SUPER DATASCIENCE
MAKING THE COMPLEX SIMPLE

SDS PODCAST EPISODE 884: MODEL CONTEXT PROTOCOL (MCP) AND WHY EVERYONE'S TALKING ABOUT IT

Jon Krohn: 00:06 This is episode number 884 on MCP, Model Context Protocol.

00:28 Welcome back to the Super Data Science podcast. I'm your host, Jon Krohn. Today we're diving into Model Context Protocol, or MCP, the hot topic taking the AI world by storm in early 2025. Large language models are pretty mind-bogglingly smart in isolation in a lot of scenarios, but they've always struggled to access information beyond your training data. This is a critical limitation. For AI to be useful, to be most useful, it needs to seamlessly connect with your files, your databases, your knowledge bases, and take actions based on that context.

01:03 Historically, connecting AI to external sources has been messy. Developers had to write custom code for each data source or API. These wired-together integrations were brittle and impossible to scale. That's where MCP, the Model Context Protocol, comes in.

01:21 Anthropic actually introduced MCP, Model Context Protocol back in November 2024, but it's only now in the past couple months that it's really taking off, and I'm hearing every other person talk about it at agentic AI conferences. Why the sudden surge in interest? First, MCP directly addresses the integration problem that's been holding back agentic AI. As we've focused on model capabilities and prompt engineering over the past couple of years, the challenge of connecting AI to real-world systems remained an open challenge. MCP provides that missing puzzle piece for production-ready AI agents.

01:57 Second, the community adoption has been explosive. In just a few months, MCP went from concept to ecosystem with early adopters, including Block, Apollo, Replit, and Sourcegraph. By February, there were over 1,000 community-built MCP servers connecting to various tools and data sources. Third, unlike proprietary alternatives, MCP is open and model agnostic. Any AI model, Claude, GPT-4, or open-source LLMs can use it, and any developer can create an MCP integration without permission. It's positioning itself as a kind of like USB or HTTP of AI integration, a universal standard.

02:38 So what exactly does MCP do? It lays out clear rules for how AI models find, connect to, and use external tools, whether querying a database or running a command. One striking feature is dynamic discovery. This is really cool. AI agents automatically detect available MCP servers and their capabilities without hard-coded integrations. Spin up a new MCP server for, say, your CRM, your customer relationship management platform, and your agent can immediately recognize and use it.

03:09 Getting started with MCP is straightforward. You first run or install an MCP server for your data source. Anthropic provides pre-built servers for popular systems like Google Drive, Slack, and databases. Then you can set up the MCP client in your AI app and invoke the model. The agent can now call MCP tool actions as needed. Before MCP, AI systems handled context integration through custom one-off API connectors, proprietary plug-in systems like OpenAI's, agent frameworks like LangChain, or retrieval-augmented generation with vector databases. MCP complements these approaches, while standardizing how AI models interact with external tools.

03:49 Now, is MCP a silver bullet? Not quite. It introduces challenges around managing multiple tool servers, ensuring effective tool usage by models, and dealing with an evolving standard. Security and monitoring also present ongoing challenges, and for simple applications, MCP might be overkill compared to direct API calls.

04:08 Now, where does MCP fit in the agentic workflow? It's not an agent framework itself per se, but rather a standardized integration layer. If we think of agents as needing profiling, knowledge, memory, reasoning, and action capabilities, well, MCP specifically addresses the action component, giving agents a universal way to perform operations involving external data or tools.

04:32 The most exciting part is the new possibilities MCP unlocks. We're seeing multi-step, cross-system workflows where agents coordinate actions across platforms. Imagine an AI assistant planning an event, checking your calendar, booking venues, emailing guests, and updating budget sheets, all through a single interface without custom integrations. Lots of potential here for you as an individual or for a company that you work for, an enterprise that you serve.

04:59 MCP could enable agents that understand their environment, including smart homes and operating systems. It could serve as a shared workspace for agent societies where specialized AIs collaborate through a common tool set. For personal assistance, MCP allows deep integration with private data while maintaining security at the same time. And for enterprises, it standardizes access while enabling governance and oversight.

05:23 Looking ahead, Anthropic is working on remote servers with OAuth, an open standard authentication protocol. They're also looking into an official MCP registry so that you, I guess, have trusted components that you can work with. Standardized discovery endpoints and improvements like streaming support and proactive server behavior. MCP is rapidly maturing into a powerful standard that transforms AI from an isolated brain into a versatile doer. By streamlining how agents connect with external systems, it's clearing the path for more capable, interactive, and user-friendly AI workflows. Pretty cool stuff from Anthropic.

06:05 All right, that's it for today's episode. I'm Jon Krohn and you've been listening to the Super Data Science podcast. If you enjoyed today's episode or know someone who might, consider sharing this episode with them. Leave a review of the show on your favorite podcasting platform, tag me in a LinkedIn or Twitter post with your thoughts, and if you aren't already, be sure to subscribe to the show. Most importantly, however, we hope you'll just keep on listening. Until next time, keep on rocking it out there, and I'm looking forward to enjoying another round of the Super Data Science podcast with you very soon.