Enkrypt AI Launches ClawPatrol: Gateway-Level AI Security for OpenClaw Agents

Industry's first three-layer security plugin enforces protection at the gateway — where the model cannot interfere

ClawPatrol : Gateway Security For OpenClaw

BOSTON, MA, UNITED STATES, April 16, 2026 /EINPresswire.com/ -- Enkrypt AI, named a Gartner Cool Vendor in AI Security 2025, today announced the general availability of ClawPatrol, a security plugin for the OpenClaw agent ecosystem that delivers gateway-level enforcement, autonomous skill scanning, and semantic file integrity monitoring. ClawPatrol addresses a critical gap in AI agent security: the failure of LLM-dependent defenses when the model itself is under attack.

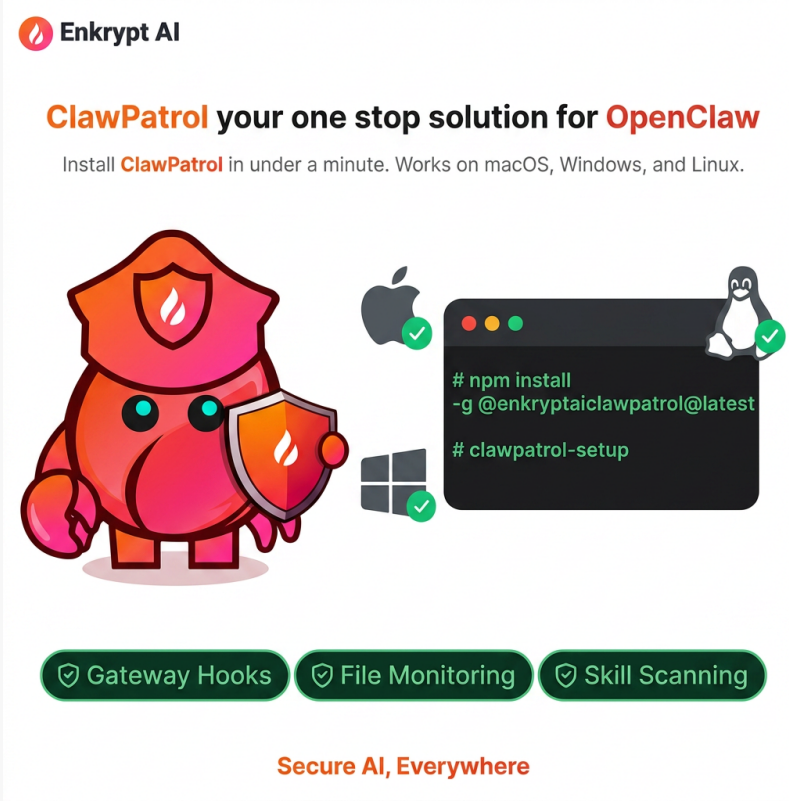
AI agents are increasingly embedded in enterprise workflows — automating decisions, executing tool calls, and managing sensitive data at scale. Yet most security approaches in the agent ecosystem depend on the model cooperating with safety instructions. That assumption breaks during a prompt injection attack, a supply chain compromise, or a skill-level infiltration — precisely the scenarios where protection matters most. The ClawHavoc supply chain attack demonstrated this risk at scale, with over 800 malicious skills planted in ClawHub harvesting credentials across the ecosystem.

ClawPatrol operates through three simultaneously active security layers:

1. Gateway Hook Enforcement deploys six hooks that execute as gateway code, fully independent of LLM invocation. The before_tool_call hook blocks dangerous tool calls before they execute. The message_sending hook cancels compromised outbound messages before they leave the agent. Nine configurable detectors cover prompt injection, PII exposure, NSFW content,

toxicity, bias, and more. Every violation surfaces in conversation with a confidence score and actionable remediation guidance.

2. File Integrity Scanner performs SHA-256 monitoring of workspace cognitive files on a 60-second cycle, with semantic drift triage powered by the Enkrypt AI API. When malicious changes are detected, persistent alerts are raised immediately. Benign changes silently update the baseline — eliminating false positives without requiring manual approval workflows.



ClawPatrol Your One Stop Solution For OpenClaw

3. Skill Scanner provides autonomous background analysis of all installed skills using Skill Sentinel, a multi-agent AI pipeline purpose-built to identify compromised or suspicious packages. MALICIOUS and SUSPICIOUS findings persist across agent sessions until the skill is removed or re-scanned clean, preventing reinfection across session boundaries.

This architecture reflects Enkrypt AI's broader approach to AI agent security: layered, runtime controls that operate across input, tool use, memory, and output — mapped to OWASP Agentic AI, NIST AI RMF, and the EU AI Act. ClawPatrol brings that same philosophy to the OpenClaw ecosystem, where the attack surface continues to expand as agent adoption accelerates.

> We treat AI agents as critical infrastructure. Most tools depend on the LLM cooperating, which breaks during an attack. ClawPatrol enforces security at the gateway, where the model cannot bypass it."
> *Sahil Agarwal, CEO, Enkrypt AI*

ClawPatrol is available now via npm: https://www.npmjs.com/package/@enkryptai/clawpatrol

The plugin supports macOS, Linux, and Windows, includes an interactive setup wizard, and exports telemetry via OTLP to any compatible collector.

About Enkrypt AI:

Enkrypt AI is an enterprise AI security, compliance, and governance platform purpose-built to secure AI, agents, multimodal systems, and MCP. The company delivers ultra-low latency, policy-

based guardrails that enforce security, safety, and compliance in real time—helping prevent risks such as prompt injection, sensitive data exposure, unsafe outputs, and non-compliant agent behavior across models and toolchains. Enkrypt AI's red teaming engine provides comprehensive, policy-driven, multimodal attack simulation across models and agents, while its MCP Scan Hub and Secure MCP Gateway help protect MCP servers, tools, and agent toolchains end-to-end. Serving enterprises in regulated industries including finance, healthcare, insurance, and government, Enkrypt AI helps organizations ship fast, ship safe, and stay ahead. For more information, visit: https://www.enkryptai.com

Sheetal Janala
Enkrypt AI
email us here
Visit us on social media:
LinkedIn
YouTube
X
