TECHNICAL BRIEF

OpenClaw, NemoClaw & Enterprise AI Governance

MCP registries make it trivially easy for AI agents to discover external tools. But neither includes governance. Reign closes the gap.

CISO | CTO | AI Platform Teams | Security Architects

March 2026 | v2.0

97M+	2 New	0%	Aug 2026
Monthly MCP SDK Downloads	MCP Server Registries	Built-in Governance	EU AI Act Deadline

OVERVIEW

Executive Summary

Anthropic's OpenClaw and NVIDIA's NemoClaw represent a new era of open MCP server registries. They make it trivially easy for AI agents to discover and connect to external tools. But neither includes governance. Enterprises need a governance layer between their agents and these registries.

CONTENTS

In This Document

BACKGROUND

What Are OpenClaw & NemoClaw?

OpenClaw is Anthropic's open-source MCP server registry. Community-contributed. Rapidly growing. NemoClaw is NVIDIA's enterprise-focused MCP registry with NVIDIA ecosystem integration. Both follow the Model Context Protocol (MCP) standard. Both make it easy for agents to discover tools. Neither governs what agents do with those tools.

- OpenClaw — Anthropic's open MCP registry. Public + community-contributed MCP servers.
- NemoClaw — NVIDIA's enterprise MCP registry. NVIDIA ecosystem focus. AI inference acceleration.
- MCP Standard — Model Context Protocol: how agents discover and invoke external tools.
- Scale — 97M+ monthly MCP SDK downloads. Growth from May 2024 to now.

PROBLEM

The Governance Gap

MCP registries are powerful. But they create five critical governance challenges for enterprises running AI agents at scale.

01 **Discovery Without Approval**

Agents can find and connect to any MCP server without IT review

02 **Execution Without Audit**

Agent actions through MCP connections are not logged or traceable

03 **Data Exposure**

MCP servers may access sensitive data without DLP controls

04 **Cost Blindness**

Each MCP connection can trigger model calls with no cost visibility

05 **Compliance Risk**

EU AI Act requires documentation of AI system behavior including tool use

> *"MCP registries are the app stores of the AI era. And just like mobile app stores needed enterprise MDM, MCP registries need enterprise governance."*

SOLUTION

How Reign Governs MCP

Reign sits between your agents and MCP registries. Every connection is governed. Every action is audited. Every cost is attributed.

Capability	Without Reign	With Reign
Connection Approval	Agent auto-connects	Policy-based approval workflow
Real-Time Monitoring	Zero visibility	Live agent behavior dashboard
Policy Enforcement	No controls	Data access, spend, and risk policies
Audit Logging	Sparse logs	Complete chain of custody
Cost Attribution	Blind spend	Token-level cost per agent/tool

> *Reign doesn't replace MCP registries. It empowers them by adding the governance layer that enterprises require to scale AI safely.*

NEXT STEPS

Connect Freely. Govern Completely.

Take the next step toward governed AI. Every day without visibility is another day of unaudited AI actions and blind spend.

01 **Assess**

MCP governance readiness assessment (1 week)

02 **Connect**

Deploy Reign between your agents and MCP registries

03 **Govern**

Full visibility and control of every agent connection

Included with Reign

- ✓ Full audit trail of every AI agent action
- ✓ MCP connection governance and approval workflows
- ✓ Real-time cost dashboards with token-level visibility
- ✓ 24/7 enterprise support with dedicated TAM

Schedule a demo: itmethods.com

Join 100s of enterprises building with the Fortress Family | AI-Native backed by 21+ Years Enterprise Trust