willow vs CLOUDFLARE

Willow vs. Cloudflare MCP Portals: different layers of the same problem

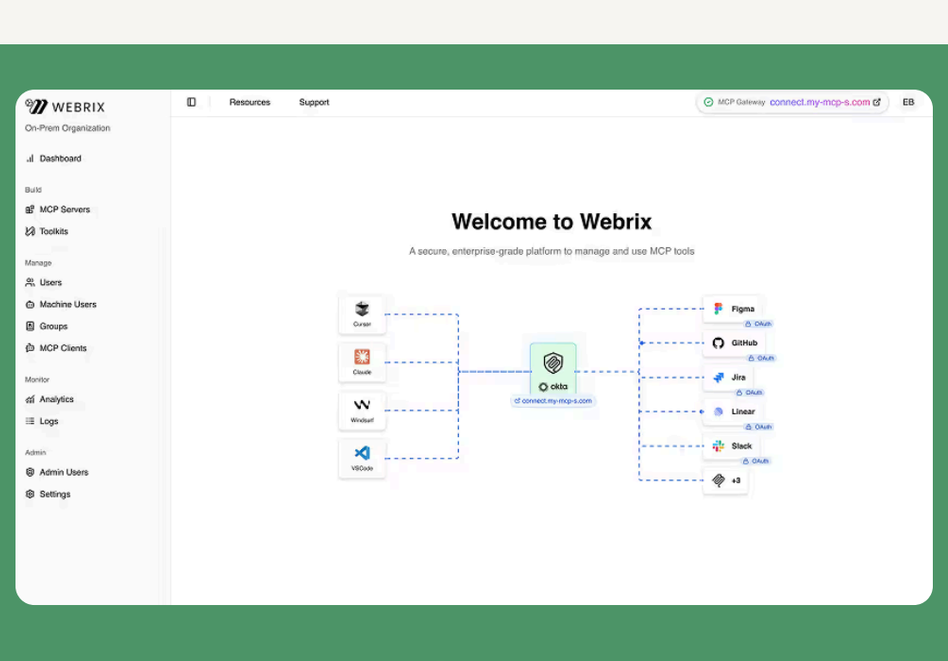
Cloudflare MCP Server Portals put the MCP servers you already run behind one governed endpoint, inside the Cloudflare One estate you already pay for. Willow is a purpose-built agent governance and enablement platform that deploys anywhere, including on-premises and air-gapped. Compare where each one fits, and where running both makes sense.

Get Started

Book a Demo

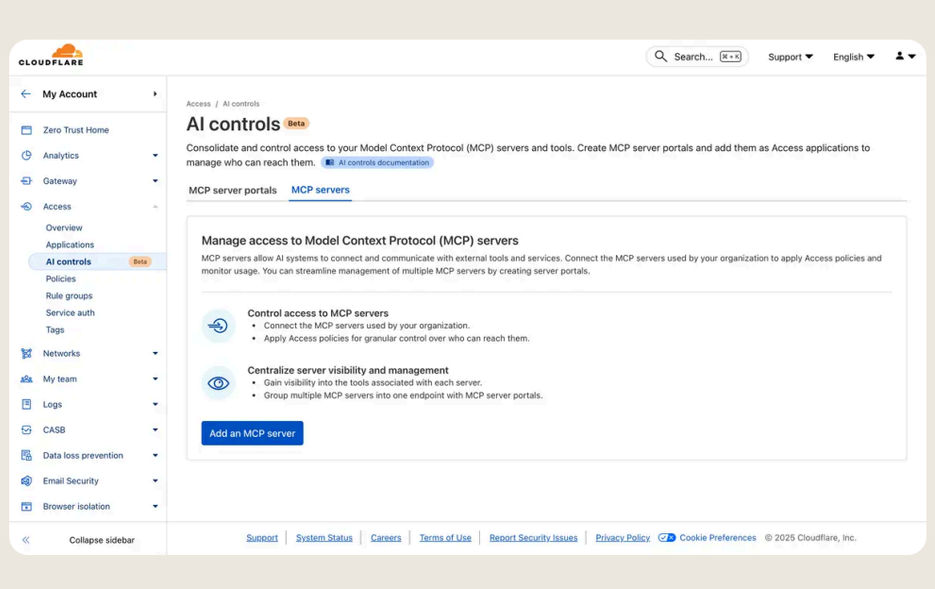
Trusted by

WIX agora papaya global innovi



Willow Admin Console

A purpose-built control plane for agent access and enablement across the organization. One product covering identity, a curated catalog, per-agent and per-action policy, endpoint discovery of unmanaged AI, employee self-service, and configuration as code. It deploys as SaaS, dedicated cloud, on-premises, hybrid, air-gapped, or with EU residency, and it is proven at Wix across roughly 5,000 weekly active users.



