

MCP Gateway with Cyberhaven's Endpoint Sensor

An MCP gateway is a smart addition to an agentic security stack. Its main job is to gate access, deciding which external apps AI agents can reach through MCP (Model Context Protocol). Protecting the data those agents handle is a different job. Cyberhaven traces the full lifecycle of your data, adapting protection to changing context.

Difference Between MCP Gateway and Endpoint Sensor

	MCP Gateway	Endpoint Sensor
Primary job	Gates which apps AI agents can access through approved MCP servers.	Monitors and protects data on the endpoint, including data moving to the web and apps that agents use.
Where it runs	Between agents and the apps they reach.	On the endpoint where agents and users work.
Shadow MCP	Sees only the MCP servers registered with the gateway.	Discovers both registered and unregistered MCP servers on the device.
Data understanding	Inspects MCP messages at a single point in time, as they pass through the gateway.	Inspects data continuously, capturing its lineage, including where it came from and how it is transformed.
Controls	Manages which apps agents can access and whether they can read, write, or delete. Limited blocking of data.	Controls data movement. Educates, blocks, and monitors data based on attributes such as data sensitivity and origin.

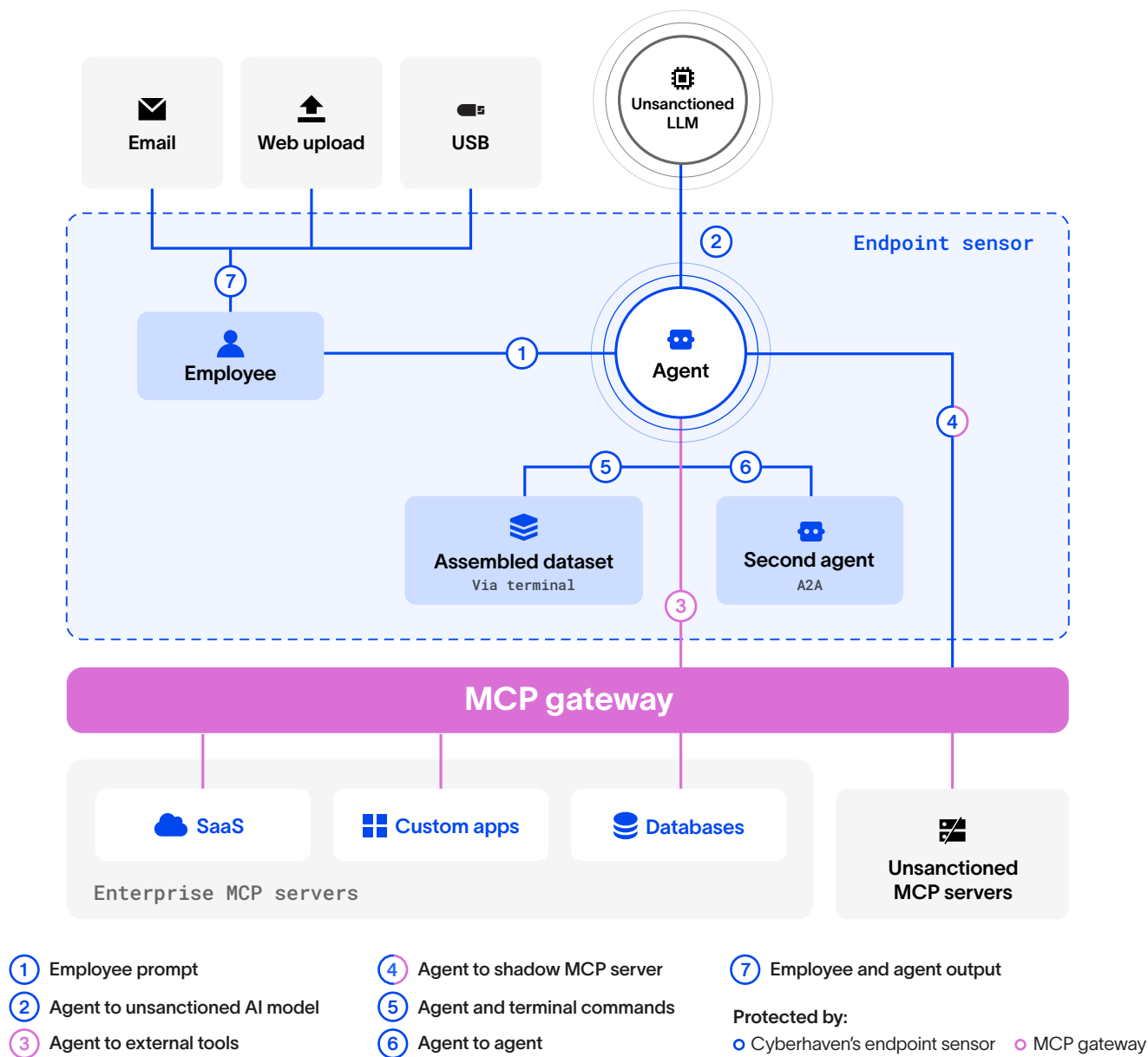
Data Exfiltration Channels Not Covered by MCP Gateways

MCP gateways monitor the traffic routed through them, from agent to third-party apps. In agentic workflows, data also moves to and through other channels not monitored by MCP gateways.

- Unapproved AI models
- Shadow MCP servers
- Agent-to-app connections (APIs, SDKs, and webhooks)
- Agents running terminal commands
- Agent-to-agent connections (A2A or Agent2Agent Protocol)
- Agents submitting data in browser sessions
- Users sharing agent output

Better Together Agentic Workflow

See how MCP gateways and Cyberhaven's endpoint sensor protect data within an agentic workflow.



Better Together Use Cases

Discover shadow MCP

MCP gateways manage approved MCP servers. Cyberhaven's endpoint sensor finds shadow MCP servers on devices.

Allow access, stop data leaks

MCP gateways let agents pull corporate data from enterprise apps. Cyberhaven's endpoint sensor recognizes its source and blocks exfiltration.

Complete the investigation

MCP gateways log activity between agent and app. Cyberhaven's endpoint sensor traces the data from origin to destination.

Evaluating an MCP gateway? See what Cyberhaven adds.

[Request a demo](#)

cyberhaven.com/request-demo

AI Changed Work.
We Protect It.

Cyberhaven is a leader in Data Security for the Agentic Enterprise, trusted by the world's most innovative companies to protect their most sensitive data. Learn more at cyberhaven.com.