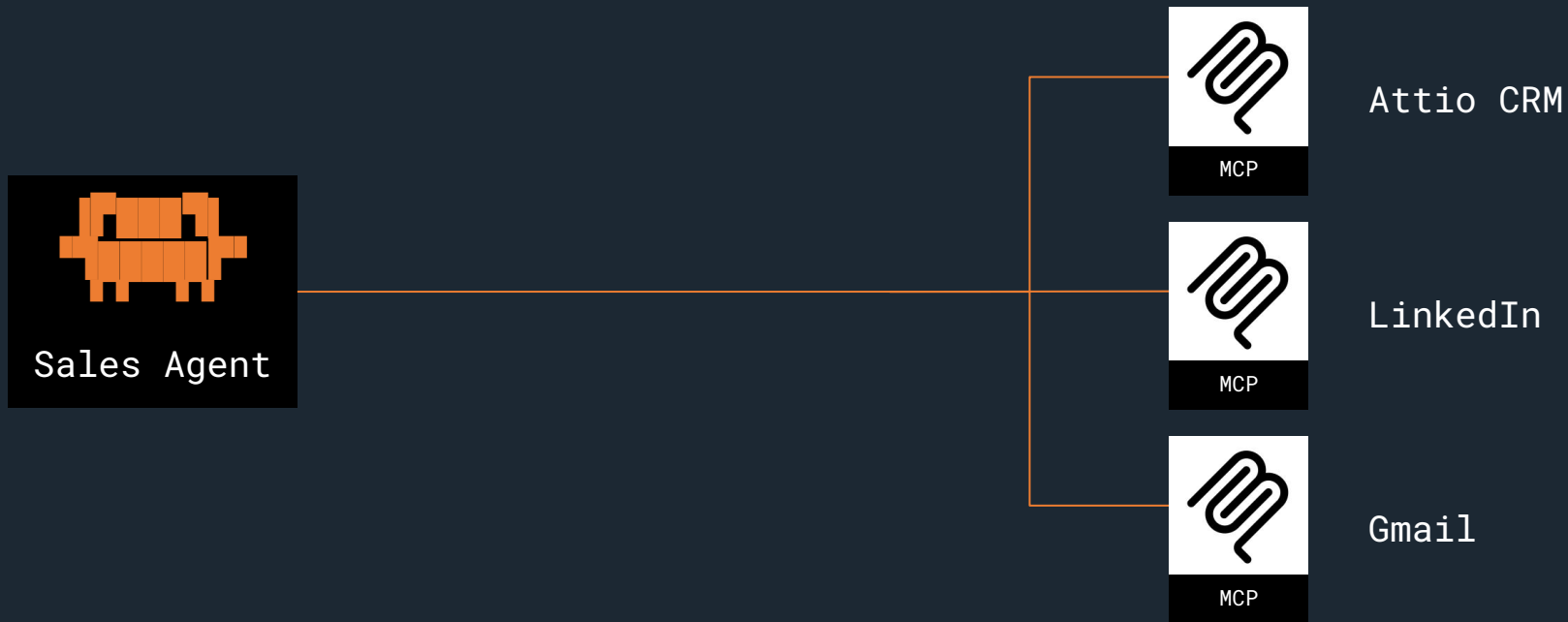


Then, it started to get unwieldy.

