

TRM Labs' Agent-Agnostic MCP Journey

Andrew Hannigan · TRM Labs × Jeremy Drouillard · Stacklok

Agenda

1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
3. The underlying open source technology: ToolHive
4. Recap and takeaways

TRM Labs is building the operating system for crimefighters. We develop intelligence software that helps detect and disrupt criminal networks.

185+

blockchains covered

600+

government agencies and financial institutions

75

countries

Crime is scaling with AI

+40%

year-over-year growth in criminal AI adoption

TRM AI-in-Crime Adoption Index, 2026

500%

growth in AI-enabled scams

TRM 2026 Crypto Crime Report

\$5.8B → \$7.2B

pig butchering losses, 2024 to 2025. TRM calls it the clearest example of a scam scaled by AI: distinct schemes up 164% in a year

FBI IC3; TRM AI-in-Crime Adoption Index

Criminals scale with AI. Defenders have to scale the same way.

TIMELINE

Accelerating AI adoption at TRM in 2026

\$ trm-agent

Profile Setup

Each profile enables a different set of tools based on your team's needs.

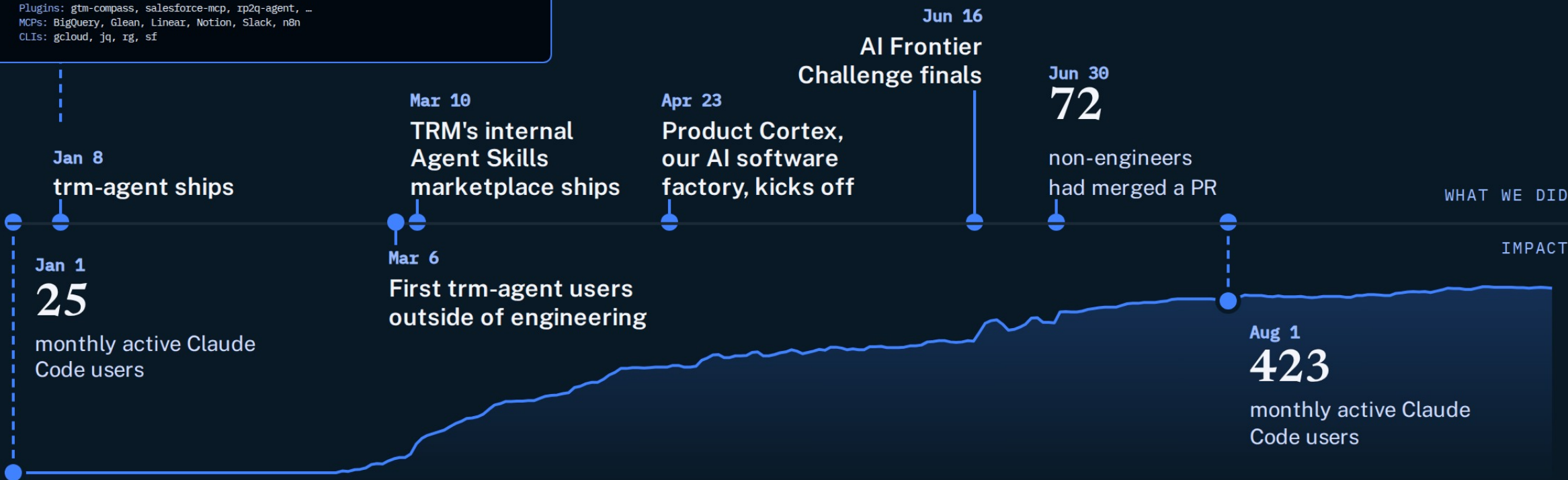
R&D

- Revenue Operations Team
- Product Marketing Team
- Intelligence Operations Team

Plugins: gtm-compass, salesforce-mcp, rp2q-agent, ...

MCPs: BigQuery, Glean, Linear, Notion, Slack, n8n

CLIs: gcloud, jq, rg, sf



Accelerating AI adoption at TRM in 2026

```
$ trm-agent
```

Profile Setup

Each profile enables a different set of tools based on your team's needs.

R&D

- Revenue Operations Team
- Product Marketing Team
- Intelligence Operations Team

Plugins: gtm-compass, salesforce-mcp, rp2q-agent, ...

MCPs: BigQuery, Glean, Linear, Notion, Slack, n8n

CLIs: gcloud, jq, rg, sf

Jan 8

trm-agent ships

Jan 1

25

monthly active Claude
Code users

WHAT WE DID

IMPACT

Aug 1

423

monthly active Claude
Code users

Accelerating AI adoption at TRM in 2026



TIMELINE

Accelerating AI adoption at TRM in 2026

```
$ trm-agent
```

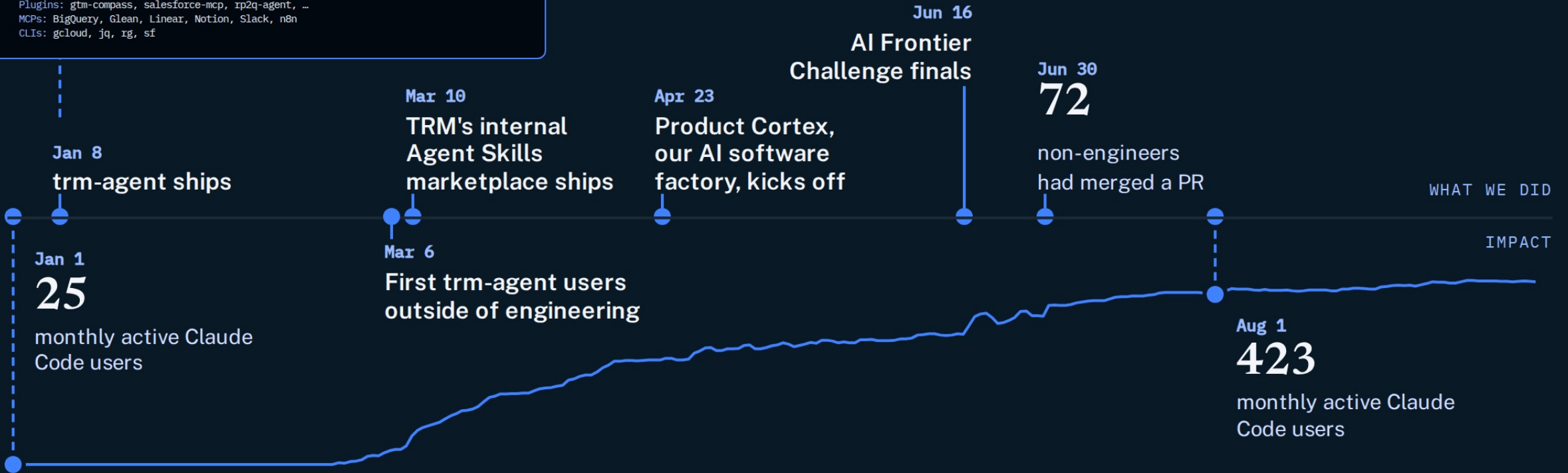
Profile Setup

Each profile enables a different set of tools based on your team's needs.

