EINPRESSWIRE

ToolHive Ensures Every Developer Can Securely Connect AI Agents to Sensitive Data and Systems with One Click or Command

New capabilities allow enterprises to use Model Context Protocol (MCP) in production environments

SEATTLE, WA, UNITED STATES, July 16, 2025 /EINPresswire.com/ -- Stacklok is paving the way to an agentic future by ensuring AI agents and models have controlled access to the right tools at the right times. Earlier today, the company added new capabilities to its popular project, ToolHive. Enterprise developers now have the option of a CLI or UI to discover pre-vetted MCP (Model Context Protocol) servers, connect them to agents with a single click or command, and strengthen security controls.

MCP provides agents and models with access to the data, services, and systems they need to complete real, important work. Enthusiasm surrounding MCP has led to exponential growth in MCP servers, with more than 5,000 MCP servers published in 2025 alone. As a result, it's hard for developers to know which MCP servers they can trust. And when they want to stand up their own MCP server, developers often struggle with configuration, runtimes, and security boundaries. As enterprise developers build and manage more MCP servers, operating at scale poses a significant barrier to adoption.

> ToolHive provides only verified MCP servers and protects secrets so that enterprises can confidently unlock the potential of MCP servers."
>
> *Craig McLuckie*

ToolHive strengthens trust in MCP servers. Today's release includes capabilities that simplify and secure MCP servers:

*Verified registry. No more guessing which MCP servers to trust. Developers can search and discover servers from ToolHive's registry, and enterprises can build custom, approved registries for their teams.

*Consistent runtimes. MCP servers are often written in different languages and to different standards. ToolHive containerizes every MCP server for consistency and integrates with Kubernetes for centralized control and observability.

*Client integrations. Configuring MCP servers is multi-step and complex. ToolHive handles the configuration of servers for popular developer tools like Visual Studio Code, Cursor, and Claude Code with a single click or command.

*Network isolation. MCP servers can make network calls in the background, potentially exposing a user to data exfiltration or malicious activity. ToolHive includes network isolation to block unauthorized connections and provide an audit trail.

*Built-in security. MCP servers require developers to store API tokens in plaintext config files. ToolHive provides secure secrets management via an encrypted vault and/or 1Password integration.

The ToolHive project was released earlier this year as a command line interface. ToolHive is now available with an intuitive user interface, so that every developer can feel comfortable connecting AI agents to MCP servers.

“The challenges to MCP adoption — complexity and security — parallel my early experiences launching Kubernetes,” said Craig McLuckie, CEO and founder of Stacklok, and co-creator of Kubernetes. “We understand that to adopt MCP, enterprises are not satisfied with a ‘minimum viable’ approach to security, so we have been intentional about building security into ToolHive from the outset. ToolHive provides verified MCP servers and protects secrets so that enterprises can confidently use MCP servers in production.”

“Docker believes containers are the right foundation for a secure, scalable, and open MCP ecosystem. ToolHive’s container-based approach to running MCP servers aligns perfectly with Docker’s mission to make trusted software delivery simple and repeatable. We’re especially excited to see ToolHive support the Docker MCP Catalog and Toolkit, reinforcing shared goals around transparency, provenance, and ease of use for AI-native development. Stacklok’s contributions are helping move this critical ecosystem forward, and we’re proud to support their work,” said Jean-Laurent de Morlhon, Sr. Vice President of Engineering, GenAI at Docker.

ToolHive is free and open source. Learn more about the project and get started today at toolhive.dev. And get involved in the future of ToolHive by exploring our GitHub repo: https://github.com/stacklok/toolhive.

Scott Buchanan
Stacklok
email us here

---

in today's world. Please see our Editorial Guidelines for more information.