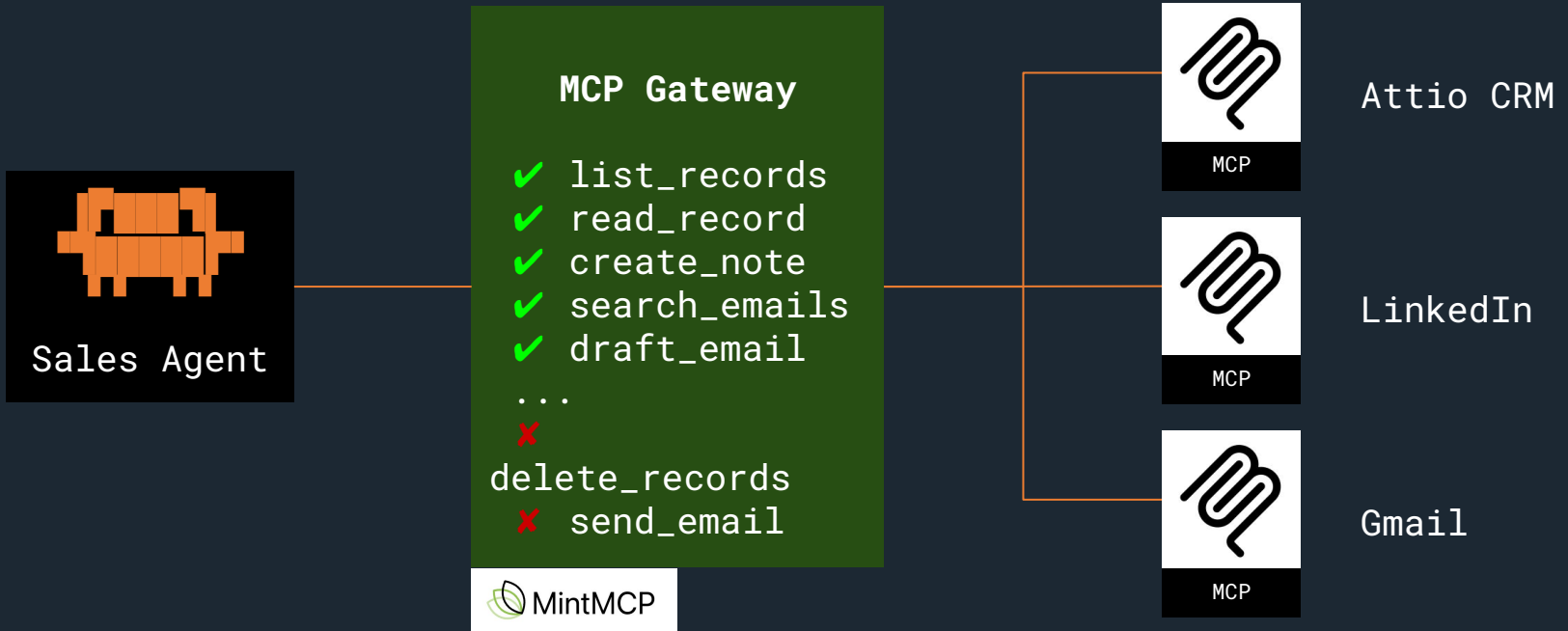
We wanted Sally social scanning agent to run in the **background** every morning, but:

- Prompt injection attacks?
- Fine-grained MCP tool permissions?
- Using OAuth MCP in a background agent?
- Whose identity is Sally using?
- What did it actually do?