Cloudflare MCP Server Portals

A centralizing endpoint inside Cloudflare One that centralizes multiple MCP servers onto a single HTTP endpoint, with per-tool enable and disable, tool aliases, automatic namespacing, and Access policy in front. It is one layer of a reference architecture that also uses Cloudflare Access for identity, Gateway and DLP for shadow-MCP detection, AI Gateway for spend limits, and Workers for hosting MCP servers you build.

Where each one wins

Cloudflare leads on four of these. Willow leads on seven.

Cloudflare wins

Certifications

Cloudflare has been ISO 27001 certified since 2019 and currently holds ISO 27001:2022, ISO 27018:2019 since 2022, and ISO 27701:2019 as both a PII Processor and PII Controller since 2021. Cloudflare for Government has held FedRAMP Moderate authorization since 2022. Willow holds SOC 2 Type II and GDPR with EU data residency, and does not hold ISO 27001 today. If your procurement requires ISO certification or FedRAMP authorization, Cloudflare clears bars Willow does not.

Cloudflare wins

Price and scale

Portals were announced as available in Open Beta for all Cloudflare One customers, with up to 50 free seats to start, riding spend you already have rather than a separate agent-governance line item. The network behind it is something no startup matches.

Cloudflare wins

Cost enforcement

AI Gateway spend limits let you set cost-based budgets, and when cumulative spend reaches the limit AI Gateway blocks further requests with a 429 response until the window resets, with the option to route to a cheaper fallback model instead of blocking. Budgets can be split by model, provider, or custom metadata such as a user or team. Willow reduces the tokens each call consumes but does not set hard spend stops. On enforcement, Cloudflare is ahead.

Cloudflare wins

Hosting MCP servers

You can build and deploy MCP servers on Cloudflare: you extend the McpAgent class and serve it as a Worker, and each instance has its own durable state backed by a Durable Object with its own SQL database. If your team is building MCP servers rather than only consuming them, that is a platform Willow does not compete with.

Willow wins

Where it runs

Portals are part of Cloudflare's cloud. Willow deploys on-premises on AWS, GCP, or Azure, hybrid, air-gapped, or with EU residency, delivered as a managed service. For a sovereign, regulated, or disconnected environment, this is the difference between a shortlist and a non-starter.

Willow wins

What it can see

Cloudflare's shadow-MCP detection reads network traffic to find remote MCP servers outside of IT oversight. That is genuine discovery. What it cannot see is what never crosses the wire. Cloudflare's own documentation notes that MCP servers using stdio transport do not expose a remote HTTP endpoint and cannot be added to a portal, and those servers are equally invisible to network-based detection. Willow's endpoint scan agent finds local MCP servers, skill files, and agents on the device itself.

Willow wins

What you connect to

Adding a server to a portal means an administrator entering its URL. There is no catalog to pick from, no marketplace, and no vetting or risk scoring of the upstream server you point at. Willow ships 1,000+ pre-built, enterprise-vetted connectors and scores each server's security posture, so the question shifts from what URL do I trust to which approved tool does this team need.

Willow wins

The build layer above the catalog

Portals govern MCP servers and the tools they expose. Willow adds skills, plugins, toolkits, and commands on top, publishable and distributable to teams, which is a layer Cloudflare's MCP surface does not attempt.

Willow wins

Enabling people

Portals expect an administrator to register servers and a user to paste one URL into a client. Willow gives employees a Connect Panel and marketplace where they browse an approved, risk-scored catalog and connect any AI client in one click, with IT approving the catalog once.

Willow wins

Governance as code

Willow syncs toolkits, skills, commands, MCP servers, and clients to GitHub as version-controlled files with pull-request review and two-way sync. Cloudflare configures portals through the Cloudflare One dashboard and API.

