✦ CuratedMCP

The system of record for Model Context Protocol

Platform Overview

Discover · Govern · Ship · Monetize

curatedmcp.com
founders@curatedmcp.com

Confidential
2026 edition

Executive summary

The Model Context Protocol is to AI agents what HTTP was to the web — the open standard that makes them genuinely useful. As of 2026, every major AI client (Claude, Cursor, Windsurf, OpenAI Agents, Gemini CLI, GitHub Copilot) supports MCP. The protocol won. But the infrastructure to use it safely, discover it easily, and monetize it as a builder still doesn't exist at scale.

CuratedMCP is the system of record for the MCP ecosystem. We help individual developers find and install MCP servers in seconds, give security teams a private registry with full audit trail, and let server builders distribute and monetize through one marketplace.

50+	6	80/20	SOC 2
Verified MCP servers	AI clients supported	Builder revenue split	Enterprise readiness

What's new this quarter: the Launcher — install MCP servers from inside Claude, Cursor, or Windsurf without ever leaving your editor. npx @curatedmcp/launcher · Free.

WHAT WE BELIEVE

Three convictions that shape the product

1. The protocol won; the infrastructure didn't. MCP adoption in 2026 mirrors HTTP in 1995. The standard exists, the clients exist, the servers exist — but discovery, governance, and monetization are still DIY. That gap is the entire opportunity.

2. Trust is the moat, not breadth. 12,000+ MCP servers exist across scattered directories. Buyers don't need more options — they need a curated, security-reviewed catalog they can actually deploy. Every server in our catalog passes a human review.

3. Distribution lives inside the AI client. Developers don't browse marketplace websites — they paste JSON into config files. The Launcher meets them there: one MCP server that finds and installs all the others.

Architecture

CuratedMCP separates the **control plane** (policy, audit, marketplace, RBAC) from the **data plane** (where tool calls actually execute). The control plane lives on CuratedMCP infrastructure. The data plane lives where it should — on the developer's machine, inside the enterprise VPC, or on the underlying SaaS API.

This separation is what makes us defensible. Competitors that host the data plane introduce latency, cost, and risk. We control the metadata and the policy — the parts where governance actually matters — and let the actual work happen at the edge.

CuratedMCP Architecture: Control Plane + Data Plane

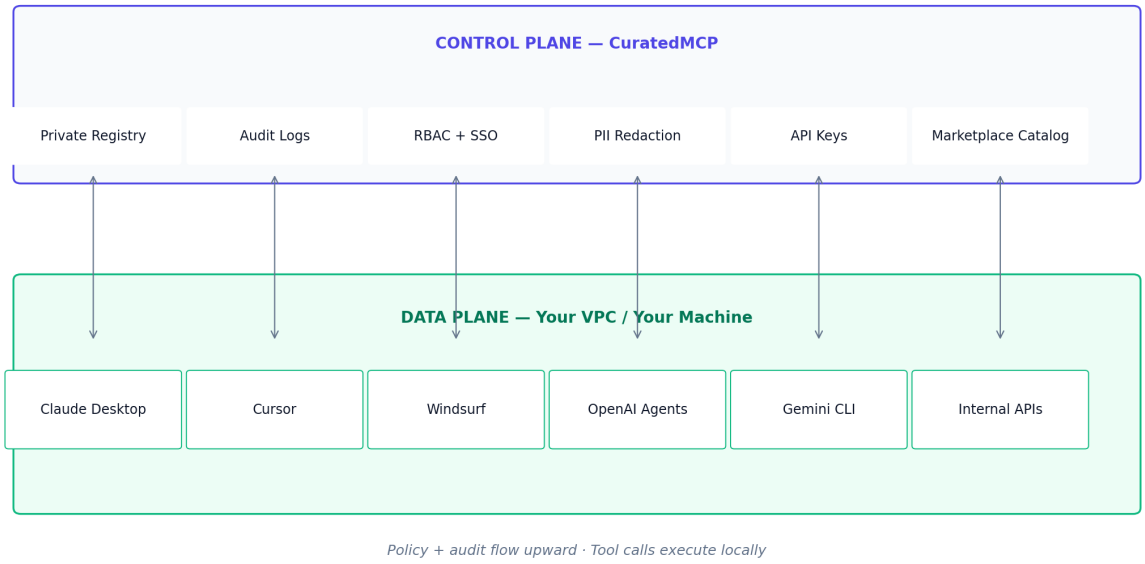


Figure: Control plane on CuratedMCP · Data plane stays at the edge.