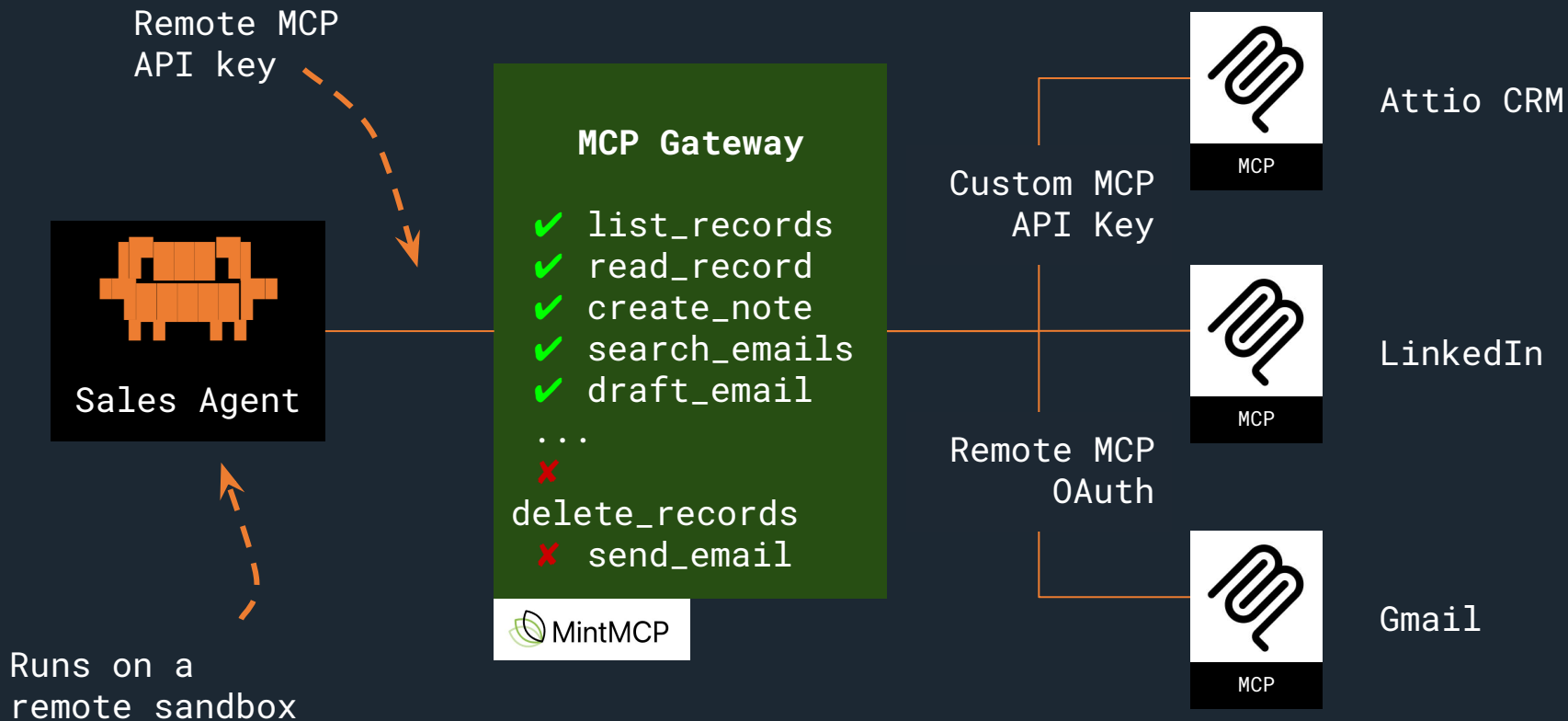
Fine-grained tool permissions | Feb 2026