R&D

- Revenue Operations Team
- Product Marketing Team
- Intelligence Operations Team

Plugins: gtm-compass, salesforce-mcp, rp2q-agent, ...
MCPs: BigQuery, Glean, Linear, Notion, Slack, n8n
CLIs: gcloud, jq, rg, sf

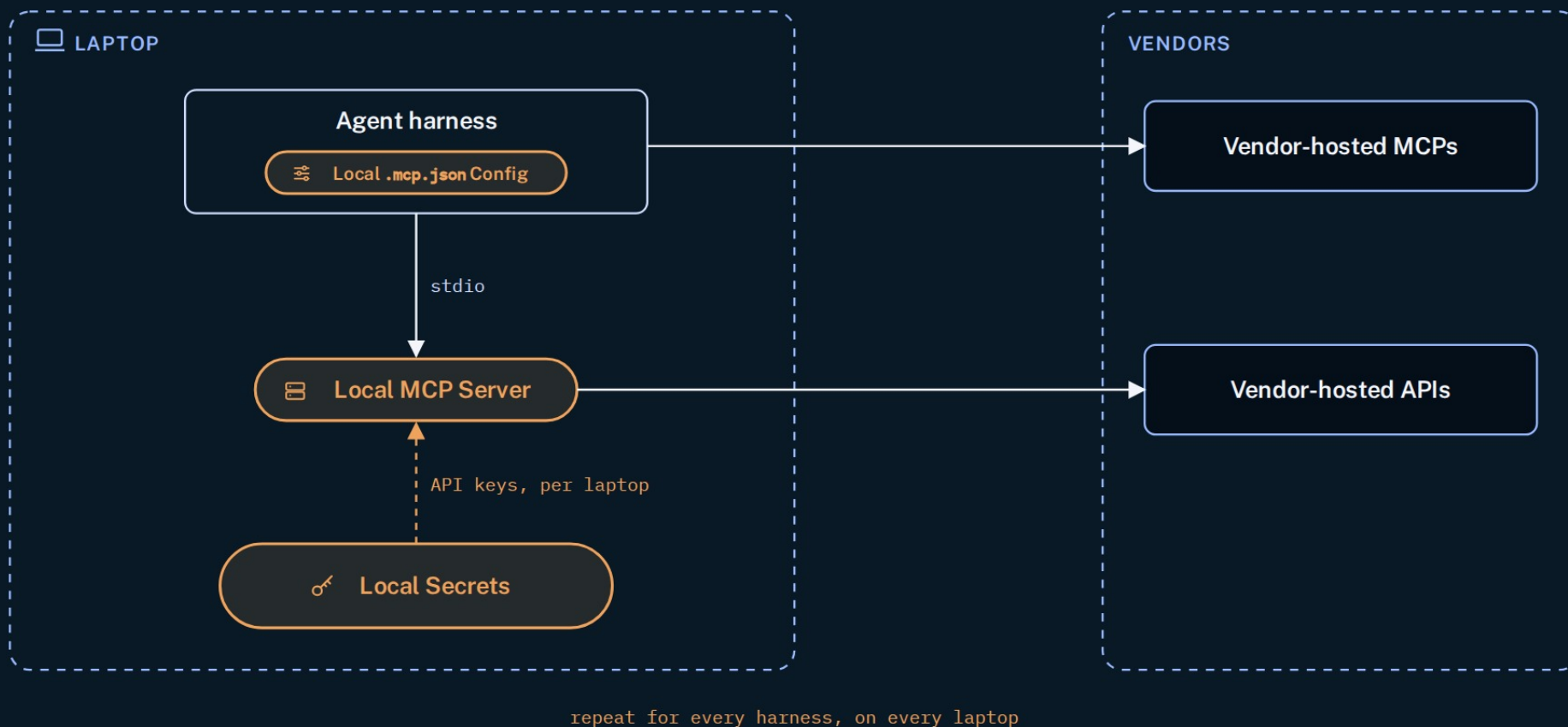


Agenda

1. TRM and its AI adoption journey
- 2. Scaling challenges and how we fixed them**
3. The underlying open source technology: ToolHive
4. Recap and takeaways