THREE AUDIENCES, ONE PRODUCT

Who buys, what they buy, why they keep buying

One platform · Three audiences · Three revenue paths

ENTERPRISE

Platform & Security teams

- Private Registry
- Governance Suite
- Audit logs · SSO · SCIM
- API Converter (internal)

$500 → custom

Govern AI tool sprawl

DEVELOPERS

AI builders & engineers

- Launcher · Marketplace
- Builder · Auditor · Sentinel
- Config Editor · Playground
- Private Counsel · Tool Pass

Free → $9–49/mo

Ship agents in minutes

BUILDERS & PARTNERS

Sellers, agencies, researchers

- Stripe Connect · 80/20
- Certified Badge
- Agency directory
- Whitepaper · Learn

Free → 80/20 rev-share

Distribute & monetize

Figure: Land at zero · expand into pro tools · convert to enterprise.

For Enterprise

Stop chasing rogue MCP configs across GitHub repos and internal wikis. Get a single, governed catalog with RBAC, audit logs, and instant revocation.

The shadow MCP problem

Every developer in your organization is now adding MCP servers to their Claude Desktop or Cursor config. Without governance, your credentials, customer data, and source code are flowing through tools nobody on the security team has reviewed. The growth curve is exponential — left alone, mid-size orgs reach 100+ unverified servers within a year.

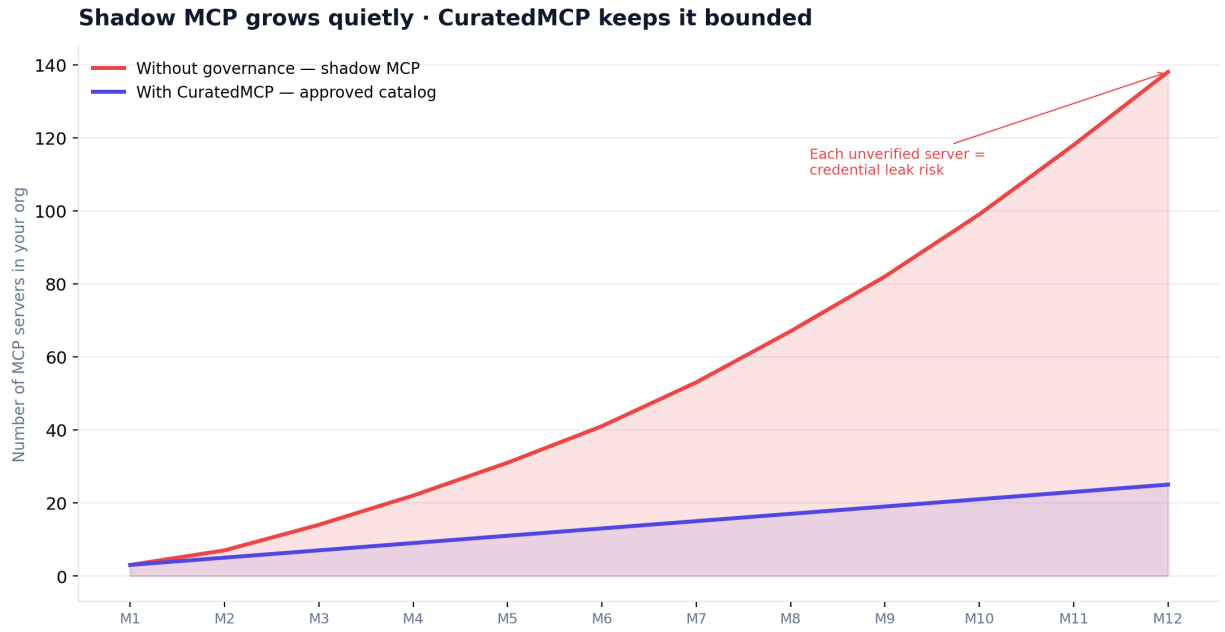


Figure: Modeled growth of unverified MCP servers in a 200-person org without governance.