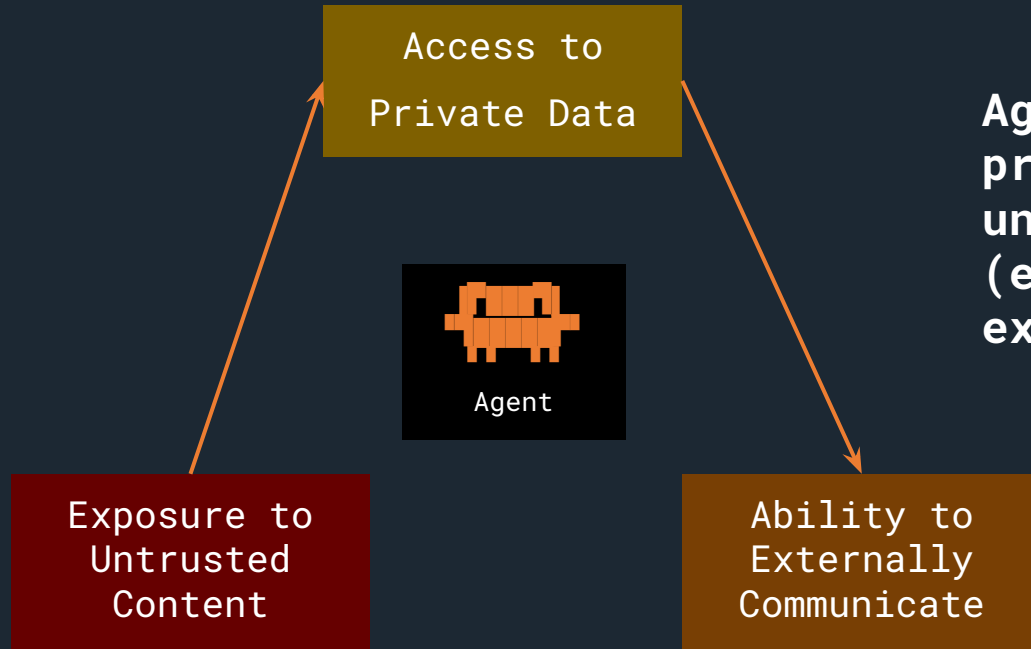
Pattern 3: MCP Gateway



Pattern 3: MCP Gateway

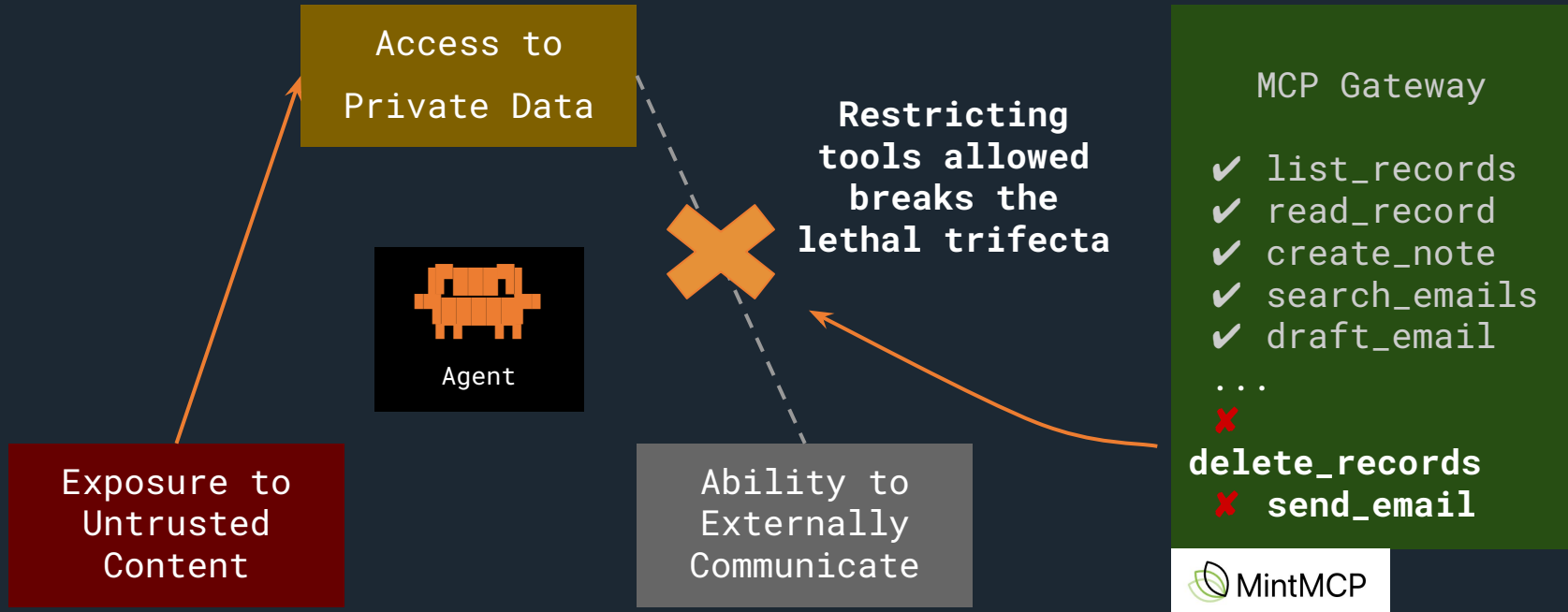


Lethal trifecta | Feb 2026



Agents can be prompt injected via untrusted content (e.g., external emails) to exfiltrate private data.

