The Aviatrix-Obot Partnership: Securing MCP Servers with Containment Architecture

Secure MCP Servers with Default-Deny, Network-Level Enforcement

MCP (Model Context Protocol) servers are one of your organization's greatest needs and greatest risks. They're essential to connect AI agents with the systems they need to access, but without the right security guardrails, they create additional attack vectors. Using MCP servers, threat actors can move laterally and exfiltrate data faster than security teams can detect them.

The Aviatrix-Obot partnership empowers organizations to use agentic AI safely by providing enterprise-grade MCP server security through containment architecture. Obot enables companies to deploy MCP servers easily; Aviatrix Cloud Native Security Fabric gives you the ability to contain potential threats through policies that govern what the server can talk to. These default-deny policies are enforced inline, at the network layer.

With this integration, anyone who tries to send data through an MCP server to an unauthorized location will get blocked, and the attempt will show up in Aviatrix logs. The threat is contained.

Through Obot's controller and Aviatrix Cloud Native Security Fabric's Firewall Policy CRD, this partnership gives customers secure agentic AI access with:

- **Granular Communication Governance for MCP Servers:** Aviatrix Cloud Native Security Fabric empowers you to set egress policies based on pod labels, not namespaces, giving you extra specificity in policy enforcement. This is not possible with Kubernetes Network Policy.

- **Multicloud Portability:** You can use one Aviatrix Firewall Policy CRD to enforce egress at the Aviatrix Spoke Gateway across Azure Kubernetes Services, Amazon Elastic Kubernetes Service, and Google Kubernetes Engine instead of writing a separate policy for each cloud.

- **Simple MCP Server Creation and Deletion:** Obot makes it easy to deploy an MCP server and delete one without policy debt. When you delete the MCP server, the Obot controller triggers garbage collection at the Aviatrix Spoke Gateway. No orphaned permits accumulate in your cluster.

“Every enterprise running AI agents is running MCP servers, often more than they realize. Without governance at the gateway and the network, a compromised agent’s blast radius extends to everything those servers can reach. Obot governs which MCP servers an agent can call. Aviatrix governs where those servers can reach. That two-layer control is what enterprise agentic AI actually requires.”

— Shannon Williams, President, Obot AI

Want to learn more about containment architecture for AI workloads? Explore Aviatrix Validated Containment Architectures.

About Aviatrix

Aviatrix® is pioneering the Cloud Native Security Fabric, the architecture the Containment Era requires. The Cloud Native Security Fabric governs every workload communication path across every cloud, every VPC, every Kubernetes cluster, and every serverless function, from a single policy plane. One rule. Universal propagation. Enforced at the workload, not at a chokepoint. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.