What we deliver

- **Private MCP Registry.** Namespaced, npm-style registry — every team installs from one approved catalog. RBAC, scoped API keys, instant revocation.
- **Governance Suite.** Pre-approved server catalog · read-only filtering · Team Config URL (one URL for the whole org) · PII auto-redaction in audit logs.
- **Internal API Converter.** Turn any internal OpenAPI spec into a governed, hosted MCP server in 30 seconds. Zero one-off integration projects.
- **Compliance posture.** SOC 2 readiness · audit log export to SIEM · SSO/SAML (Okta, Azure AD) · SCIM provisioning · 730-day retention · SLA + named support.

30-day pilot, no commitment. Procurement pack delivered Day 1 (DPA, SSO checklist, audit-log sample). Onboarding within 5 business days. curatedmcp.com/enterprise/pilot

For Developers

Skip the JSON-config rabbit hole. Find the right MCP server, install it in 30 seconds from inside your editor, and ship.

The Launcher (NEW)

Find and install MCP servers from inside Claude, Cursor, or Windsurf — no copy-paste JSON, no GitHub hunting. Add one line to your config, then ask the assistant to find a server.

```
"curatedmcp": { "command": "npx", "args": ["-y", "@curatedmcp/launcher"] }
```

The full developer toolkit

Tool	What it does	Price
Launcher	Install MCP servers from inside Claude/Cursor/Windsurf	**Free**
Marketplace	50+ verified servers · 6-client install configs	**Free**
Agent Builder	Describe goal → get personalized MCP stack + playbook	**Free**
MCP Auditor	CLI scans configs for credential leaks & risky servers	**Free / $9 Pro**
Sentinel	Local stdio firewall — intercept every tool call, enforce policy	**$19.99/mo**
Private Counsel	Local RAG over your docs · LanceDB · offline embeddings	**$29/mo**
Sovereign Suite	Auditor Pro + Private Counsel bundle	**$49/mo**
Config Editor	Visual editor across 6 MCP clients	**Free**
OpenAPI → MCP	Paste any OpenAPI URL · get a working MCP server in 30s	**Free**
Tool Pass	Hosted endpoint w/ web search, weather, news	**$9/mo**

Discovery surfaces complete the picture: **Templates** (pre-built agent role configs), **Stacks** (community-shared bundles), **Compare** (side-by-side server comparison), **Playground** (test any server in browser before installing), and per-server × per-client **Install Guides**.

For Builders & Partners

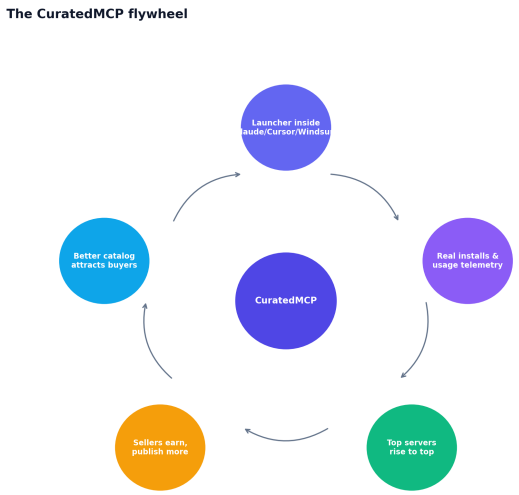
Publish, distribute, and monetize MCP servers through a single funnel. Builders keep 80%. We handle Stripe, hosting, certification, and discovery.

How builders earn

- **Stripe Connect onboarding.** Automatic payouts. No manual invoicing. Listing analytics, reviews, support inbox in your dashboard.
- **Certified Program.** Annual security certification — code review + dependency scan + behavior analysis + 'Certified by CuratedMCP' badge that unlocks enterprise procurement.
- **Agency Programme.** Tiered partner directory + intake for agencies deploying MCP for clients. Rev-share on referred enterprise deals.
- **Playbooks marketplace.** Sell pre-built MCP stack guides — ready-to-use configurations for specific use cases.