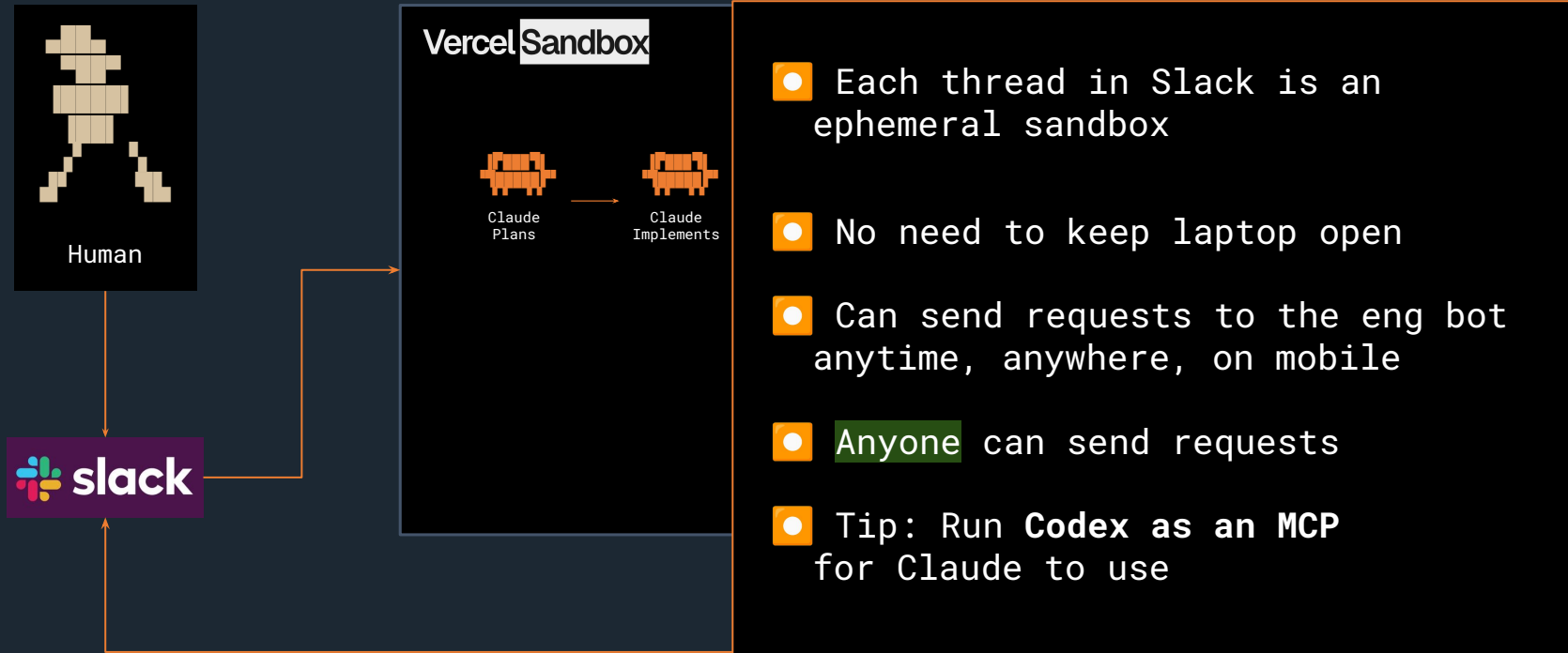
Lethal trifecta | Feb 2026



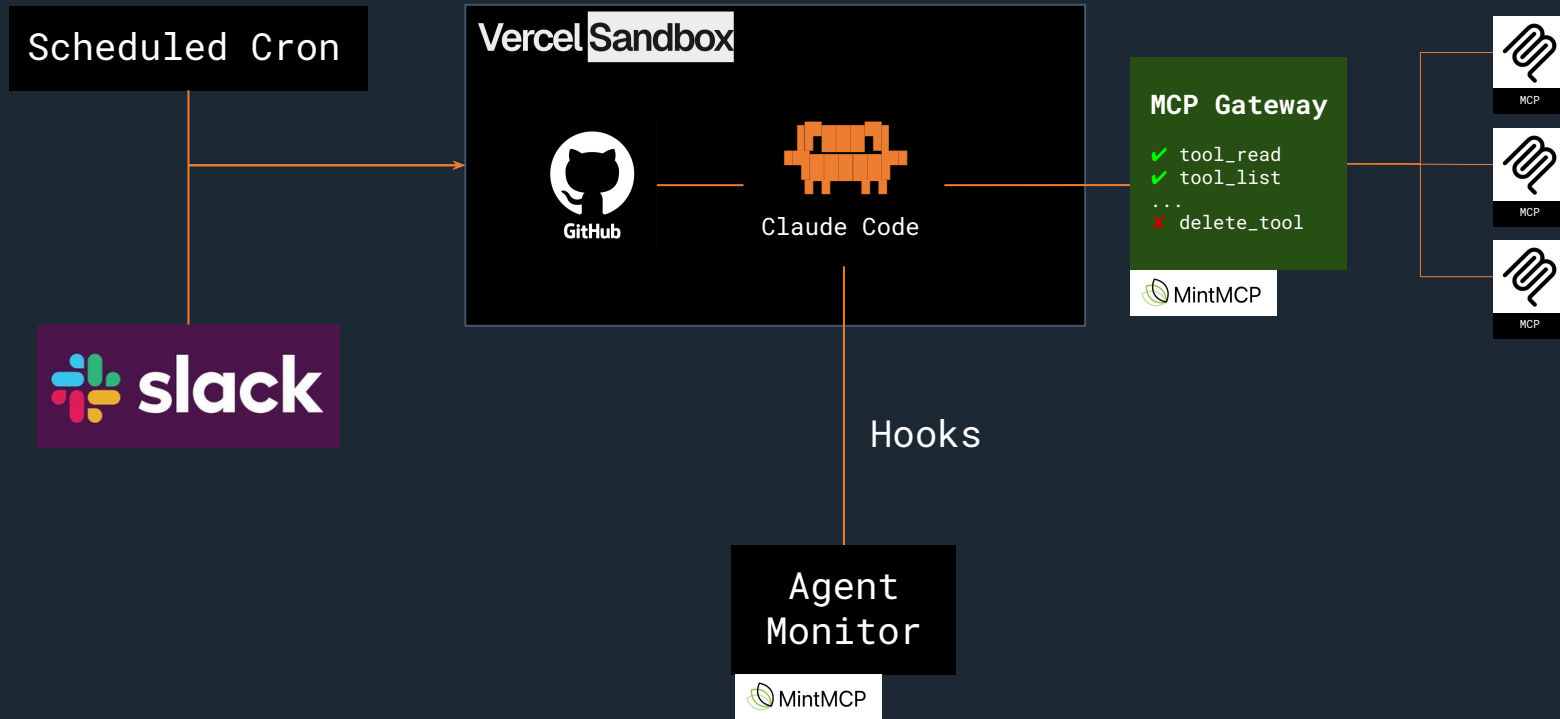
Engineering agents | Feb 2026



Engineering agents | Feb 2026

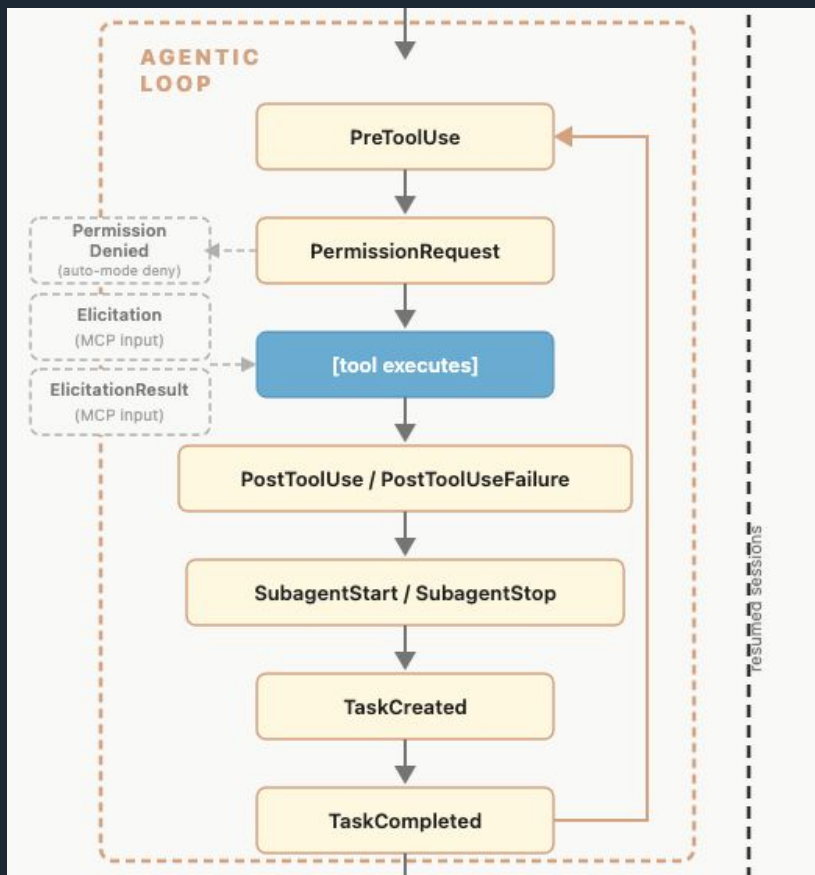


Pattern 4: Slack for all Agents





Pattern 5: Hooks for Monitoring



- Examples: PreToolUse, PostToolUse
- Call scripts on trigger
- Collect telemetry and apply guardrails

Agent Monitoring

Agent activity

Real-time view of all agent activity by your team. Last updated Apr 1 at 10:44 AM.

Dashboard	Live Activity	Last 24 Hours		
Timestamp	User	Status	Agent	Tools
2026-04-01 10:45:42	dan-loop	✓	✶	Bash cd /tmp/repo && git fetch
2026-04-01 10:45:42	dan-loop	✓	✶	Bash cd /tmp/repo && git fetch
