Enabling the Resilient, Agentic AI Internet Era

Building the network, security, and platform the autonomous web depends on

Max Imbiel
Field CISO

Cloudflare · Network Strategy & Cloudflare One

Security Network Munich Meetup · July 25 2026 · Cloudflare

THE SHIFT

Agents are the new users of the Internet

Each era changed who consumes the web — and what the network underneath has to deliver.

Web 1.0–2.0

Pages & apps

Humans browse and click. Content is rendered for visual, cognitive parsing in a browser.

Cloud era

APIs & services

Software calls software. Programmatic access scales beyond a single human at a keyboard.

2026 →

Autonomous agents

Agents perceive, reason, and act — interrogating data layers and calling tools at machine speed.

Source: Cloudflare Research — Data Structure of the Agentic Web

1 prompt

...can fan out into hundreds of autonomous tool calls

Agents don't make one request and wait. A single goal triggers parallel, multi-step workflows — calling LLMs, MCP tools, and internal systems at machine speed.

Minutes–hours

Typical agent workflow duration

Untrusted code

Agent output is model-generated, not human-reviewed

Dozens of systems

CRM, ERP, ticketing, databases per task

WHAT IS AN AGENT?

An agent is a loop that runs on the network

Unlike a stateless API call, an agent maintains context and acts on the world over time.

PERCEIVE

Take a goal or prompt and gather context from data layers and tools.

→

THINK

Reason with an LLM to plan the next step toward the goal.

→

ACT

Call MCP tools, APIs, and internal systems — often writing or executing code.

→

OBSERVE

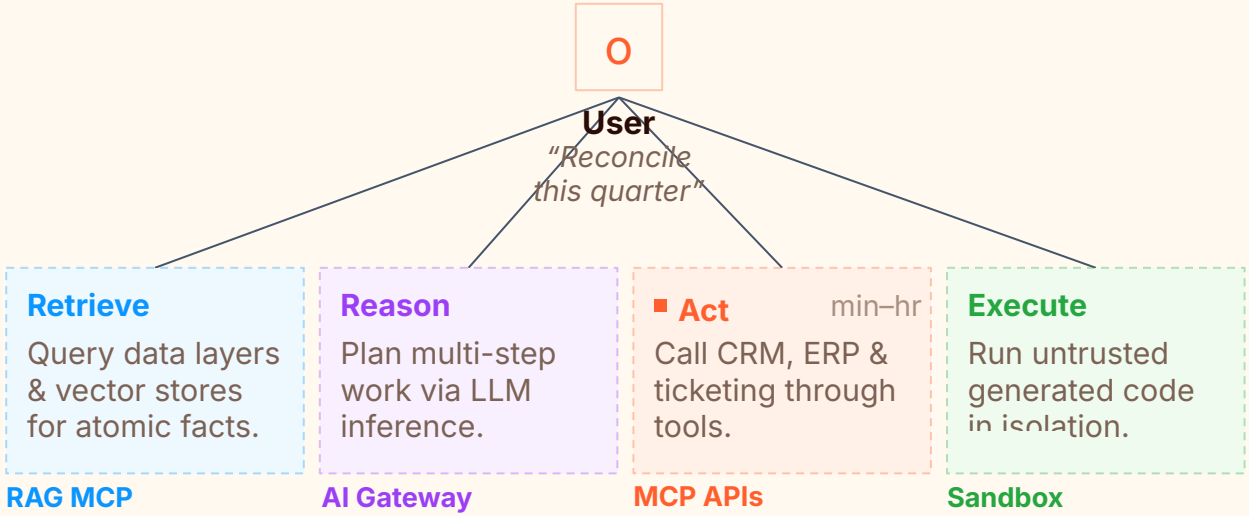
Persist state, evaluate results, and survive failures across long workflows.

Agents run untrusted code, need persistent state, call many external systems, and must survive failures

THE SHIFT

One goal, many concurrent workloads

This fan-out is why the agentic Internet stresses the network in entirely new ways.



Each branch is authenticated, rate-limited, and auditable — or it isn't. That gap is the opportunity.

01

THE FOUNDATION

Resilience is a property of every layer

Agents amplify everything: a single weak layer no longer slows one user — it stalls thousands of autonomous workflows at once.

