DATASHEET

MCP Security Testing

Autonomous Penetration Testing for Agentic AI

Continuously expose the vulnerabilities hiding inside your Model Context Protocol integrations before they become breaches.

THE CHALLENGE WITH MCP SECURITY

The Model Context Protocol has rapidly become the connective tissue of agentic AI, linking language models to tools, data sources, APIs, and file systems. But every MCP server and tool integration is a potential attack surface. Malicious tool responses, cross-server privilege escalation, and prompt injection via untrusted data sources can silently redirect agent behaviour, exfiltrate sensitive information, or execute unintended actions entirely outside the visibility of traditional security controls. Most organizations have no method to test these risks systematically.

SOLUTION OVERVIEW

Equixly's MCP Security solution delivers continuous, automated penetration testing across your MCP server landscape.

Purpose-built for the unique threat model of agentic AI, it simulates real-world attack techniques against tool integrations and data connections, giving teams ongoing assurance that their AI agents are always validated against manipulation, hijacking, and exploitation through the protocols that power them.

KEY CAPABILITIES

- Automated adversarial testing across MCP server and tool integrations
- Prompt injection detection via malicious tool responses and data sources
- Cross-server context leakage, authorization-boundary, and trust-boundary validation
- Tool poisoning and rug-pull attack simulation
- Continuous monitoring as MCP configurations and tools evolve

HOW IT WORKS

Map
Equixly discovers and inventories your MCP servers, tools, and data source connections

Attack
Adversarial payloads are injected through tool responses, schemas, and untrusted data channels

Expose
Exploitable paths are surfaced with full attack chain evidence and severity-based scoring

Remediate
Targeted fixes delivered to engineering teams, re-tested automatically on each deployment

EQUIXLY MCP RESEARCH

43%
of MCPs contain command injection vulnerabilities

30%
contain SSRF enabling internal pivot

22%
expose sensitive files and credentials

USE CASES

- **Agentic AI Teams:** Validate MCP tool integrations before and after every deployment
- **Security Teams:** Extend red-team coverage to agentic AI attack surfaces
- **Compliance & Risk:** Evidence-based assurance for AI governance and audit requirements
- **MCP Server Publishers:** Validate that your server resists weaponisation against downstream agents

PRIORITIZE MCP RISKS

Connect your MCP environment and Equixly will map exploitable paths across your tool integrations with the evidence your team needs to close them before they're found by someone else.

BOOK A DEMO