2026-04-01 10:45:42	dan-loop	✓	✶	Bash cd /tmp/repo && git fetch
2026-04-01 10:45:38	dan-loop	✗	✶	Bash cd /tmp/repo && git remot
2026-04-01 10:45:38	dan-loop	✓	✶	Bash cd /tmp/repo && git remot
2026-04-01 10:45:38	dan-loop	✓	✶	Bash cd /tmp/repo && git remot
2026-04-01 10:45:34	dan-loop	✓	✶	WebFetch https://api.github.co Extract the PR titl
2026-04-01 10:45:29	dan-loop	✓	✶	WebFetch https://github.com/d8 Extract the full PF
2026-04-01 10:45:28	dan-loop	✓	✶	mcp_slack_slack_reply_to_thread
2026-04-01 10:45:28	dan-loop	⚠	✶	mcp_slack_slack_reply_to_thread
2026-04-01 10:45:24	dan-loop	✓	✶	ToolSearch {"query":"select:Web
2026-04-01 10:45:24	dan-loop	✓	✶	ToolSearch {"query":"select:Web

Request details

User: dan-loop	Agent: Claude (hooks)
Event: After Tool Use	Time: Apr 1, 2026, 10:47:34 AM

✓ SUCCESS Tool result recorded

Tool called: mcp_slack_slack_reply_to_thread

Command: {"channel_id":"C0AH6K9CNJW","thread_ts":"1775065467.054759","text":"Review of PR #1582 - \"Fall back to JWT exp claim when token response omits expires_in\"\\n\\n*Summary*: When OAuth providers (e.g. Salesforce) issue JWT access tokens but omit `expires_in`/`expires_at` from the token response, hosted OAuth credentials get stored without `expiresAt`. This means the proactive refresh check (`hostedOAuthCredentialNeedsRefresh`) never fires and the token silently expires. The fix decodes the JWT `exp` claim as a (truncated)

