

THE PLUMBING OF THE AI AGENT ECONOMY

MCP and the infrastructure layer beneath autonomous AI



August 2026



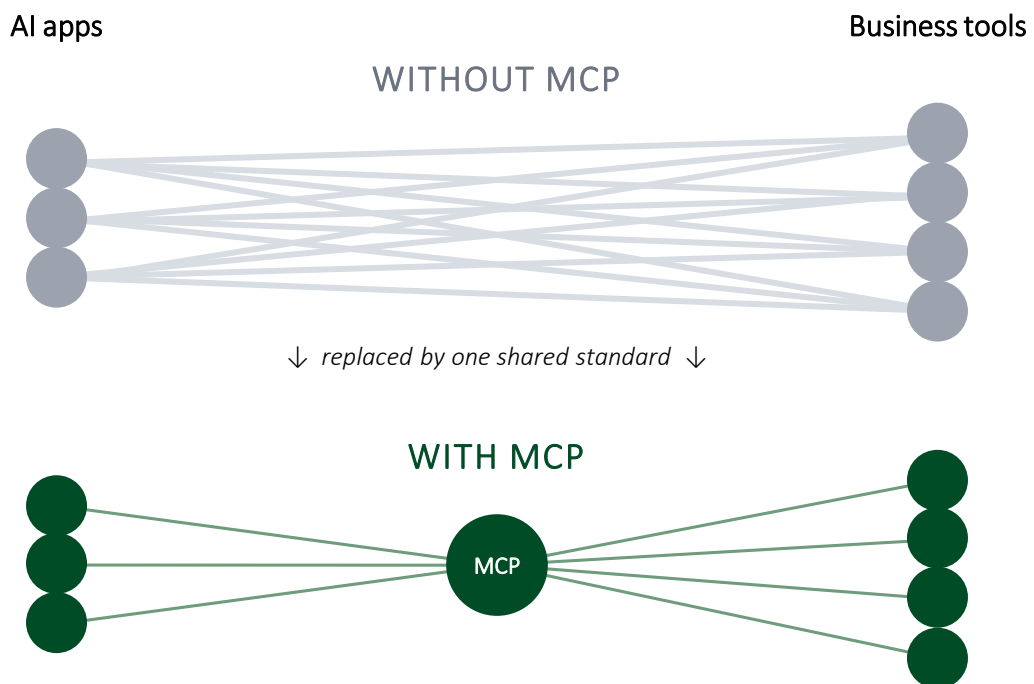
SECTION 01

What Is MCP, and Why It Plays a Vital Role



An AI chatbot on its own can only talk - it can't check a calendar, pull a number from a database, or send an email. Connecting it to real tools by hand doesn't scale: 10 AI apps and 100 tools could mean up to 1,000 custom connections, each needing upkeep forever. MCP is the shared set of rules that removes that problem - not a product or an app, but a common language.

Figure 1 - The Same Connections, Before and After a Shared Standard



Building each of those connections by hand is expensive. If you have 10 AI applications and 100 business tools you want them to reach, the old approach could require up to 1,000 separate custom connections - each one written by an engineer, each one needing maintenance forever.

THE CORE IDEA

MCP is not a product, an app, or something you buy - it's a shared language, closer to a common electrical-plug standard than to a piece of software.

