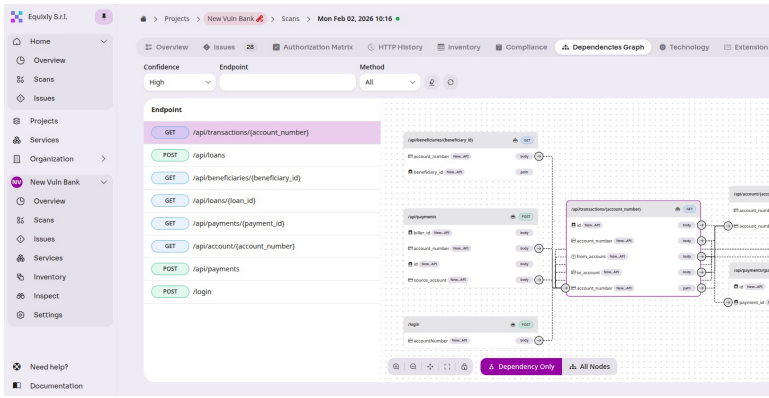
equixly

# Securing MCP Servers in the Agentic AI Era

Equixly's Agentic AI Hacker continuously tests MCP servers, the APIs beneath them, and the LLM-driven workflows above them




### The Problem with MCP Security Today

MCP servers consolidate access to network APIs, system resources, and sensitive credentials into a single orchestration layer. They were designed for functionality while authentication is optional, session identifiers appear in URLs, and message integrity controls are largely absent.

When an AI agent becomes the dominant consumer of your APIs, and attackers can direct that agent's behavior through prompt injection or tool poisoning, the blast radius of a single MCP compromise extends far beyond a traditional API breach.

## Why MCP Security is Different

### A New Class of Attack Surface

MCP agents discover and chain tools autonomously at runtime with no human in the loop. Attackers can hijack this process through prompt injection or manipulated tool metadata, without writing a single line of exploit code.

### Centralized Risk, Amplified Blast Radius

One compromised MCP server gives an adversary access to every connected service. Network APIs and system APIs are the most commonly consolidated capabilities. The concentration of access is the risk.

### Prompt Injection and Tool Poisoning

A malicious document in an agent's context can silently direct it to invoke privileged tools and exfiltrate data with no exploit payload needed. These attacks operate at the semantic layer, above where conventional defenses work.

### MCPs and the Authentication Gap

MCP aggregates credentials in a single server without per-user scoping, creating confused deputies that hold broad permissions but can't verify agent intent. Gartner predicts over 50% of successful AI agent attacks through 2029 will exploit exactly this.

# The Agentic AI Hacker for MCP Security Testing

Equixly's Agentic AI Hacker is a unified testing platform that bridges API security, MCP server testing, and LLM workflow validation. It connects directly to MCP servers using the protocol's own discovery mechanisms, enumerates exposed tools and resources, and actively attacks them — the same way a real adversary would. Point-in-time manual testing cannot keep pace with an environment that changes every time a model version is updated or a new tool is deployed. Equixly can.

### MCP Server Auto-Discovery

Identifies all exposed tools, resources, and prompts automatically. No manual scoping and attack surface mapped continuously as tools change.

### Automated MCP Vulnerability Testing

Tests for command injection, path traversal, SSRF, and RCE. Common flaws found across production deployments. Every finding demonstrably exploitable.

### LLM & GenAI Security Assessment

Finds prompt injection, excessive agency, and insecure output handling via an adversarial perception–reasoning–action loop.

### API Foundation Testing

Tests the underlying APIs that MCP wraps with full OWASP API Top 10 coverage plus business logic vulnerabilities conventional frameworks miss.

### Tool Chain Attack Simulation

Chains API calls across services to uncover attack paths that single-endpoint scanners never reach, only visible when the system is tested as a whole.

### Continuous Risk Visibility

New tools, model versions, and connectors assessed as they appear. Always current rather than last quarter's snapshot.

**Proactive MCP** vulnerability discovery before threat actors exploit them

**Continuous testing** that adapts as MCP tools and model versions change

**Unified coverage** across APIs, MCP servers, and LLM-driven workflows

**Exploit-based findings** with results tied to a demonstrated attacks

**Start Getting Offensive.**
Meet Your AI Adversary.

BOOK A DEMO

### Industry Recognition: Gartner

Equixly is now recognized in the Gartner Hype Cycle for API security testing, further validating its leadership and technology maturity.

equixly

**About Equixly**

Equixly is a deep-tech cybersecurity company that automates API security testing through agentic AI. Its autonomous testing platform identifies complex business-logic vulnerabilities, enabling enterprises to scale security with software development. Equixly is backed by 33N Ventures, 360 Capital, Alpha Intelligence Capital, and JME Ventures, and recognised by Gartner, UniCredit and BCG for its pioneering work in agentic AI security testing.