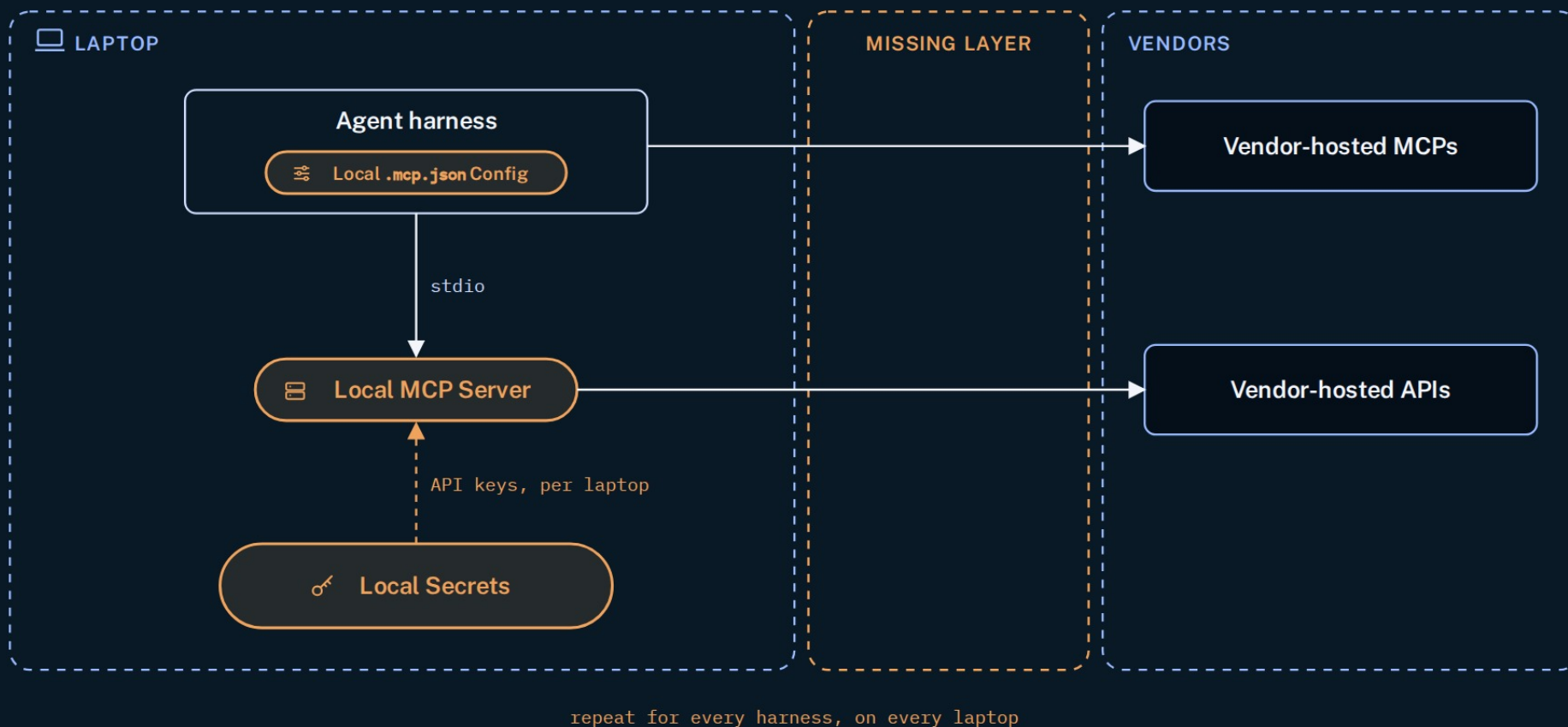
BEFORE

Every laptop was its own integration

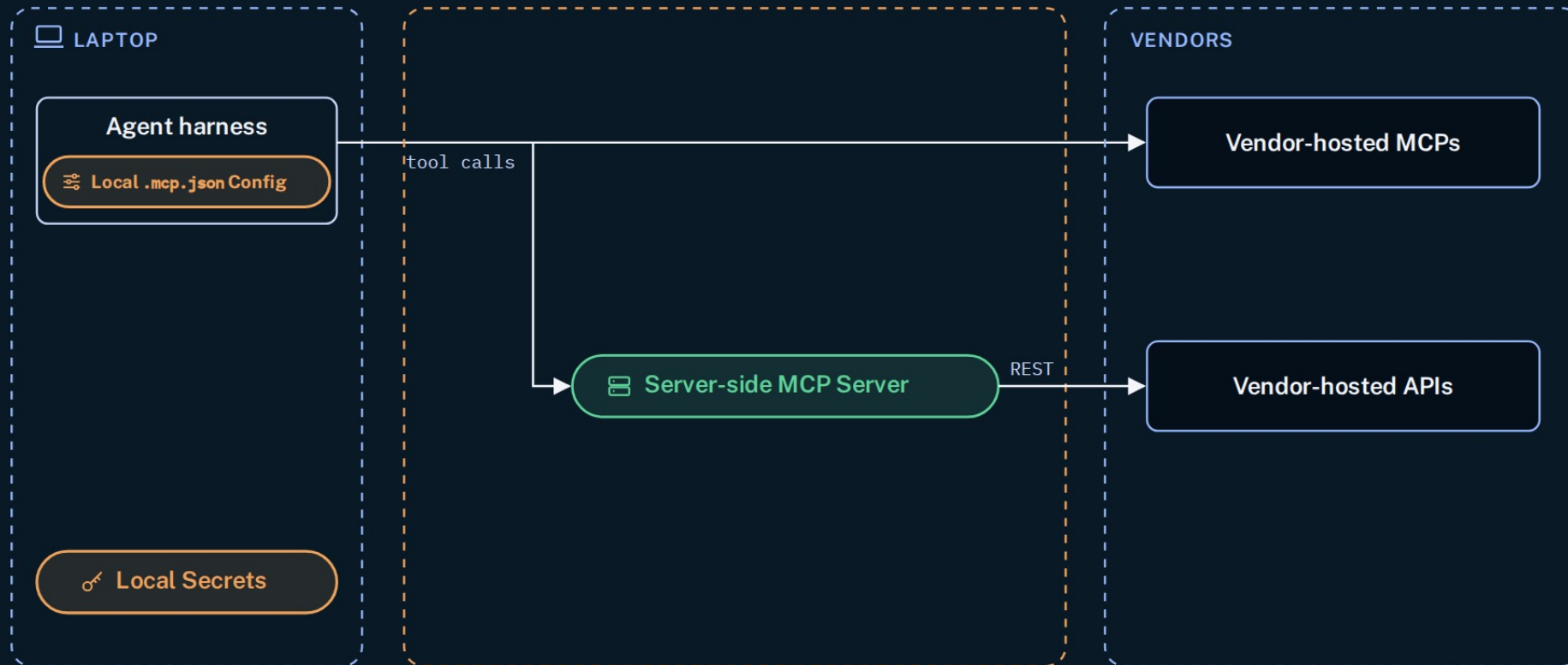


BEFORE