THE FOUNDATION

What Internet resilience actually means

Resilience emerges only when every layer is redundant. Strength in one cannot offset weakness in another.

1

Physical

Diverse fiber corridors & cable landing stations — no single chokepoint

2

Network / Routing

Multi-homing, IXP peering, and RPKI to contain BGP misconfigurations

3

Application

Distributed caching, load balancing, and failover so no single node is essential

4

Socio-economic / Policy

Competition, multiple ISPs, and open peering reduce systemic single points of failure

Source: Cloudflare Research — What is Internet Resilience?

THE FOUNDATION

Resilience tiers, applied to our own network

Cloudflare's Multi-Colo PoP (MCP) architecture turns resilience into discrete, k-of-n engineering targets.

	MCP Lite	MCP Tolerant	MCP Resilient
Compute	**1-of-n colo** Maintenance on a server colo without re-routing all traffic.	**1-of-n colo** Parallel compute colos across the metro.	**1-of-n colo** Redundant server colos, diverse sites.
Edge routers	**1-of-1 edge** Single edge router per site.	**1-of-2 edge** Redundant edge routers, single site.	**1-of-2 sites** Edge routers split across two sites.
Survives	**Colo maint.** Planned maintenance windows.	**Device crash** Any single network device failure.	**Datacenter loss** Loss of a whole datacenter, no metro failure.

02

THE CONTROL PLANE

Securing the agentic web

Resilient pipes aren't enough. Agents introduce brand-new attack vectors — and most are deployed by engineers, outside IT's control.

THE CONTROL PLANE

The new risks customers are raising

Three months of customer conversations since MCP Server Portals launched — the recurring pain points.

Shadow MCP

MCP servers spun up by engineers

No central rollout, authn, or authz — unlike managed applications.

Prompt injection

New attack vectors

Prompt hijacking, untrusted data poisoning agent behavior.

OAuth sprawl

Proliferated tokens & grants

Hundreds of employees clicking consent grants they don't fully understand.

Agent ≠ human

Delegated permissions break down

Agents inherit user RBAC — without human judgment as a backstop.

No circuit breaker

Runaway cost & DoS

Looping agents can flood an MCP server or rack up a model bill.

