CLOUDFLARE

Control Plane for the Agentic Internet

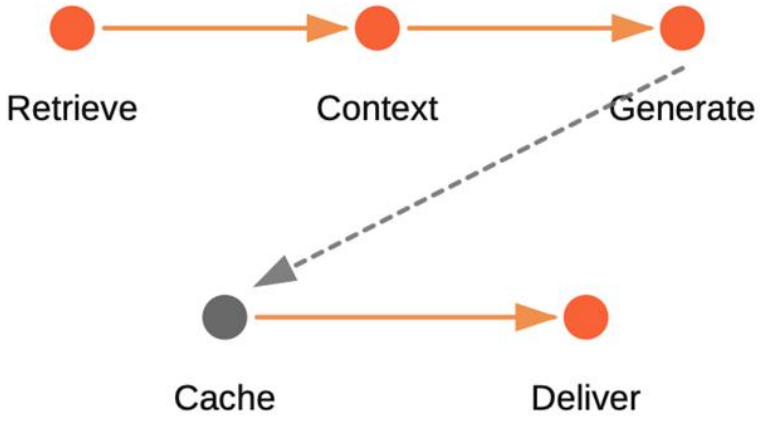
Anand Guruprasad
Customer Engineering Leader
Cloudflare Canada

CLOUDFLARE

Multi-user AI is still a hard engineering problem

A hard chain to preserve.

Identity alone does not carry item-level permissions end to end.



Define the enforcement boundary. Test its limits. State the residual risk.

Sources: The Agent Access Model • OS observer tracking (historical plan; limitations documented)

CLOUDFLARE

An approved route must also be a usable route

When the approved path feels harder, a shortcut becomes tempting.

Staff need

Find guidance.
Draft a response.

APPROVED ROUTE

Necessary controls, poorly joined up



UNAPPROVED SHORTCUT

Open a personal tool → paste → get an answer

Keep the controls. Remove avoidable friction. Make the safe route usable.

CLOUDFLARE

Three boundaries for trusted operations

SEE

Who may receive the information?



Sources • Recipients • Sharing

DO

What is it allowed to change?



Scope • Tools • Approval

DEFEND

Can we stop, investigate and recover?



Evidence • Containment • Recovery

Identity + policy + enforcement + evidence

CLOUDFLARE

Sharing has three different meanings



Share the recipe

Fresh state.
Explicit connections.



Share the live tool

Verify recipients.
Constrain future access.



Share the result

Apply release policy.
Transformation ≠ clearance.

> Shareability of software ≠ shareability of information.

CLOUDFLARE

Share the tool. Not the keys.

Software is reusable.

Authority must be explicit.



USE THE APP | SEE THE SOURCES | AUTHORIZE ACTIONS

CLOUDFLARE

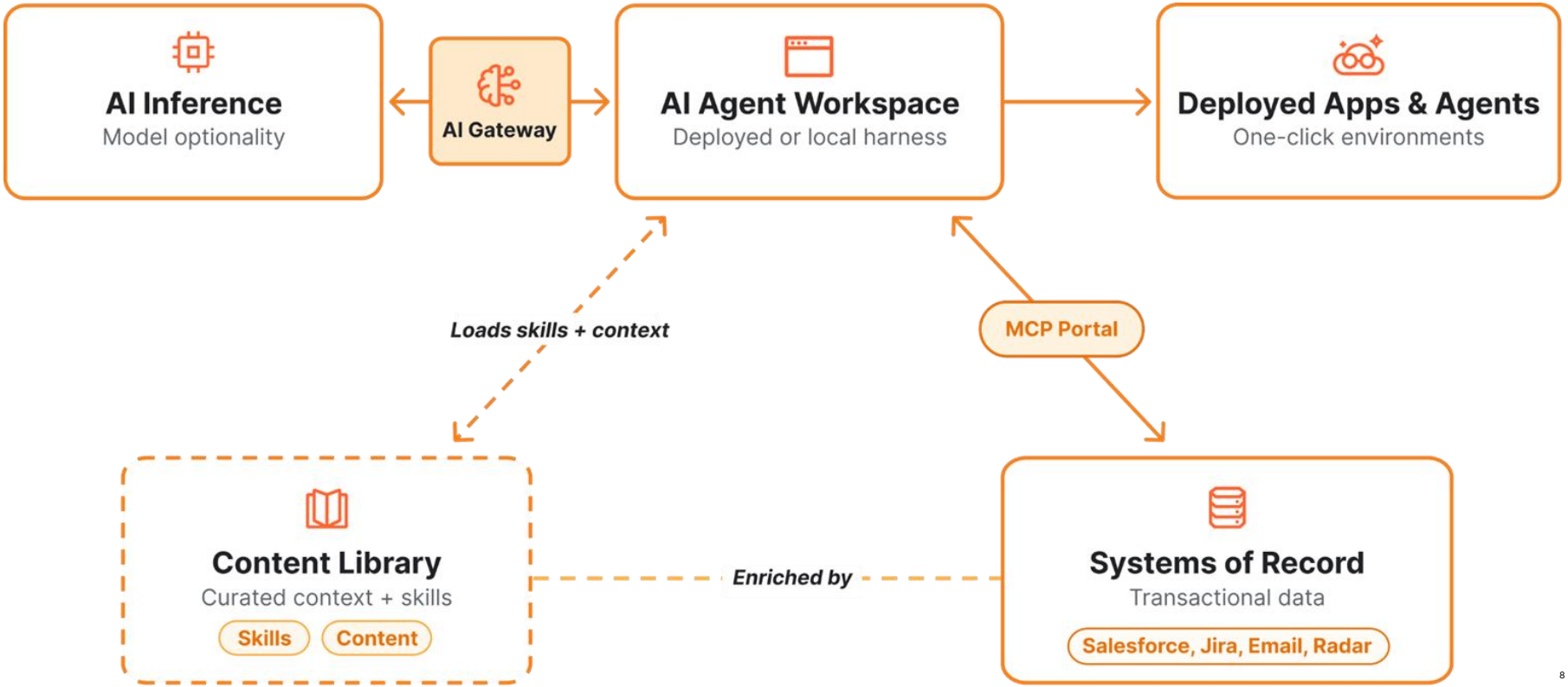
The agent needs a capability, not the credential



Constrain resources, operations, arguments and recipients.

Sources: Cloudflare OS architecture • Open-source repository

Cloudflare's agentic workspace



Equip and enable *every* team member to do more



One-Click AI Agent Workspace

Full agent harness running in a Cloudflare container available to every employee seconds after they start work. Build apps, outputs, and manage agents.



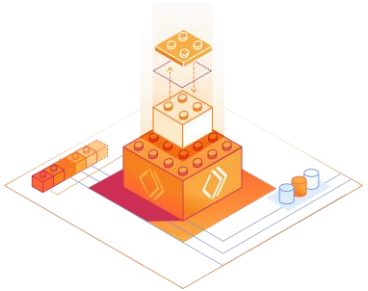
Centrally Managed Context Layer

Curate the jobs-to-be-done across the organization, and our institutional knowledge, into material that any team member can use in their workspace.



Secure System of Record Access

Provide access to critical data and systems of record across the organization while tightly scoping what a user can access and what they can do.



Model Optionality by Use Case and Role

Default to the right model by task or role to control cost without slowing down productivity gains.