TECHNOLOGY INDUSTRY

# Put AI Agents to Work Faster Using MCP

By Tom Martin, Daniel Sack, Djon Kleine, Niels Degrande, and Nicolas de Bellefonds

**INTERVIEW** AUGUST 01, 2025 3 MIN READ

Many companies are racing to build AI agents. However, as their use becomes widespread, the challenges of scalability and interoperability are becoming clearer.

The core problem is integration with the digital world. To do useful work, agents typically need access to the CRM, the ERP system, databases, messaging tools, and more. However, as more agents and tools get added to the ecosystem, this gets dramatically more complex.

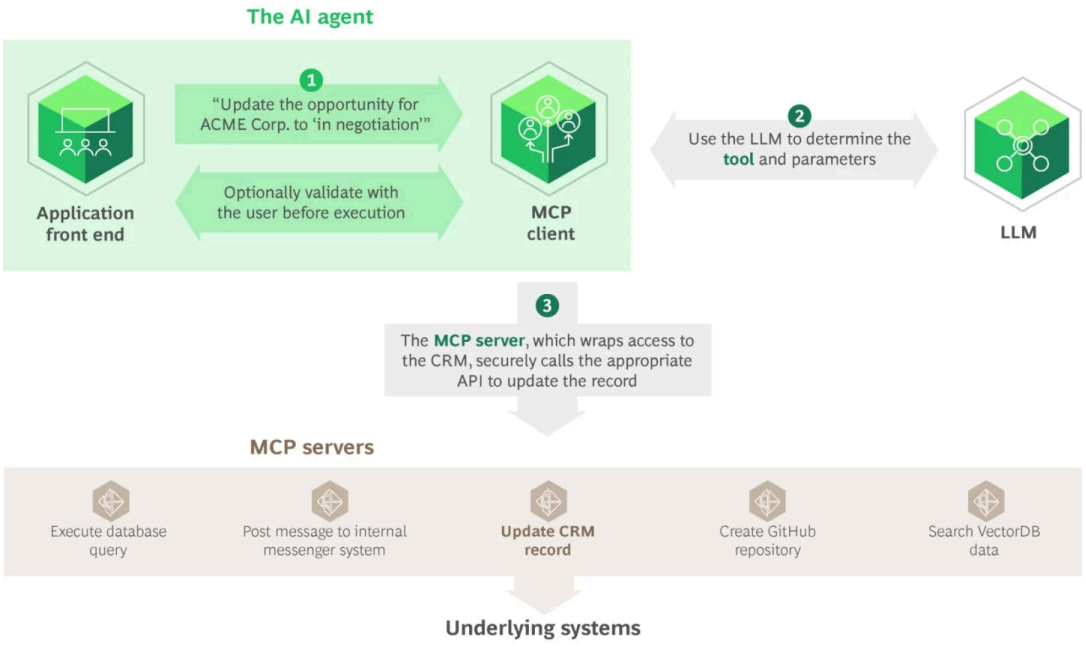
The solution is a deceptively simple idea with outsized implications: the Model Context Protocol (MCP). Built and open-sourced by Anthropic, MCP is emerging as the de facto standard for connecting AI agents to other systems, including those built by OpenAI, Google, and Amazon.

# The So What

**MCP is like a USB-C port for AI agents—a standardized link that greatly reduces the headaches of connecting large language models (LLMs) to tools and data.**

Launched in late 2024, it is an open-source protocol that standardizes how agents access tools and data, acting like a universal adapter between AI agents and the tools, data, and prompts they use. (See the exhibit.) Without it, a new integration would be needed every time an agent needs to use a tool, meaning the number of integrations would rise quadratically as AI agents spread throughout the organization. With MCP, however, integrations can be reused, so the effort increases only linearly. As more AI agents are created, the time and effort saved increase. As such, the benefits grow fast, not just steadily. Scaling up becomes much cheaper and faster.

How MCP Connects AI Agents to the Information Ecosystem




**Source:** Anthropic Model Context Protocol.

An MCP server is more than just a REST API. MCP supports complex, session-based interactions that can reference previous activity, which helps AI agents act more dynamically and interactively and become, in effect, the new all-stars on your team. And it's not just for AI: non-AI systems can use it too, adding flexibility and functionality to other integrations.

# Dive Deeper

MCP doesn't just accelerate building agents—it helps build *better* agents. MCP enables agents to evolve from pre-set workflows based on chains of prompts to true autonomous agents. This is because:

- **MCP servers are much more than ways to access tools and data.** They also announce their capabilities to AI agents (and large language models in general) and can offer prompt templates that help AI agents understand how to effectively access those tools and data. This helps agents reason about which tools to use and how to sequence them for effective planning.
- **MCP can boost task autonomy and execution.** Using MCP servers, agents can dynamically use multiple tools and coordinate execution across complex, multi-tool workflows without brittle, hard-coded logic. This fosters greater task autonomy and adaptability.
- **MCP can improve memory and knowledge use.** MCP servers enable agents to easily access real-time transaction data or vector databases, augmenting their memory and contextual understanding.

Other standards are emerging to support the ecosystem, such as the A2A standard from Google, which is designed to facilitate interactions between agents.

# Now What

To capture the value created by MCP, organizations must:

- **Take a strategic approach to integrations.** Start with the high-value use cases for AI agents in the organization and think about the integrations they need. Here, MCP can serve as a firm foundation for future growth in agents.
- **Stay agile and foster continuous learning.** The AI technology landscape, including standards like MCP and emerging agent-to-agent protocols, is evolving at an unprecedented pace. CIOs and CTOs must cultivate a mindset of collective curiosity, experimentation, and rapid adaptation. They should encourage pilot projects, learn from both successes and failures, and be prepared to integrate new tools and methods as they mature.

- **Make security a foundation, not an afterthought.** As always, more power brings more risk. The expanded “AI surface attack area” due to MCP demands a proactive security posture. Teams must implement robust security measures including strong authentication, role-based access control for every tool call, version pinning (preventing updates creating security or compatibility issues), and trust domain isolation (blocking access from untrusted network connections). Comprehensive logging of agent reasoning is essential to debug and improve performance. It is vital to consult with CISO and legal teams on the implications of MCP. Our recommendation is to treat all tool logic and servers as untrusted. Organizations should use private MCP registries to expose only a curated list of trusted servers. And although there is a lot of MCP code on GitHub—a welcome sign of its fast adoption—it should only be used after exhaustive verification.

---

MCP has arrived at the right moment. As organizations start to scale their agent deployments, MCP offers the infrastructure to do it right. Using MCP can not only efficiently deliver agents that work; it can evolve, scale, and deliver better enterprise value.

Yes, it is still early days for MCP. It is still evolving technically, and in time rival solutions may yet emerge. However, MCP’s rapid acceptance by many major players shows that the ecosystem around AI and AI agents is evolving—and improving—fast. For firms building out AI agents, the road is clear for efficient rollout at scale.

# Authors


## Tom Martin

Platinion Associate Director
London

## Daniel Sack

Managing Director & Partner
Stockholm

## Djon Kleine

Managing Director & Partner
San Francisco - Bay Area

## Niels Degrande

Partner
Stockholm

## Nicolas de Bellefonds

Managing Director & Senior Partner
Paris

## ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.