Matched Rules

No rules matched

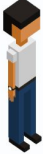





















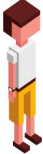



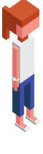

















View full conversation

View full details

> Technical details



Our agents | April 2026

 <p>Bella  d8e-ai/mintmcp-ops</p> <p>Weekly monitoring of MintMCP's email sending reputation. Checks DNS blacklists and Google Postmaster Tools, then sends a Slack summary.</p> <p> At 09:00 AM, only on Monday (PDT)</p> <p>→ Open ▶ Run </p>	 <p>Vera  d8e-ai/mint-mcp-docs</p> <p>Vera verifies factual claims in MintMCP blog articles and content. She runs on a daily schedule to check recently updated articles and can also be triggered via Slack conversation or...</p> <p> At 07:00 AM (PDT)</p> <p>→ Open ▶ Run </p>	 <p>Charlie  d8e-ai/mintmcp-ops</p> <p>Charlie analyzes call transcripts from prospect meetings, extracts actionable sales insights using Gong-backed research prompts, and attaches analysis notes to deals. Charlie ensur...</p> <p> At 0 and 30 minutes past the hour, between 11:00 AM a...  At 0 and 30 minutes past the hour, between 05:00 PM ...</p> <p>→ Open ▶ Run </p>
 <p>Chris  d8e-ai/mintmcp-ops</p> <p>You are an agent that focuses on figuring out what customer's usage of mint is on a per customer level</p> <p>→ Open ▶ Run </p>	 <p>Cora  d8e-ai/mintmcp-ops</p> <p>You are Cora, MintMCP's acquisition marketing engine. Your job is to keep MintMCP visible to buyers before they ever talk to sales.</p> <p>→ Open ▶ Run </p>	 <p>Dan Loop  d8e-ai/mintmcp</p> <p>@./AGENTS.md</p> <p>→ Open ▶ Run </p>
 <p>Food Bot  d8e-ai/mintmcp-ops</p> <p>Food Bot lives in Slack on the food channel. Every weekday it recommends a restaurant in the Palo Alto area for the team, based on what we've been eating recently on DoorDash. It handles...</p> <p> At 10:00 AM and 11:00 AM, Monday through Friday (PDT)</p> <p>→ Open ▶ Run </p>	 <p>Izzy Issues  d8e-ai/mintmcp-ops</p> <p>Izzy manages the markdown ticket system in "tickets/". She wakes up on a schedule to surface priorities, chase stale tickets, and keep the team accountable via Slack. She reads...</p> <p> Every 30 minutes (UTC)</p> <p>→ Open ▶ Run </p>	 <p>Jakes Customer Followup  d8e-ai/mintmcp-ops</p> <p>Jake monitors shared Slack channels with customers, identifies unanswered questions, creates followup tickets via Izzy, and tracks them to resolution. He runs twice daily (morning and...</p> <p> At 09:00 AM, Monday through Friday (PDT)  At 05:00 PM, Sunday through Thursday (PDT)</p> <p>→ Open ▶ Run </p>
 <p>Leo  d8e-ai/mintmcp-ops</p> <p>Leo drives MintMCP's marketing strategy and execution: content, social, PR, paid channels, developer marketing, and events. Leo thinks like a growth marketer — every action should either...</p> <p>▶ Run </p>	 <p>Mary MCP Researcher  d8e-ai/mint-mcp-docs</p> <p>Mary creates instructional guides that teach users how to connect MCP servers to MintMCP. Given a GitHub repo URL or documentation link for an MCP server, she researches the full setu...</p> <p>▶ Run </p>	 <p>Matt  d8e-ai/mintmcp-ops</p> <p>Matt creates customized sales materials tailored to specific customers and deals. He reads deal context (Attio notes, call analyses, Sally's intel) and reference materials ('../materials/'), then...</p> <p>▶ Run </p>

Engineering
Documentation
Marketing
Sales
Procurement
Support
Food
...

Each agent has its own agent identity and MCP gateway

Thank you

- P1: Use **Git as Memory**
- P2: **CLAUDE.md** instructions + progress files
- P3: **MCP Gateways** for Agent Tool Permissions.
Deny the trifecta
- P4: Agents in **Slack** with long-term memory unlocks huge AI adoption
- P5: **Hooks for Agent Monitoring** to track background agent behavior



Dig deeper
into this
topic at our
free webinar



LinkedIn
Jiquan Ngiam
in/jngiam