Willow wins

Being one product

Cloudflare's MCP governance is assembled from Access, Portals, Gateway and DLP, AI Gateway, and Workers. Each is strong. Together they are a reference architecture you wire up and maintain. Willow ships the equivalent scope as a single platform.

Two limits worth knowing

These are in Cloudflare's own documentation and they matter if you are scoping a portal deployment.

Each portal supports up to 40 MCP servers, and only remote HTTP servers can be added, since servers that use stdio transport only do not expose a remote HTTP endpoint and cannot be added to an MCP server portal.

Some Access controls do not carry through the portal. Cloudflare documents that independent MFA, purpose justification, and temporary authentication will not be enforced for MCP servers authorized through a portal, and that AI prompt profiles do not apply to MCP server portal traffic. If those controls are part of your design, apply them on direct Access policies rather than assuming portal coverage.

The Bottom Line

Willow is a full-stack AI governance platform with shadow AI detection, unified build & runtime guards, infrastructure-as-code via GitHub, and a plugin marketplace for enterprise-wide governance. Cloudflare MCP Portals offers fast, cloud-only deployment with Zero Trust security for teams already in the Cloudflare ecosystem.

Cloudflare is the better fit when

You are already standardized on Cloudflare One, your MCP servers are remote HTTP endpoints, and what you need is to centralize and curate them behind Access policy without buying another platform. It rides spend you already have, its certifications are deeper than Willow's, and AI Gateway can enforce hard spend limits that Willow cannot.

Willow is the better fit when

Governing MCP access is one part of a larger job. It deploys on-premises, air-gapped, hybrid, or in the EU rather than only on a vendor's cloud. It discovers the AI on employee devices, including local servers and skill files that never cross the network. It ships a curated catalog with risk scoring, gives employees self-service, and manages the whole configuration as reviewed code in GitHub.

Run both when

You host MCP servers on Cloudflare Workers and want Willow governing how employees and agents reach them. These operate at different layers and do not conflict.

The layer map

Layer	Cloudflare	Willow
Identity in front of MCP	Cloudflare Access policies, with service tokens so automated systems can authenticate against Cloudflare One policies	OAuth 2.0, OIDC, SAML, JWT, SSO across Okta, Entra, JumpCloud, Google and more, with SCIM lifecycle
Governing MCP access	MCP Server Portals: aggregate, curate per tool, apply policy, log	The gateway: curated catalog, per-agent and per-action policy, guards, full audit
Sourcing what employees connect to	Admin enters each server's HTTP URL; no catalog, marketplace, or vetting of upstream servers	1,000+ pre-built, enterprise-vetted connectors with per-server risk scoring
Skills, plugins, and toolkits	Not offered; portals govern MCP servers and their tools	Skills, plugins, toolkits, and commands, published and distributed to teams
Discovering unmanaged AI	Gateway and DLP detect shadow MCP in network traffic, for remote servers	Endpoint scan agent finds local and remote MCPs, skills, and agents on the device, risk-scored
Enabling employees	Not addressed; an admin registers servers and users paste a portal URL	Connect Panel and marketplace, one-click self-service for any employee
Cost control	AI Gateway sets cost-based budgets and blocks or reroutes when exceeded	Token and context optimization, with usage analytics by team and tool
Hosting MCP servers	Build and deploy MCP servers on Cloudflare Workers via the McpAgent class, each backed by a Durable Object	Not offered; Willow governs consumption rather than hosting servers
Where it runs	Cloudflare's cloud	SaaS, dedicated cloud, on-premises, hybrid, air-gapped, EU residency

Deployment and sovereignty

Where the control plane runs, and who holds the data.

Willow approach

- Deploy as SaaS, dedicated cloud, on-premises on AWS, GCP, or Azure, hybrid with a stateless runtime pod local to you, or fully air-gapped.
- EU data residency is available.
- It typically goes live in about ten days.

Cloudflare approach

- Portals run on Cloudflare's global network as part of Cloudflare One.
- Portals run on Cloudflare's global network as part of Cloudflare One.
- The trade is that you inherit a global network, its latency profile, and its resilience.

Bottom line

This is the cleanest split on the page. If your security team requires the control plane inside your own environment, Cloudflare is not a candidate and Willow is. If you want someone else's global network doing the work, that is exactly what Cloudflare is for.