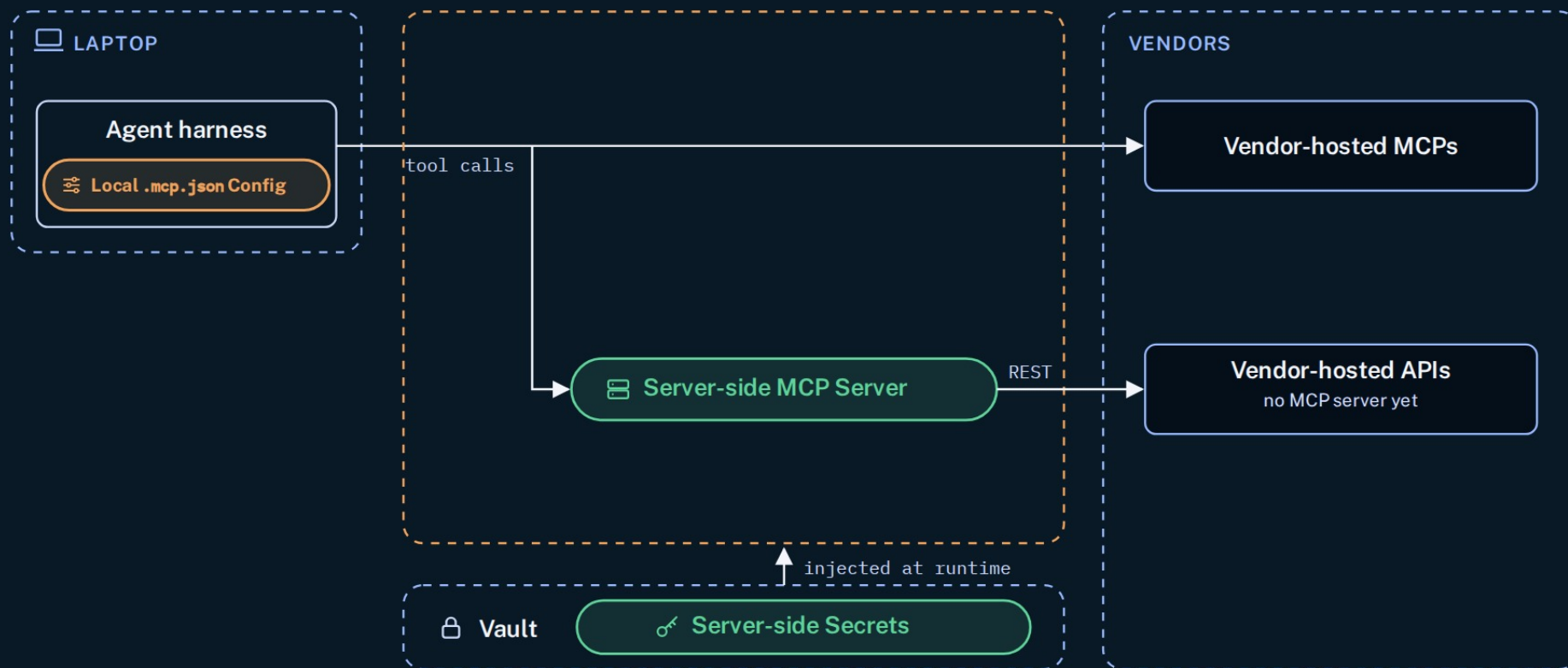
Every laptop was its own integration



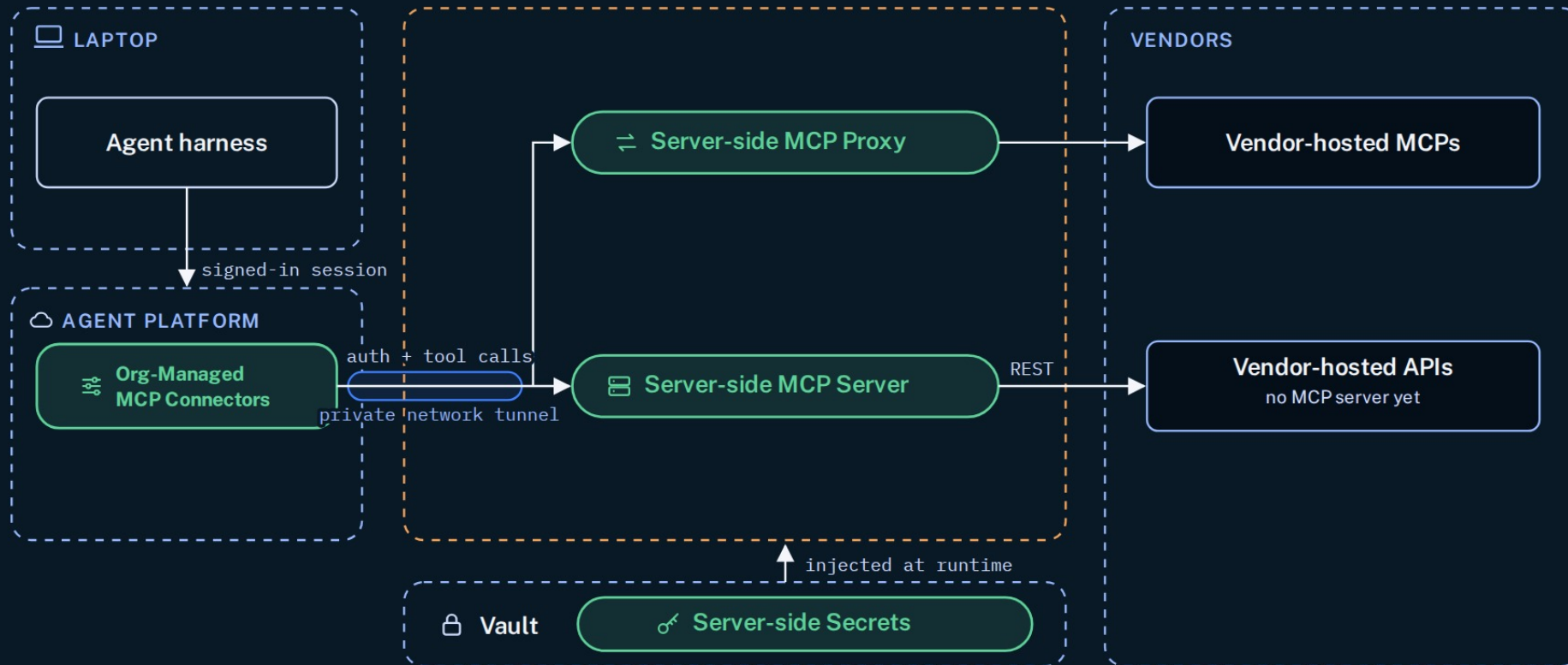
Run MCP servers server-side, not on laptops



