Salt Security Launches Salt MCP Finder Technology: the Discovery Engine for MCP Servers in Agentic AI Deployments

LONDON, UNITED KINGDOM, November 25, 2025 /EINPresswire.com/ -- New capability uncovers invisible MCP servers and consolidates discovery into a unified inventory, giving security teams the visibility required to manage risk in the rapidly expanding Agentic AI Action Layer.

Salt Security, the leader in AI agent and API security, today announced Salt MCP Finder technology, the industry's first dedicated discovery engine for Model Context Protocol (MCP) servers, the fast-proliferating infrastructure powering agentic AI. MCP Finder provides organisations with a complete, authoritative view of their MCP footprint at a moment when MCP servers are being deployed rapidly, often without IT or security awareness.

The invisible backbone of agentic AI and the newest blind spot in cybersecurity
As enterprises accelerate the adoption of agentic AI, MCP servers have emerged as the universal API broker that lets AI agents take action: retrieving data, triggering tools, executing workflows, and interfacing with internal systems. But this new power comes with a new problem: MCP servers are being deployed everywhere, by anyone, with almost no guardrails.

- Developers spin them up for prototyping.
- Business units deploy them to connect agents to SaaS tools.
- Vendors and contractors introduce them during integration projects.
- Open-source MCP servers get dropped into repos and shipped to production.
- Internal business teams are deploying MCPs alongside new internal APIs to support shadow agentic workflows, outside the visibility of IT or security.

This wave of adoption sits atop fractured internal API governance in most enterprises, compounding risk. Once deployed, MCP servers become easily accessible, enabling agents to connect and execute workflows with minimal oversight. This becomes a major source of operational exposure.
The result is a rapidly growing API fabric of AI-connected infrastructure that is largely invisible to central security teams. Organisations do not know:

- How many MCP servers are deployed across the enterprise
- Who owns or controls each server
- What APIs and data each server exposes

- What actions agents can perform through accessible MCP tools
- Whether corporate security standards are followed and basic security controls like authentication, authorisation, and logging are in place

Recent industry observations show why this visibility crisis matters. One study showed that only ten months after the launch of the MCP, there were over 16,000 MCP servers deployed across Fortune 500 companies. Another (https://www.enkryptai.com/blog/we-scanned-1-000-mcp-servers-33-had-critical-vulnerabilities?) showed that in a scan of 1,000 MCP servers, 33% had critical vulnerability and the average MCP server had more than 5. MCP is quickly becoming one of the largest sources of "Shadow AI" as organisations scale their agentic workloads.

According to Gartner® "Most tech providers remain unprepared for the surge in agent-driven API usage. Gartner predicts that by 2028, 80% of organisations will see AI agents consume the majority of their APIs, rather than human developers."

Gartner further stated, "As agentic AI transforms enterprise systems, tech CEOs who understand and implement MCP would drive growth, ensure responsible deployment and secure a competitive edge in the evolving AI landscape. Ignoring MCP risks falling behind as composability and interoperability become critical differentiators. Tech CEOs must prioritise MCP to lead in the era of agentic AI. MCP is foundational for secure, efficient collaboration among autonomous agents, directly addressing trust, security, and cost challenges."*

A prerequisite for governing the AI Action Layer
Salt's MCP Finder technology solves the foundational challenge: you cannot monitor, secure, or govern AI agents until you know what attack surfaces exist. MCP servers are a key component of that surface.

"You can't secure what you can't see," said Nick Rago, VP of Product Strategy at Salt Security. "Every MCP server is a potential action point for an autonomous agent. Our MCP Finder technology gives CISOs the single source of truth they need to finally answer the most important question in agentic AI: What can my AI agents do inside my enterprise?"

Salt's MCP Finder technology delivers complete, automatic MCP inventory through three discovery layers
Salt's MCP Finder technology uniquely consolidates MCP discovery across three systems to build a unified, authoritative registry:

1. External Discovery – Salt Surface (https://salt.security/surface) Identifies MCP servers exposed to the public internet, including misconfigured, abandoned, and unknown deployments.
2. Code Discovery – GitHub Connect (https://salt.security/integrations/github) Using Salt's recently announced GitHub Connect capability, MCP Finder inspects private repositories to uncover MCP-related APIs, definitions, shadow integrations, and blueprint files before they're deployed.

3. Runtime Discovery – Agentic AI Behavior Mapping (https://salt.security/agentic-ai) Analyses real traffic from agents to observe which MCP servers are in use, what tools they invoke, and how data flows through them.

Together, these sources give organizations the single source of truth required to visualise risk, enforce posture governance, and apply AI safety policies that extend beyond the model into the actual action layer.

Salt's MCP Finder technology is available immediately as a core capability within the Salt Illuminate™ platform.

*Source: Gartner Research, Protect Your Customers: Next-Level Agentic AI With Model Context Protocol, By Adrian Lee, Marissa Schmidt, November 2025.

About Salt Security: The Salt Security API Protection Platform delivers comprehensive, AI-powered security, enabling organisations to confidently manage and secure their APIs throughout their entire lifecycle, regardless of where they are deployed. By integrating its deep, contextual API threat detection with native AWS services like AWS WAF, Salt creates a powerful, closed-loop security system. Salt's platform provides panoramic and continuous discovery of the entire API Fabric, proactive API posture governance, and adaptive, real-time threat protection.

Bethany Smith
Eskenzi PR
+44 20 7183 2843
beth@eskenzipr.com
Visit us on social media:
LinkedIn