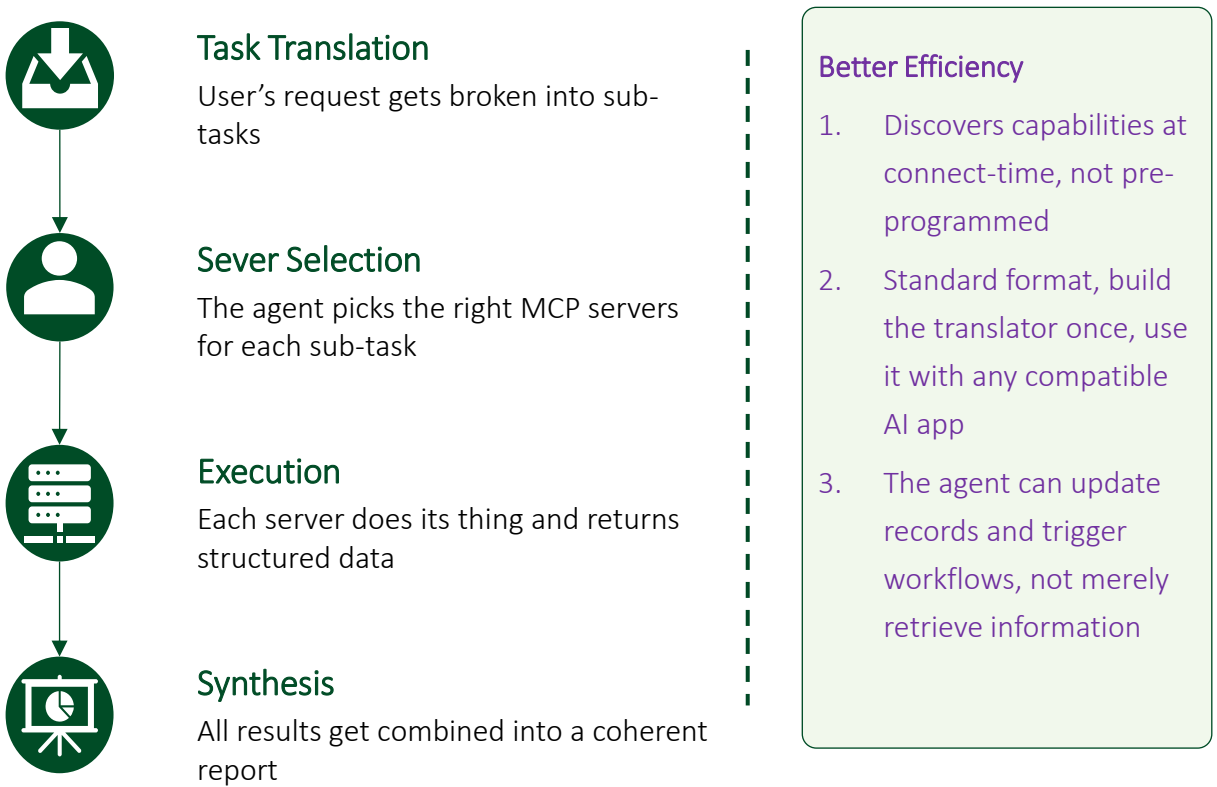


How MCP Actually Works, Step by Step



Think of it as a conversation between two parties: the AI application a person is using - a chatbot, a coding assistant, an internal tool - and a small translator program sitting in front of each business system it needs to reach.

Figure 2 - The MCP Workflow



WHY THIS IS DIFFERENT

This isn't the same as loading a document into the chat. MCP lets an AI fetch fresh information on demand - and take actions, not just read them. An AI handed a customer file can describe the customer; one connected through MCP can update the record.



SECTION 03

Who Controls MCP



Anthropic created MCP and released it in November 2024. In December 2025 it gave the standard away: Anthropic, Block, and OpenAI founded the Agentic AI Foundation under the Linux Foundation, so the agent ecosystem wouldn't splinter into competing formats.

Foundation Membership, by Tier

BOARD-SEAT MEMBERS



ADDITIONAL MEMBERS



170+ member organizations as of April 2026

WHAT THIS MEANS COMMERCIALLY

When eight companies that compete fiercely with each other agree to govern something jointly, that thing has stopped being anyone's competitive advantage - it's become shared road, not private property.



SECTION 04

The Fastest Adoption Curve in AI Infrastructure



**97 MILLION
INSTALLATIONS**

MCP passed on 25 March 2026. For perspective, React took roughly three years to reach 100 million monthly downloads - MCP reached a comparable scale in about sixteen months.