Blind spots

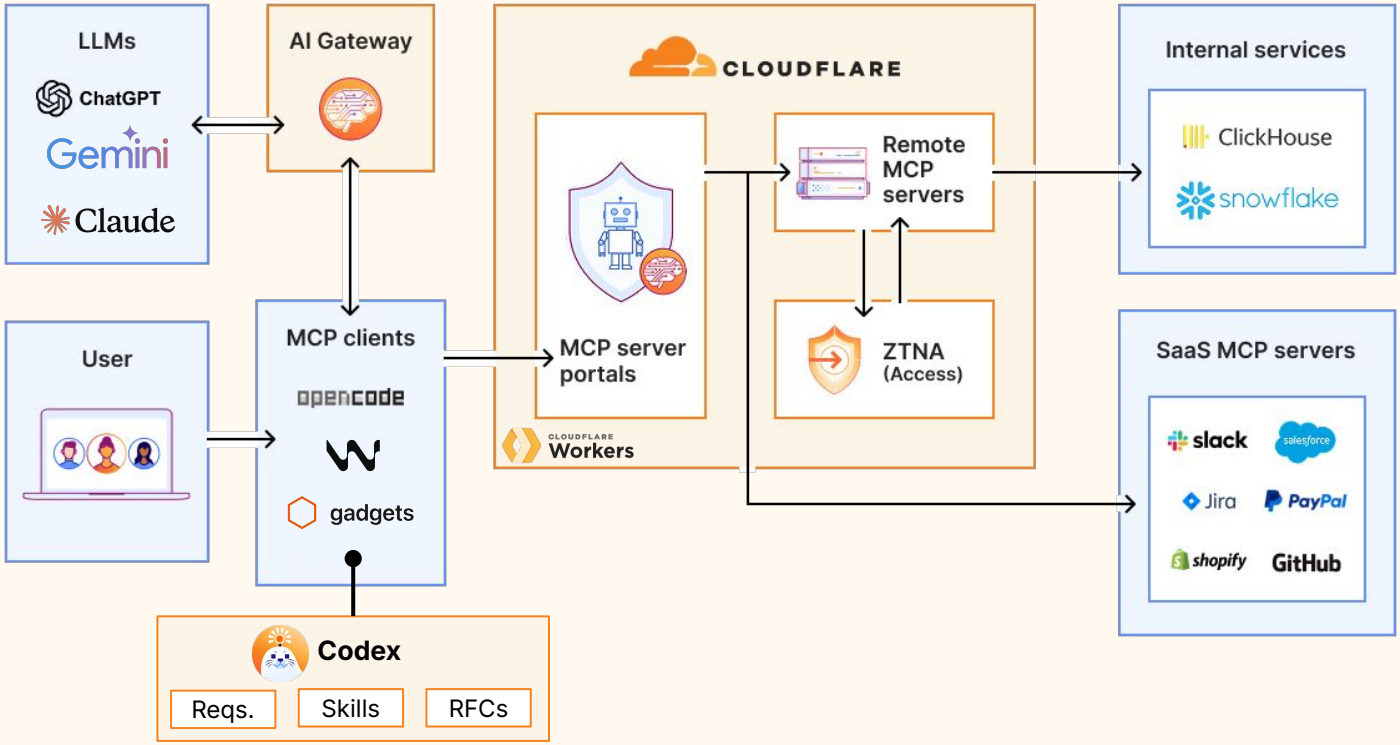
No data control

MCP servers have no native filtering or detection of sensitive data.

THE CONTROL PLANE

A reference architecture for agentic AI

Every hop between the agent and your systems becomes a control point Cloudflare can inspect, authenticate, and rate-limit.



WHY CLOUDFLARE

What agents need maps to products we already run

WHAT AGENTS NEED	CLOUDFLARE PRODUCT
Run untrusted agent code safely	**Workers + Sandboxes**
Persistent agent state & memory	**Durable Objects**
Route & cost-control model calls	**AI Gateway**
Inspect prompts & responses	**Firewall for AI**
Centralize & govern MCP servers	**MCP Server Portals**
Authenticate agents & users	**Access (OAuth)**
Control egress & sensitive data	**Gateway (SWG) + DLP**

03

THE OPPORTUNITY

Why Cloudflare wins this era

The agentic Internet needs one network that is resilient, programmable, and secure — at the same edge, in front of every request.

THE OPPORTUNITY

One network, three structural advantages

Agents touch the network on every step — and Cloudflare is already on that path.

1

Resilient by design

A multi-homed, RPKI-secured, MCP-tiered network engineered to survive datacenter loss without metro failure — the substrate agents run on.

2

Programmable at the edge

Workers, Durable Objects, and Sandboxes give agents compute, persistent state, and safe code execution next to every user, globally.

3

Secure by default

Firewall for AI, AI Gateway, MCP Portals, Access, and DLP turn every agent hop into an inspectable, governed control point.

The same edge that serves humans is already the chokepoint for agents.

WHAT THIS ENABLES

From assisted to autonomous

As resilience and controls mature, the human moves from operator to overseer — mirroring DNS's own evolution from one server to anycast.

TODAY

Assisted

Agents draft and recommend; controls log and coach. Portals centralize MCP usage.

HUMAN ROLE

Operator

Human approves every action

NEXT

Supervised

Agents act within policy guardrails. Firewall for AI and DLP gate sensitive steps.

HUMAN ROLE

Reviewer

Human in the loop on risk

HORIZON

Autonomous

Federated agents collaborate and self-route, with the network as the trust boundary.

HUMAN ROLE

Overseer

Human sets goals & limits

Source: Cloudflare ARC — RFC: Evolution of the Infrastructure Agent System

THE TAKEAWAY

Build the network the agents will depend on

Resilient at every layer. Programmable at the edge. Secure on every hop.
That is how Cloudflare enables the agentic AI Internet era.

```
$ npm create cloudflare@latest -- --template=agents
```

developers.cloudflare.com/agents Cloudflare One — MCP Portals Cloudflare Research

CLOUDFLARE

Thank you

enterprise@cloudflare.com
cloudflare.com/de-de