Move secrets off laptops into Vault

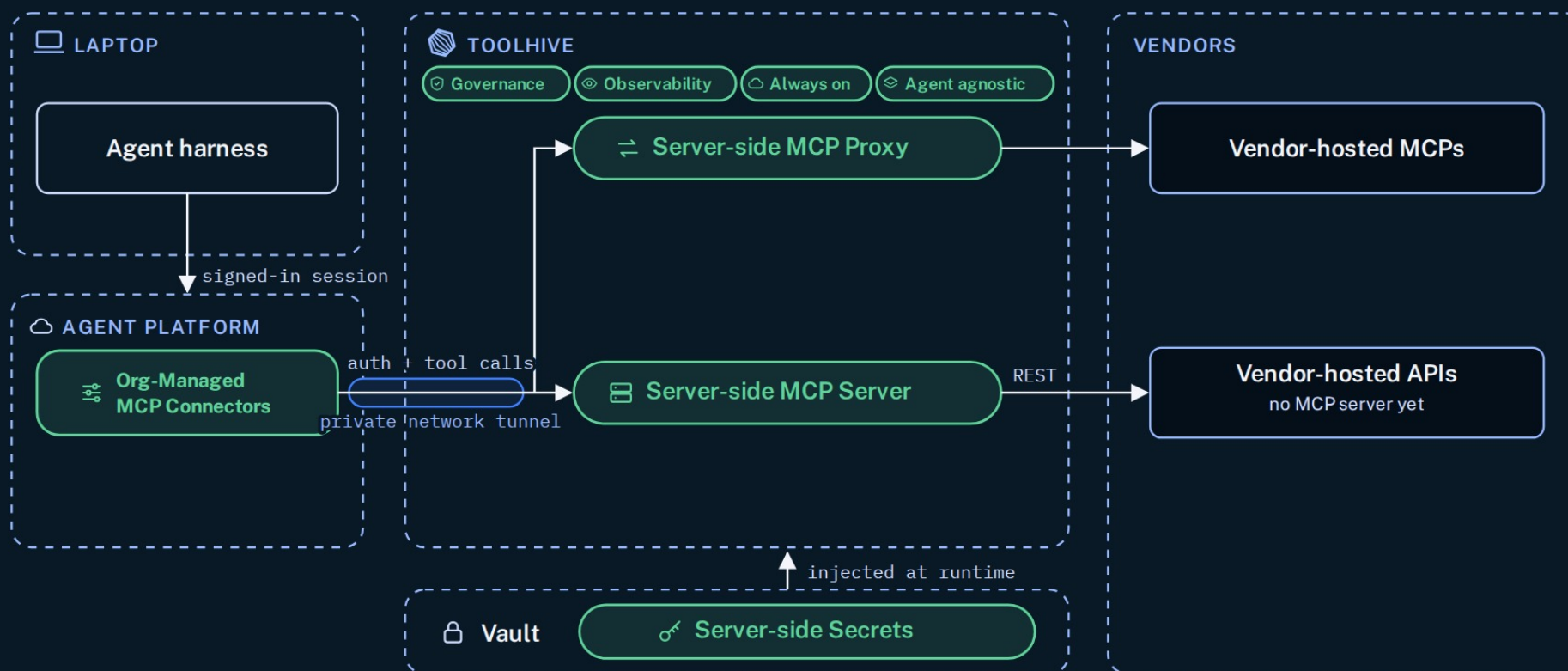


Configure MCP once for every agent



AFTER

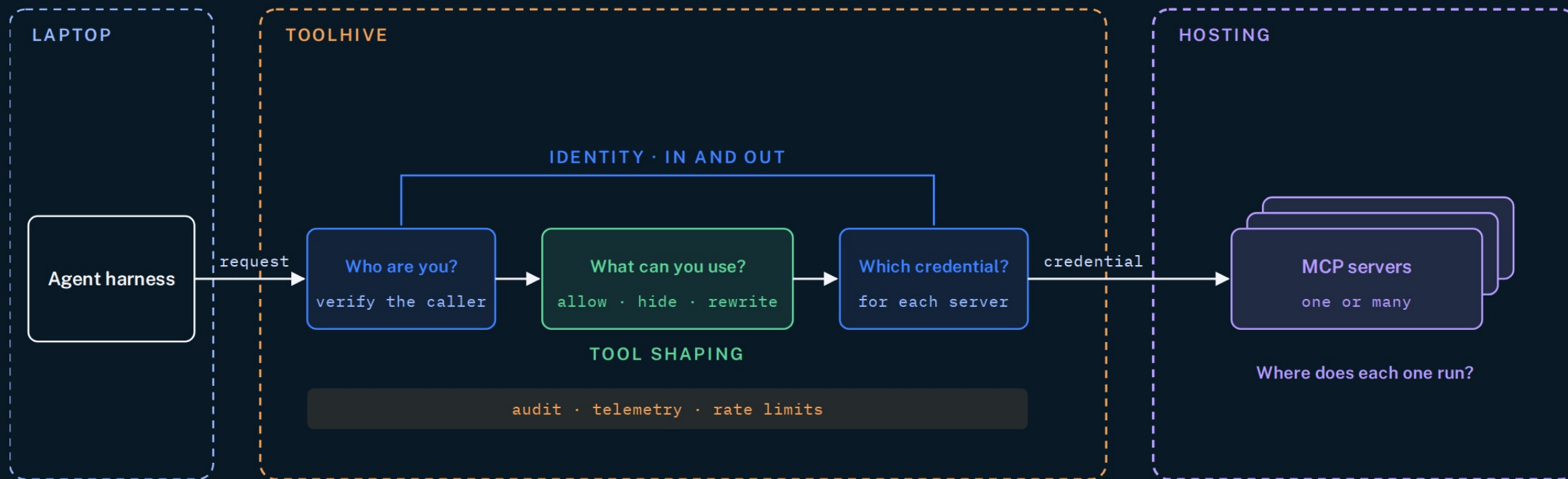
Scalable AI Platform built around ToolHive



Agenda

1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
- 3. The underlying open source technology: ToolHive**
 - Tool shaping
 - Identity
 - Hosting
4. Recap and takeaways

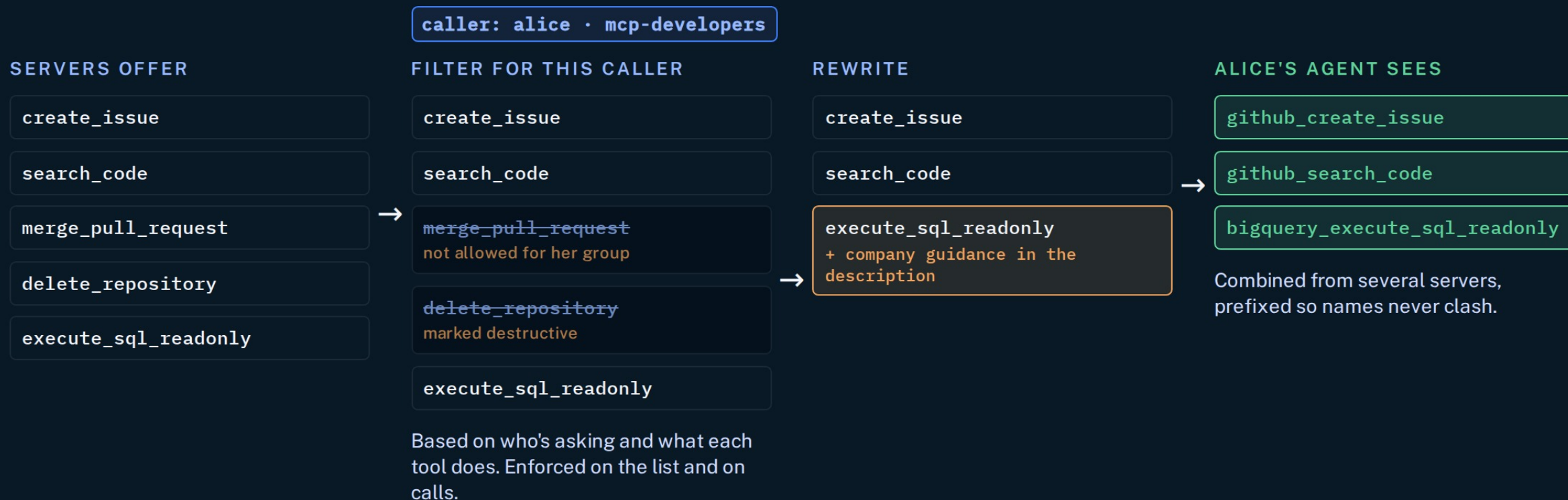
One request, three jobs



Agenda

1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
- 3. The underlying open source technology: ToolHive**
 - Tool shaping
 - Identity
 - Hosting
4. Recap and takeaways

Shape what each person's agent sees



Embed company best practices into your tool descriptions

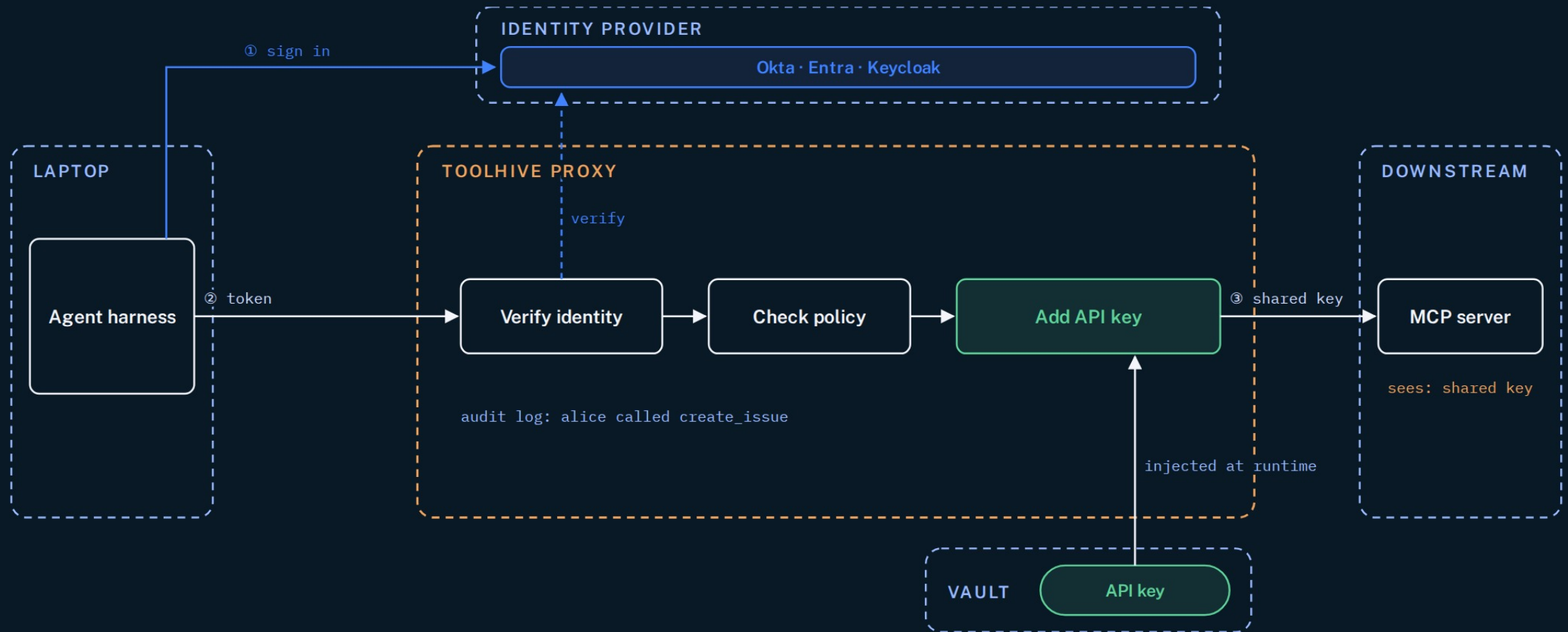
```
# MCPToolConfig · remote-proxy/bigquery-tool-config.yaml
toolsOverride:
  execute_sql_readonly:
    description: |
      <trm_guidance>
      Always set projectId to `trm-dev` unless told otherwise.
      It is the only project TRM users can create BigQuery jobs in. projectId
      selects where the job runs and bills. Queries may still read any table
      you have access to with fully-qualified project.dataset.table names.
      </trm_guidance>
      Run a read-only SQL query in the project and return the result...
```

Distribute company context through the protocol itself. Don't rely on agent skills for proper tool usage. Customize the tool description itself and every agent benefits.