Time to Reach ~100 Million Downloads / Installs

MCP

16 months

React

36 months

170+

Foundation members, April 2026

110M

Downloads per month, April 2026

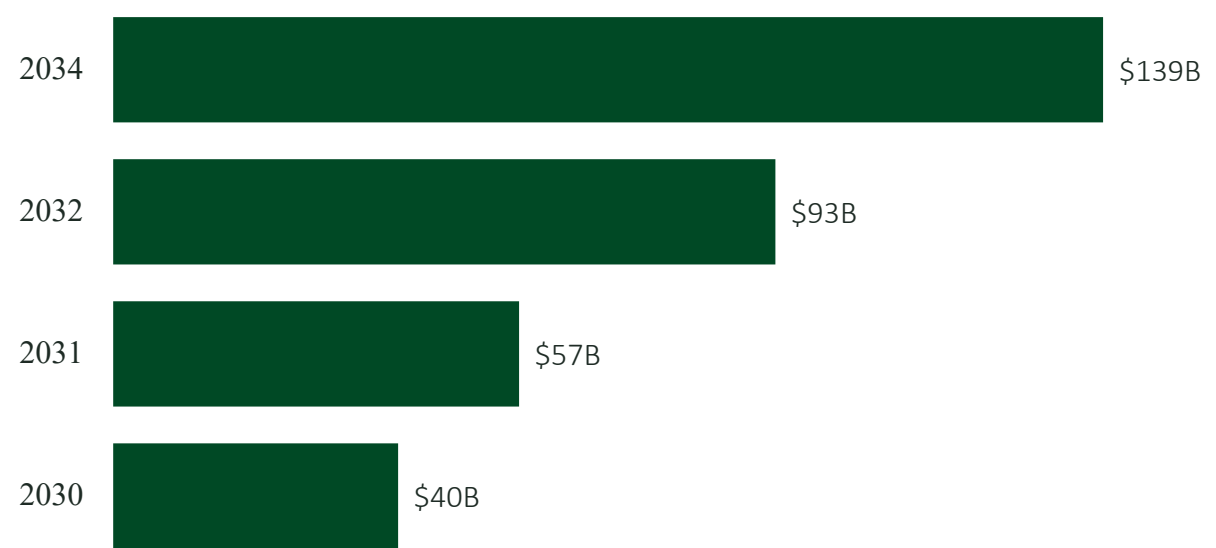


Why Now, and How Fast Is It Growing



Worldwide AI spending is forecast at \$2.52 trillion in 2026, up 44% year over year - mostly data centers, chips, and services. Within it, Gartner projects \$201.9 billion spent specifically on agentic AI in 2026, overtaking chatbot spending by 2027. Narrow further to software built purely to run AI agents, and five major research firms disagree sharply on where it lands - though all agree it's growing at a tight 40-45% a year.

Figure 2 - Forecast Market Size for Agentic AI Software



WHY ANYONE BELIEVES THE GROWTH

McKinsey estimates AI agents could add \$2.6-4.4 trillion of value annually across business use cases. Companies that have finished a deployment report strong returns - Deloitte puts the average at 171% return on investment, rising to 192% in the United States, roughly triple what conventional automation delivers.

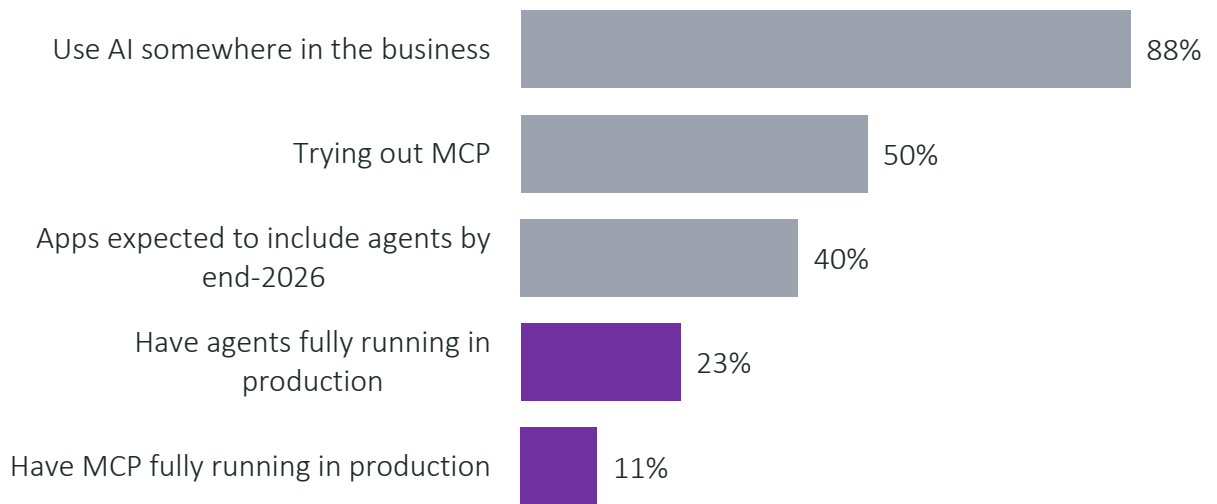


The Most Important Number in This Market



Demand is not the constraint - getting the technology to work in production is. Nearly nine in ten organizations use AI somewhere, and Gartner expects 40% of enterprise apps to include task-specific agents by the end of 2026. But McKinsey finds only 23% of organizations have scaled agent deployments, and Gartner expects more than 40% of current agent projects to be cancelled by 2027.

Figure 3 - Interest Is Nearly Universal; Completion Is Rare



Half experimenting, one in nine reaching production - the defining gap in this market today. Each bar is a different survey with a different base group, so read the shape rather than the arithmetic.

WHY THE GAP EXISTS

It isn't that the models aren't smart enough, or that the standard is unavailable. Once an agent can act rather than answer, someone must own who authorized it, on whose behalf, and what happens if it fails. Most organizations can't yet say — so the pilot never gets signed off.



