SALT

SOLUTION BRIEF

Salt MCP Finder Technology: The Discovery Engine for MCP Servers

Introduction

AI adoption has moved faster than security governance. Across the enterprise, teams are deploying autonomous AI agents that rely on **Model Context Protocol (MCP)** servers to access sensitive data and execute business actions. This new **Agentic AI Action Layer** is powerful but invisible, creating a massive, unmanaged attack surface.

Most security leaders lack a single source of truth for this infrastructure. They cannot answer fundamental questions: Where are my MCP servers? What tools do they expose? Are they compliant with our security policies?

Salt Security introduces Salt MCP Finder Technology: the industry's first centralized system of record for AI agent infrastructure. It consolidates discovery from external exposure, code, and runtime into a single, authoritative view, giving security leaders the visibility and context they need to govern AI with confidence.

The Challenge: The Surge in Agent-Driven APIs

Traditional security tools were not built for the machine-to-machine speed and scale of AI agents. Enterprises today face a critical visibility gap where AI infrastructure is deployed faster than it can be tracked.

Without a unified and complete view of MCP Servers, organizations face significant risks:

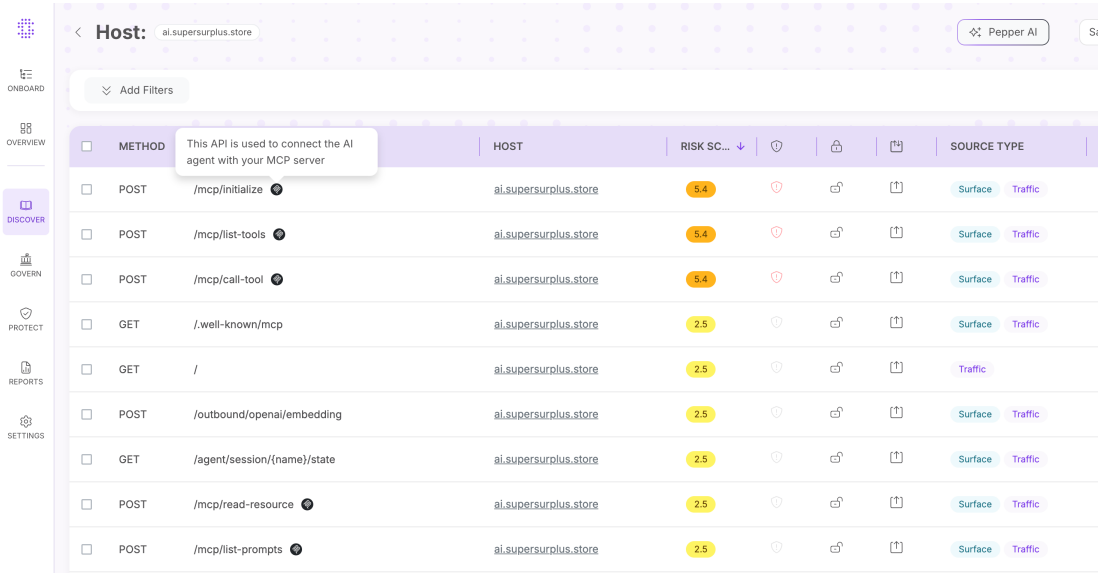
- **Invisible "Shadow AI":** Developers define MCP servers in private code or deploy them without approval, bypassing security review.
- **Fragmented Visibility:** Security teams cannot see the full picture of their AI

estate. Assets are scattered across source code repositories, cloud accounts, and runtime environments, with no single tool to correlate them.
- **Unquantified Risk:** You cannot assess the risk of an AI agent if you don't know which MCP servers it connects to or what tools those servers expose.
- **The Governance Gap:** Without an inventory, you cannot enforce policy. You cannot apply risk scoring or security rules (like "Block external access to sensitive data") if you don't know the asset exists.

The Solution: Salt MCP Finder Technology

Salt MCP Finder Technology is your unified inventory for the Agentic AI Action Layer. It automatically discovers, catalogs, and maps every MCP server across your organization, whether it's exposed to the internet, defined in code, or communicating in runtime.

It transforms fragmented data into a **Single Source of Truth**, enabling you to:



- **Unified Inventory:** See all MCP servers, hosts, and endpoints in a single, central view, regardless of where they reside or how they were deployed.
- **Risk Visualization:** Instantly understand your AI infrastructure's risk profile. MCPView maps every exposed tool, action, and data source, allowing you to see exactly what capabilities an AI agent has.
- **Governance Ready:** Once inventoried, apply applicable governance rules directly to your known assets. For example, you can automatically flag any MCP server that returns sensitive data or is exposed to the public internet, ensuring policy enforcement scales with your AI adoption.

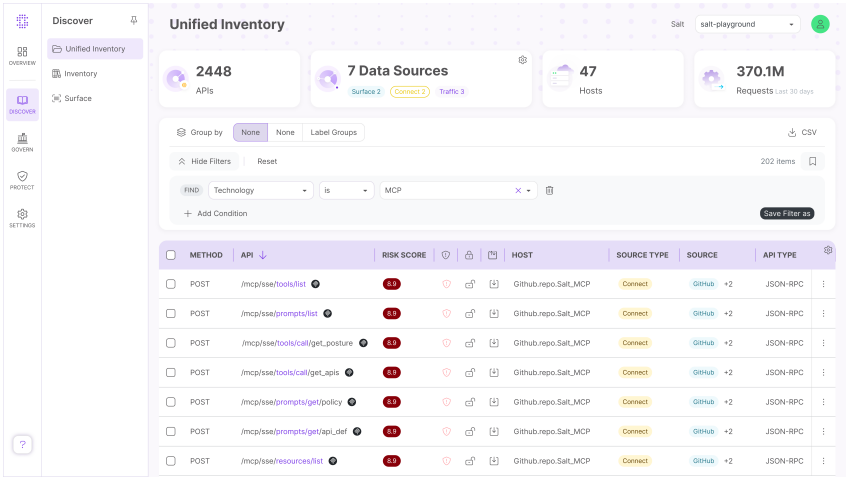
How MCP Finder Technology Works: The Three-Phase Discovery Engine

Manual spreadsheets can't keep up with AI. Salt MCP Finder Technology is populated automatically using a unique, three-pronged discovery engine that secures every stage of the lifecycle:

- **External (Salt Surface):** The first step is securing your perimeter. We identify

forgotten or zombie MCPs exposed to the public internet, allowing you to close immediate gaps that attackers could exploit.

- **Code (GitHub Connect):** The proactive step. We scan private repositories to find MCP blueprints and shadow integrations before they are deployed. This "shift-left" visibility allows you to catch misconfigurations at the source.
- **Runtime (Agentic AI):** The continuous step. We monitor live traffic to observe the actual behavior of AI agents, tool usage, and data flow. This ensures that the runtime environment aligns with your security policy.



Conclusion

The Agentic AI Action Layer represents a fundamental shift in how software executes. It requires a fundamental shift in visibility. **Salt MCP Finder Technology** turns that risk into a managed, visible asset. Don't let the surge of AI agents outpace your security; inventory your AI estate today with Salt MCP Finder Technology.