Agenda

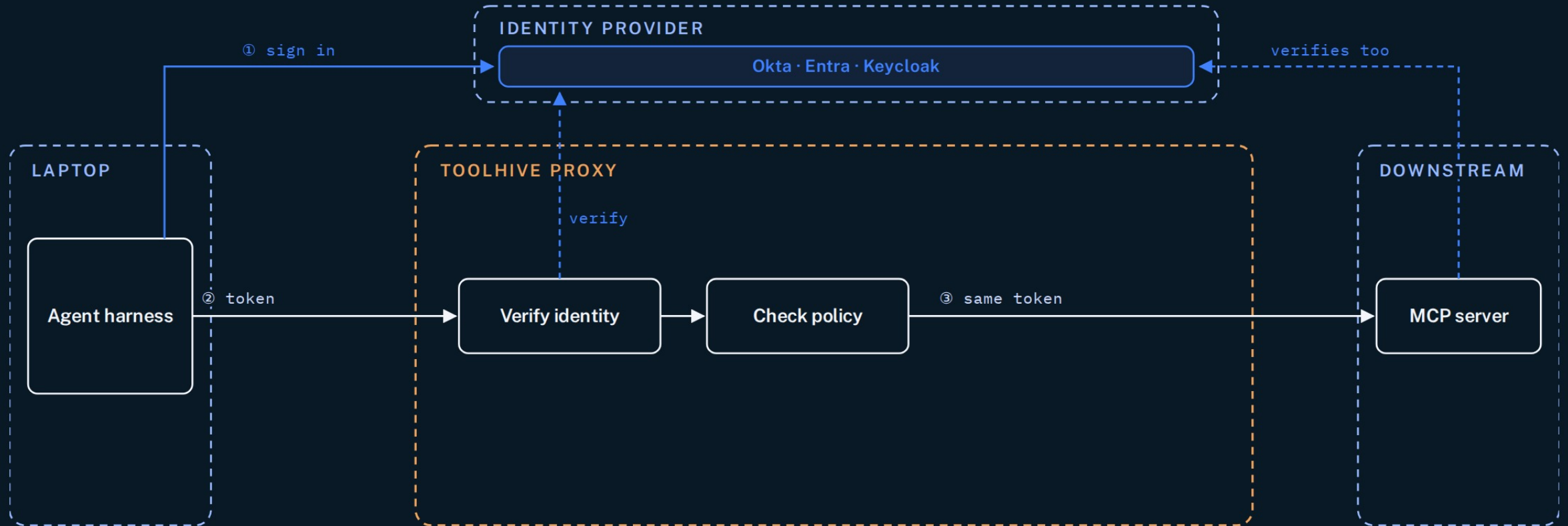
1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
- 3. The underlying open source technology: ToolHive**
 - Tool shaping
 - **Identity**
 - Hosting
4. Recap and takeaways

Known user, shared key



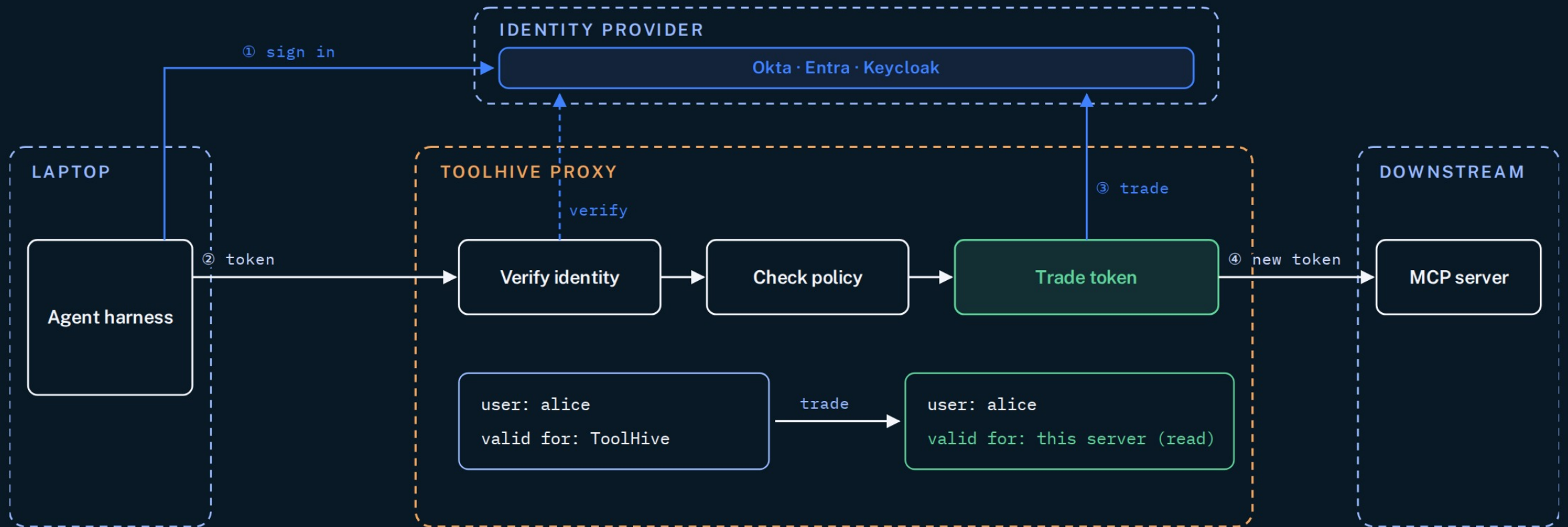
Works with any server. It sees one shared account.