Discovering unmanaged AI

Finding what employees are already running.

Willow approach

- An endpoint scan agent deploys through Jamf, Intune, JumpCloud, or GPO and finds unmanaged MCP servers, skill files, and AI agents on the device.
- Coverage spans web and local usage, with risk scoring.
- A browser extension adds visibility into web AI usage and OAuth flows in managed Chrome.

Cloudflare approach

- Gateway and DLP detect shadow MCP in network traffic.
- Detection scans HTTP logs for MCP hostname and URL patterns and inspects POST bodies for JSON-RPC methods.
- This surfaces remote MCP servers outside of IT oversight, and they can be blocked.

Bottom line

Both discover unmanaged MCP. The difference is the vantage point. Cloudflare sees the wire, which is powerful for remote servers and blind to anything local. Willow sees the device, which is where stdio servers and skill files live. If your risk is a developer wiring a local MCP into a coding agent, that is an endpoint problem.

Employee enablement

Getting approved tools into people's hands without a ticket queue.

Willow approach

- Employees browse an approved, risk-scored catalog in the Connect Panel and marketplace and connect any AI client in one click.
- IT approves the catalog once and sets a per-user policy of none, needs-approval, or allow.
- When the identity provider deprovisions a user through SCIM, their access goes with them.

Cloudflare approach

- An administrator registers each MCP server in a portal and curates which tools are exposed.
- Users point their client at the portal endpoint.
- Tool aliases let you rename or re-describe tools, and namespacing prevents collisions across servers.

Bottom line

Cloudflare's per-tool curation is genuinely good. What Portals do not attempt is the enablement half: there is no catalog to browse, nothing to request, and no self-service path. That is a deliberate scope choice on their side, and it is the largest altitude gap between the two products.

Cost and token control

Two different answers to the same bill.

Willow approach

- Token Usage Analytics shows where tokens come from across MCP servers, toolkits, skills, and tool responses, by team, tool, and use case.
- The tool-response output format can be optimized to JSON Compact, CSV, YAML, or TOON.
- That cuts tokens returned on every call rather than capping what a person may spend.

Cloudflare approach

- AI Gateway spend limits set cost-based budgets calculated from token usage and model pricing.
- When a budget is exhausted, requests are blocked with a 429, or rerouted to a cheaper fallback model.
- Code Mode collapses tools into a single code tool and is documented as providing up to 5x savings in token usage with the minimize tools option.

Bottom line

Cloudflare wins this one. It enforces, and Willow does not. Willow's contribution is on the other side of the equation, reducing what each call costs in the first place. If a hard budget ceiling is the requirement, that is AI Gateway.

One platform or five

How much assembly the answer requires.

Willow approach

- Identity, catalog, policy, guards, discovery, self-service, audit, and configuration as code ship as one product.
- One console, one support relationship.
- Configuration syncs to GitHub with pull-request review.

Cloudflare approach

- The equivalent scope spans Access for identity, Portals for curation and policy, Gateway and DLP for detection, AI Gateway for spend, and Workers for hosting.
- Every piece is capable.
- Cloudflare's own guidance presents them as a reference architecture.

Bottom line

If you already run Cloudflare One and have a platform team comfortable wiring products together, the assembly is a reasonable trade for bundled pricing and a network you trust. If you want agent governance to arrive as a product rather than a project, that is the case for Willow.

Why enterprises pick Willow

> We are six to ten months ahead of most companies in AI adoption. More code to production, fewer incidents, real outcomes. Willow is what made it possible to move that fast without slowing down our security posture.

Asaf Yonay
Head of AI Core, Wix

WIX

Wix needed a secure, governed way to connect employees and agents to internal tools, documentation, and workflows. With Willow, the AI Core team built the enterprise MCP infrastructure that now supports nearly 600 tools and 300,000+ weekly tool calls across engineering, product, design, HR, finance, legal, and business teams.

60%
of enterprise AI rollouts stall on security review
Source: Gartner, 2025

84% / 91%
of developers use AI coding tools, with up to 91% of these tools unmanaged or unapproved by IT and security teams
Source: European Cyber Security Organization

Most
enterprises have no visibility into shadow AI usage
Source: IDC, 2025