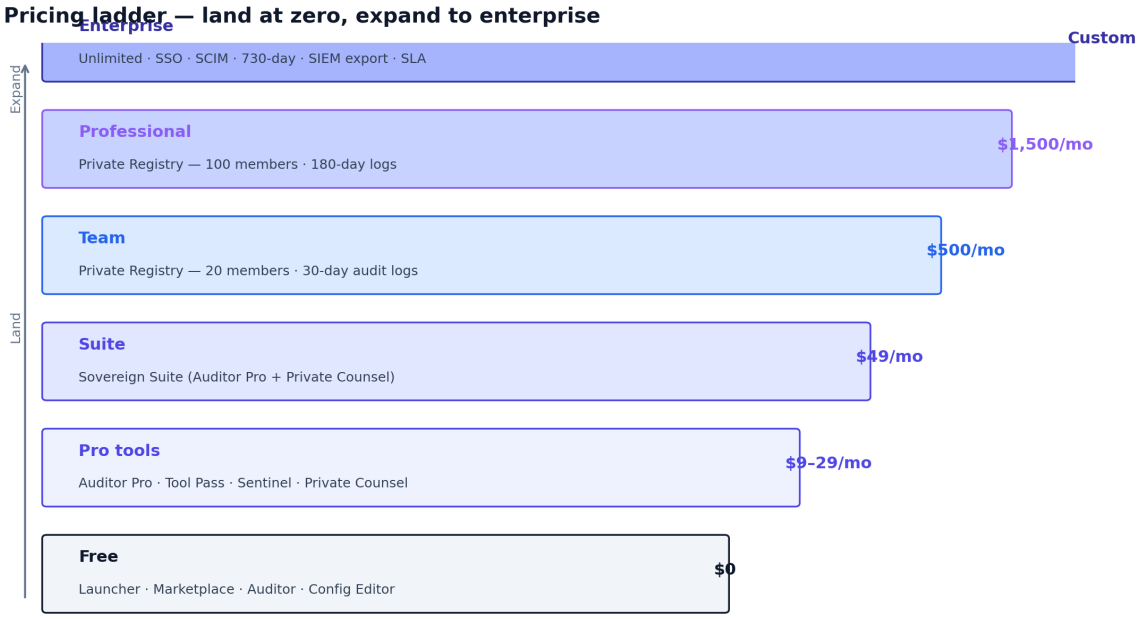
The flywheel

The Launcher is the engine. Every install is daily-active distribution. More installs surface better servers. Better servers attract more buyers. More buyers attract more sellers. More sellers grow the catalog. Every loop strengthens the next.



Pricing — land at zero, expand to enterprise

Free tier earns trust. Pro tools convert individual buyers. Team and Enterprise tiers capture the budget where MCP governance actually lives.



Where we sit in the market

Existing MCP directories optimize for breadth — listing every public server they can scrape. We optimize for the trust-and-breadth quadrant: wide enough to be useful, curated enough to be deployable.

Competitive landscape — MCP marketplaces, end of 2026



Why now — and why us

WHY NOW

MCP went from beta protocol to industry standard in 18 months. Every major AI client now supports it. Enterprise security teams are starting to ask 'who approved this MCP server?' — and getting no good answer. The market moves from experimentation to governance in 2026. The company that owns the trust layer wins the decade.

WHY US

We are the only platform that serves all three audiences at once: individual developers (Launcher, Marketplace), security teams (Private Registry, Audit), and builders (80/20 split, Certified). Each audience reinforces the others. Developers create the user demand that pulls enterprise procurement. Builders supply what both want. Security review of every listing is the trust anchor that makes the rest credible.

Get started

Enterprise / Security teams — curatedmcp.com/enterprise/pilot

Developers — curatedmcp.com/launcher · curatedmcp.com/marketplace

Builders — curatedmcp.com/dashboard/seller-setup

Press & investors — founders@curatedmcp.com

The protocol won. The infrastructure is being built right now. Be one of the people building on it — or governing it — before it reaches everyone else.