Same token, both sides



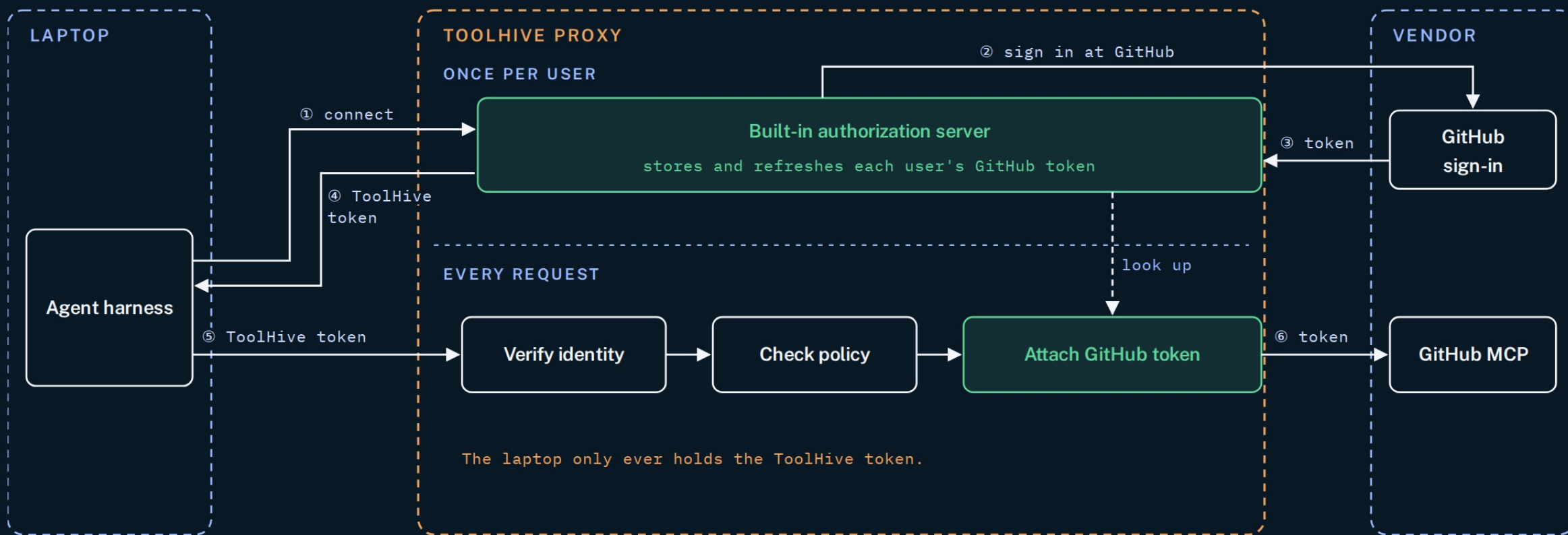
Simplest way to pass identity along. The server checks the same token.

Same identity provider, narrower token



The vendor only trusts its own sign-in

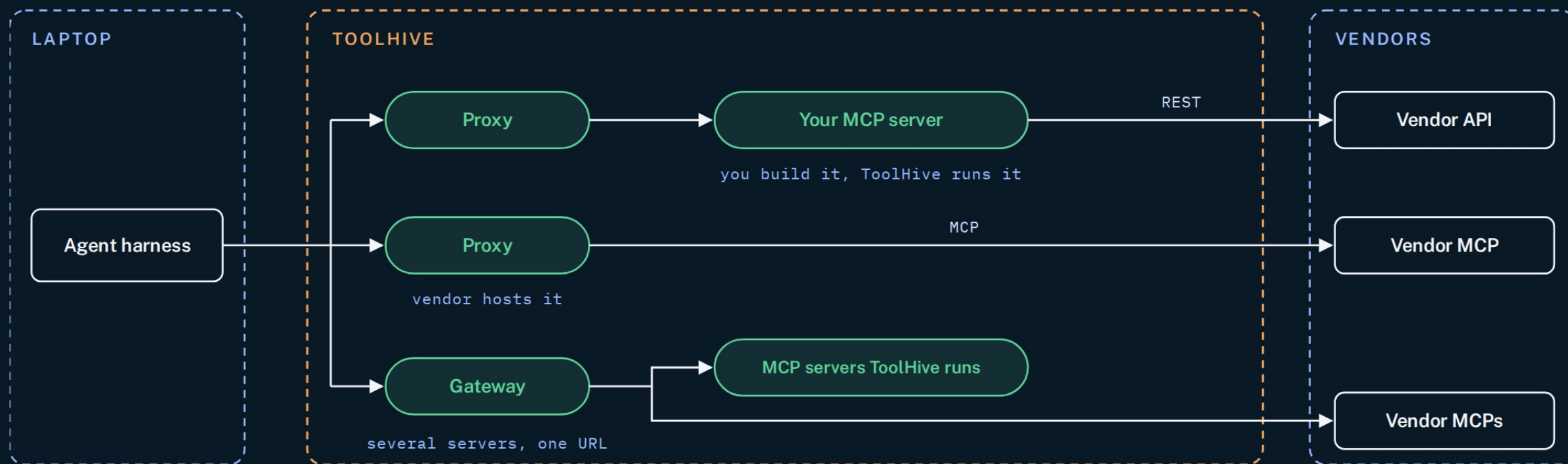
GitHub won't accept your corporate token, and won't trade it for one of its own. Each user has to sign in at GitHub.



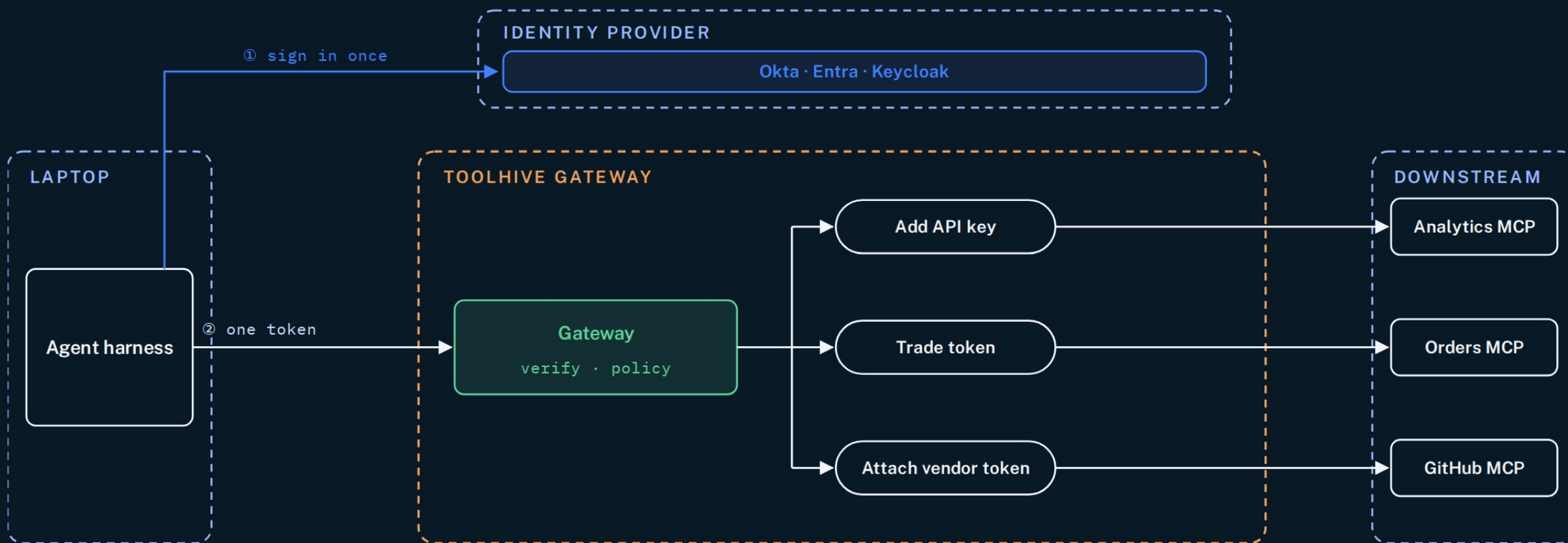
Agenda

1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
- 3. The underlying open source technology: ToolHive**
 - Tool shaping
 - Identity
 - **Hosting**
4. Recap and takeaways