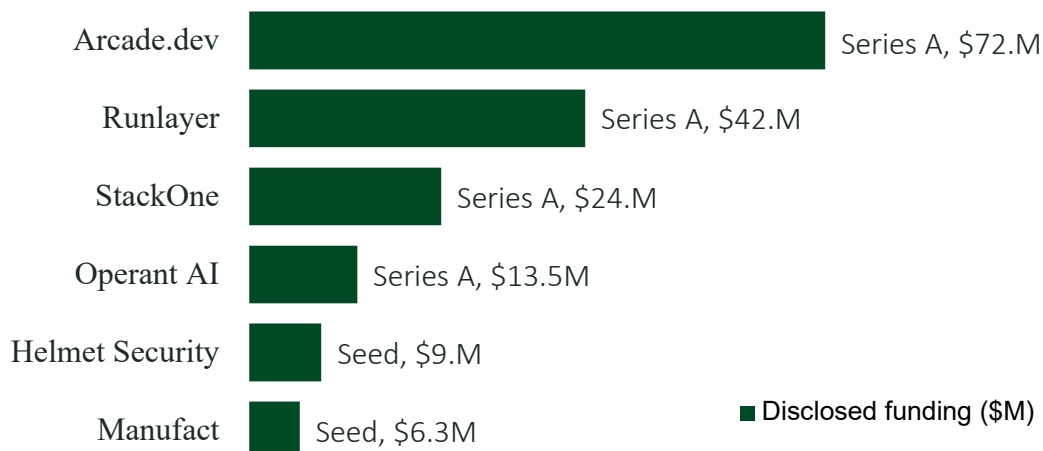
SECTION 07

Where the Money Is Actually Going



Follow the capital and the thesis becomes concrete. The companies raising money are the ones building the operational layer around MCP - the tooling that makes agents safe and manageable enough to leave the pilot stage.

Figure 4 - Venture Funding to date for MCP Infrastructure and Security



- ✓ Arcade authored the MCP spec's own enhancement proposal, then built the product that follows it best
- ✓ Manufact - three people, out of Y Combinator - already has 6M+ downloads and users at NASA, Nvidia, and SAP

WHY THE TIMING MATTERS

Four of the six rounds shown closed between November 2025 and June 2026, and two companies moved from seed to Series A in about seven months. Total disclosed capital here is roughly \$167 millions.



SECTION 08

What could go wrong? Three risks worth raising



MCP servers are being deployed faster than they're being secured. A scan of 1,000 servers by Enkrypt AI found critical vulnerabilities at scale, and researchers separately found hundreds left publicly exposed with no basic authentication. One widely used component - over 437,000 downloads, integrated by Cloudflare, Hugging Face, and Auth0 - carried a critical flaw of its own: a single weak piece used by everyone becomes everyone's problem.

The standard is shifting underneath everyone as well. A new spec takes effect 28 July 2026 - cheaper to run at scale, but it moves critical security responsibility from the standard onto developers and operators. Companies built on the old assumptions face a migration cost and new obligations they may not be staffed for.

33%

of 1,000 scanned MCP servers had critical vulnerabilities

492

servers found publicly exposed with no authentication or encryption

\$28K

real daily on-chain volume behind one network's touted \$50M headline figure

By April 2026, one payments network for AI agents touted headline transaction volume that on-chain data showed was mostly test and gamed activity, not real commerce. Transaction counts, tool calls, and agent counts are cheap to inflate.

THE PATTERN TO WATCH FOR

Ask what fraction of any usage number represents a customer who chose to pay.



SECTION 09

Implications for an Investor



Compliance with the standard is not a business. MCP is jointly governed by eight competing giants precisely so no one can own it - saying a product supports MCP describes a dependency, not an advantage. Durable value sits above the standard (proprietary data, entrenched workflows, real distribution) or in the operational work it deliberately leaves undone: permissions, audit trails, identity, and safe execution.

The timing case rests on one gap closing. The market grows 40%+ a year on nearly every estimate, yet only about one organization in nine has MCP running in production. That gap closes via better governance tooling - which favors infrastructure - or Gartner's forecast 40% project-cancellation wave, which favors whoever consolidates the application layer after.

\$167M

disclosed capital across the visible names, nearly all at seed or first round

\$200B

forecast agentic spending this year - the scale this is still early against

4 of 6

rounds closed in the last eight months - the window is narrowing

THE ONE QUESTION TO ASK

Not 'do you support MCP.' When your agent takes the wrong action inside a customer's business, who is accountable, and what in your product proves what happened? A crisp answer means they're selling into the real bottleneck - no answer means they're selling a feature.



Thank you!

www.6igmaventures.com
info@6igmaventures.com