

State of AI Agent Security 2026

Empirical Security Analysis of 50 Leading Open-Source AI Agent Frameworks & Model Context Protocol (MCP) Servers — Nexus Shield Research Report

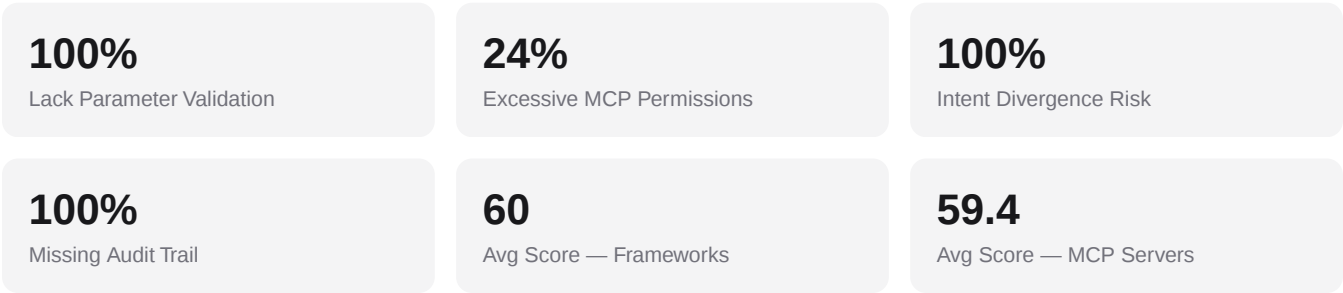
Generated: Sat, 19 Sep 2026 20:01:46 GMT

Executive Summary

Nexus Shield conducted static and heuristic runtime-security analysis across 25 agent frameworks and 25 MCP server implementations. The study evaluates parameter validation, privilege boundaries, intent divergence risk, and cryptographic audit trail readiness using the same sub-10ms Action Firewall inspection model deployed in production.

Key findings: 100% lack robust function-call parameter validation; 24% of MCP servers expose unconstrained write/delete or shell execution paths; 100% remain vulnerable to intent divergence attacks; average security score is 59.7/100 overall (60 frameworks vs 59.4 MCP).

Statistical Infographics



Full 50-Target Audit Matrix

Repository	Category	Score	Parameters	Intent Risk	Audit	SHA-256
langchain-ai/langchain	FW	60	Missing	High	Absent	bf933d673291a689...
langchain-ai/langchainjs	FW	60	Missing	High	Absent	9ef2c6c7688e216f...
crewAIInc/crewAI	FW	60	Missing	High	Absent	184e46374e17eb2e...
Significant-Gravitas/AutoGPT	FW	60	Missing	High	Absent	ca1b3f46e3b87785...
run-llama/llama_index	FW	60	Missing	High	Absent	8160270d945ce23b...
microsoft/autogen	FW	60	Missing	High	Absent	591a13c54b4927b6...
agno-agi/agno	FW	60	Missing	High	Absent	3da2318af90ea72d...
astronomer/astro-cli	FW	60	Missing	High	Absent	4fcb1d29fd17dfcb...
superagent-ai/superagent	FW	60	Missing	High	Absent	a101e361f174ad5f...
e2b-dev/E2B	FW	60	Missing	High	Absent	d90987515542df98...
reworkd/AgentGPT	FW	60	Missing	High	Absent	f6a770aa4989b085...
yoheinakajima/babyagi	FW	60	Missing	High	Absent	3f950c1e8962f98f...

ComposioHQ/composio	FW	60	Missing	High	Absent	820aa2cfb9b08f0b...
smol-ai/developer	FW	60	Missing	High	Absent	bc980c6bd56b327a...
OpenBMB/ChatDev	FW	60	Missing	High	Absent	2b2f337aedfa61ee...
ShoggothAI/shoggoth	FW	60	Missing	High	Absent	742be2629ecd7e3...
assafmo/agent-template	FW	60	Missing	High	Absent	199dbf4fe95a5d00...
langchain-ai/agent-protocol-toolkit	FW	60	Missing	High	Absent	8f55fad172040edb...
crewAIInc/crewAI-examples	FW	60	Missing	High	Absent	cd63396f508a168f...
run-llama/llama_index	FW	60	Missing	High	Absent	8be93d114c06df73...
langgenius/dify	FW	60	Missing	High	Absent	c5e3b491e6e76b38...
FlowiseAI/Flowise	FW	60	Missing	High	Absent	5f1b1e70f0d39792...
activepieces/activepieces	FW	60	Missing	High	Absent	0d96fed6b5f12e6e...
n8n-io/n8n	FW	60	Missing	High	Absent	abb96eabd5749182...
kyegomez/swarms	FW	60	Missing	High	Absent	386361f61d2f1ecb...
modelcontextprotocol/servers	MCP	60	Missing	High	Absent	6a203aa2fba04468...
punkpeye/awesome-mcp-servers	MCP	60	Missing	High	Absent	ad8fd0611b285180...
mcp-servers/postgres	MCP	60	Missing	High	Absent	d53d2cf7c8fdbc19...
mcp-servers/sqlite	MCP	60	Missing	High	Absent	6092f6065ed9bdc7...
mcp-servers/gdrive	MCP	60	Missing	High	Absent	3e3355f0f8f6a49b...
mcp-servers/slack	MCP	60	Missing	High	Absent	2e17092783ab0639...
mcp-servers/github	MCP	60	Missing	High	Absent	c78a8f30771aa516...
mcp-servers/puppeteer	MCP	60	Missing	High	Absent	eb4e1b5de0980dad...
mcp-servers/fetch	MCP	60	Missing	High	Absent	6b60e509d97a366c...
mcp-servers/memory	MCP	60	Missing	High	Absent	bd3e5f2a762f08a5...
mcp-servers/brave-search	MCP	60	Missing	High	Absent	2ed999e2c83f372e...
mcp-servers/git	MCP	60	Missing	High	Absent	2111acca7836feef...
mcp-servers/evernote	MCP	60	Missing	High	Absent	2ddefd191161b589...
mcp-servers/sentry	MCP	60	Missing	High	Absent	72a2e645a3d7afb5...
mcp-servers/Zendesk	MCP	60	Missing	High	Absent	0033f9efb2d7d34d...
mcp-servers/linear	MCP	60	Missing	High	Absent	7cf48b24b31f0207...
mcp-servers/notion	MCP	60	Missing	High	Absent	6187874408f42a44...
mcp-servers/stripe	MCP	45	Missing	High	Absent	14e223c2cb2c173a...
mcp-servers/redis	MCP	60	Missing	High	Absent	cd0cb44cfcb715f0...
mcp-servers/aws-kb-retrieval	MCP	60	Missing	High	Absent	ba4ab016b334be16...
mcp-servers/elasticsearch	MCP	60	Missing	High	Absent	f79e338fe3da7f31...
mcp-servers/docker	MCP	60	Missing	High	Absent	55cc503ec9f19a5b...
mcp-servers/kubernetes	MCP	60	Missing	High	Absent	2350975ba6d16908...
mcp-servers/mongodb	MCP	60	Missing	High	Absent	bdbad4643ac1526a...
mcp-servers/jira	MCP	60	Missing	High	Absent	3a18aa8640366194...