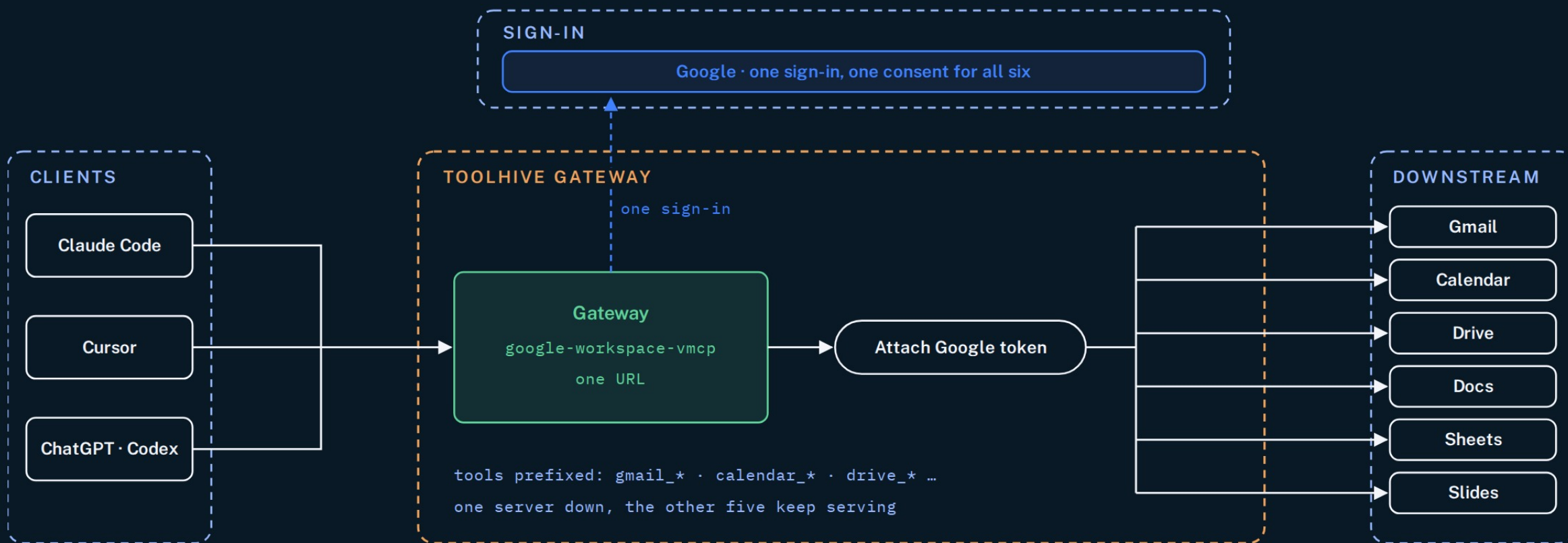
Two shapes: proxy and gateway



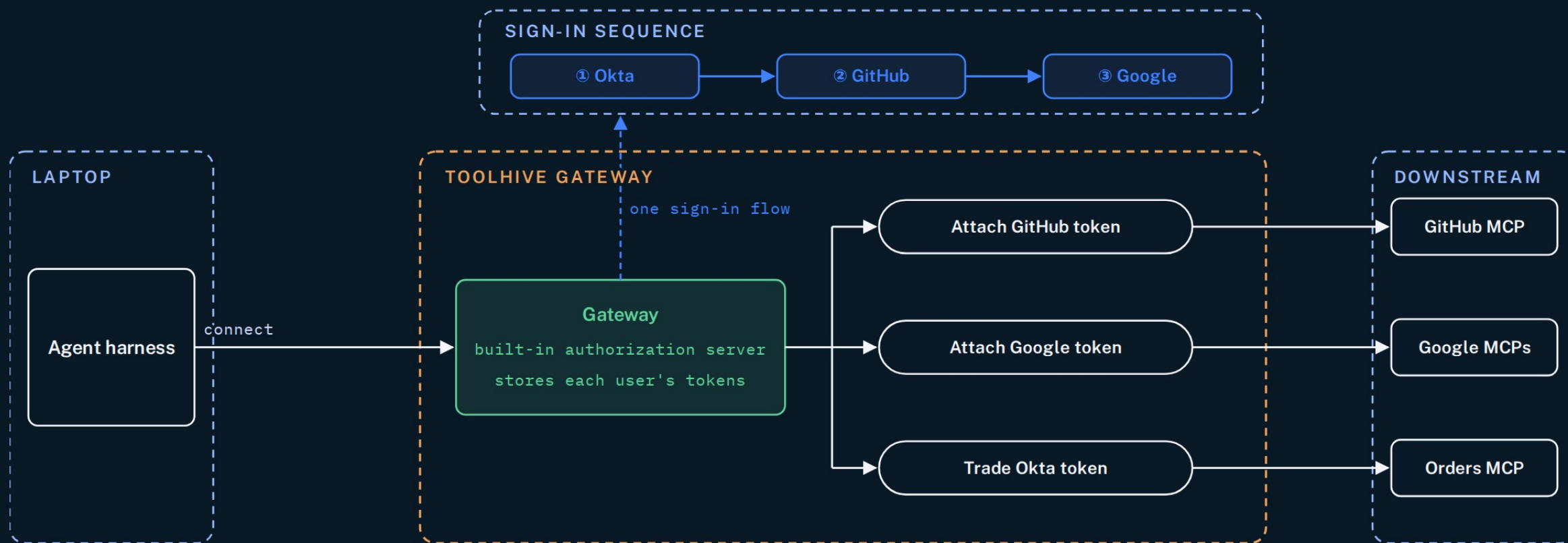
One endpoint, the right credential for each server



Consolidate multiple MCP servers behind a single auth flow



One sign-in, many vendors



Agenda

1. TRM and its AI adoption journey
2. Scaling challenges and how we fixed them
3. The underlying open source technology: ToolHive
- 4. Recap and takeaways**

One layer, three jobs

Tool shaping

Each person's agent sees only the tools it should.

Filter by who's asking and what each tool does. Rewrite descriptions to carry company guidance.

Identity

Verify the caller once. Give each server the credential it needs.

Pick a recipe per server, from a shared key to the user's own vendor token. Laptops never hold a credential.

Hosting

A proxy in front of one server, or a gateway in front of many.

Local or remote, behind one sign-in and one URL.

What TRM achieved with ToolHive, and what we learned

65

services and vendors available through ToolHive

- 1 **Delete the laptop-centric model.**
Run MCP servers and secrets behind ToolHive instead of on laptops, so every agent gets the same tools.

36,438

tool calls per day, on average

- 2 **Ship now, align later.**
Don't let vendors lagging on MCP block your org. Front their API yourself, then swap to their MCP behind the same endpoint.

94%

of all MCP tool calls go through ToolHive

- 3 **Empower your team to extend the platform.**
Adding a service is a pull request, and an agent skill writes it for you.

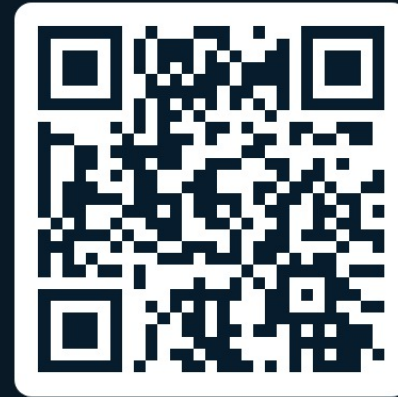
THANK YOU

Thank you, Toronto



Try ToolHive

github.com/stacklok/toolhive



Join TRM

trmlabs.com/careers

Andrew Hannigan · TRM Labs × Jeremy Drouillard · Stacklok

Case study: stacklok.com/case-studies/trm-labs