SALT

FEATURE BRIEF

# Salt GitHub Connect: Expanding Agentless "In-Minutes" Discovery to Code

## Introduction

Organizations trust the Salt Cloud Connect capability for its proven, agentless discovery model. This functionality enables rapid API discovery and under-10-minute deployments by automatically gathering API-specific information across cloud platforms such as AWS, Azure, GCP, Kong, and MuleSoft. It delivers immediate, traffic-free visibility and a "wow" moment of value.

However, many security gaps originate before an API ever reaches the cloud. They start as code. As organizations adopt AI, developers are defining Model Context Protocol (MCP) servers and their APIs in private GitHub repositories, creating a critical shift-left blind spot.

## The Problem: The "Shift-Left" MCP Blind Spot

While Salt's Cloud Connect capability is essential for finding cloud-native API sprawl, security teams face a new, pre-deployment challenge:

- **Hidden AI Infrastructure:** Developers are building and adopting AI agents, creating MCP-to-API connections that are hidden in private source code.
- **Noisy, Ineffective Scanners:** Traditional code scanners (SAST) are not designed for this. They are noisy, generic, and cannot distinguish a high-risk MCP configuration from a simple API call.
- **Fragmented Risk Posture:** Without a way to connect code-level governance to runtime security, teams have a fragmented view, unable to see the full API lifecycle. cubilia curae; Aenean sed pharetra neque. Ut scelerisque aliquet lorem a faucibus.

## Solution: Salt GitHub Connect

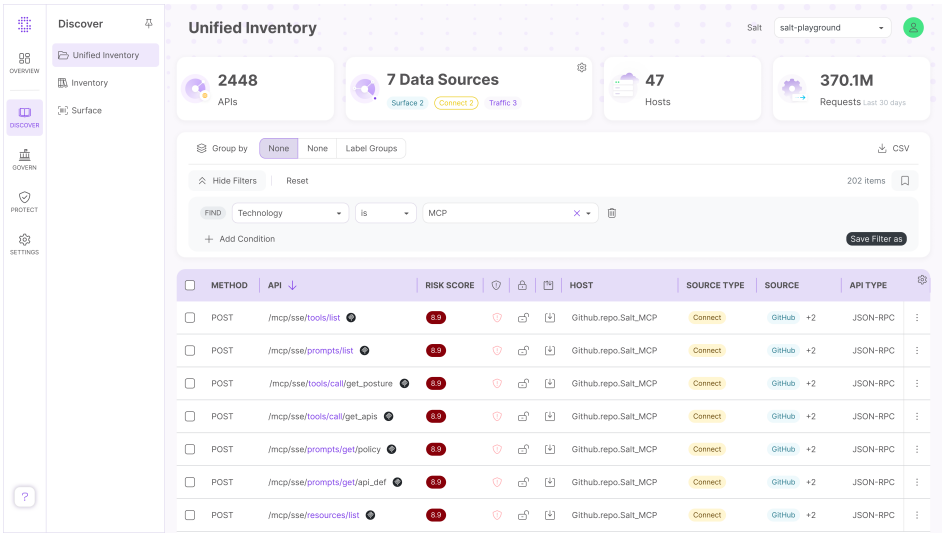
Introducing Salt GitHub Connect, the latest expansion of the Salt Cloud Connect functionality. It extends the same agentless discovery methodology you already trust for the cloud to your GitHub repositories.

This is not a general-purpose scanner. It is a precision tool designed to address AI security issues by scanning code for MCP-related APIs and posture gaps.

This new capability bridges the gap between code and cloud. It feeds its shift-left findings directly into the Salt Illuminate™ platform, providing an immediate inventory and risk baseline that complements Salt's deeper, full-lifecycle inspection.

## Key Features & Benefits

- **Expands the Trusted Cloud Connect Capability:** Provides the same agentless discovery model, in minutes time-to-value, and ease of use that customers already love, now for source code.
- **Precision "Shift-Left" Discovery:** A targeted scanner that focuses on high-risk MCP-related APIs and posture gaps, eliminating the noise of traditional SAST tools.
- **Immediate, Traffic-Free Risk Scoring:** Leverages the Risk Score for Connect feature to immediately prioritize discovered MCP APIs with a quantifiable risk score, without requiring any traffic collection.




- **Finds "Hosted Elsewhere" Risk:** Identifies integration patterns for third-party MCPs and AI agents, even when the MCP is hosted elsewhere.
- **A Core Part of the Agentic AI Action Layer:** Provides the code component of Salt's "first and only" platform for securing MCPs across code, runtime, and the external surface.

## Conclusion

Don't wait for a security incident to reveal a vulnerability in your AI applications. Salt GitHub Connect extends the rapid, agentless discovery model of the Cloud Connect capability to shift-left. This enables you to secure the Agentic AI Action Layer by finding and governing high-risk MCP-related APIs in your source code, long before they ever reach production.