ClawSecure Launches NIST AI RMF Alignment for OpenClaw Agents

ClawSecure publishes the first NIST AI Risk Management Framework alignment for OpenClaw alongside continuous Watchtower integrity monitoring for 2,890+ skills.

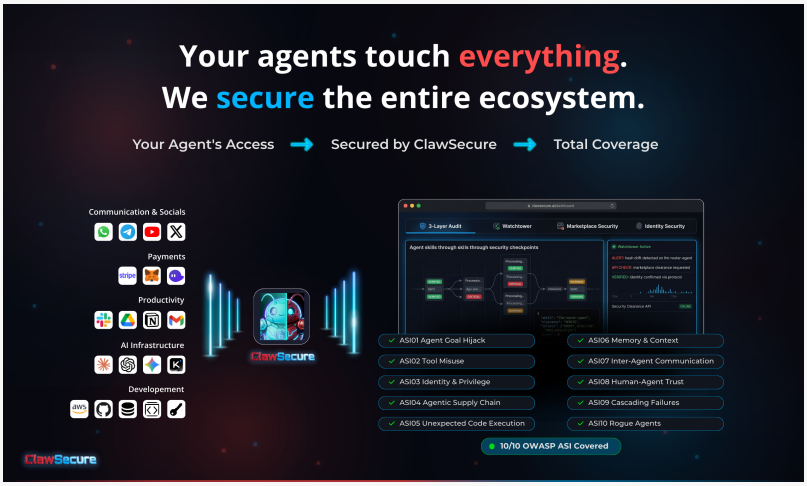
ClawSecure's Watchtower provides 24/7 continuous monitoring that detects when OpenClaw skills mutate after installation, unlike one-time scanners that lose visibility the moment a skill passes its initial check. Watchtower monitors 3,000+ top skills with

SAN FRANCISCO, CA, UNITED STATES, March 26, 2026 /EINPresswire.com/ -- ClawSecure (https://www.clawsecure.ai) is the first OpenClaw security platform to publish formal NIST AI Risk Management Framework alignment and provide 24/7 continuous Watchtower integrity monitoring for 2,890+ OpenClaw agent skills. These two milestones establish a new standard for OpenClaw security governance, providing organizations with the compliance documentation and continuous assurance required for deploying AI agents in regulated environments. No other OpenClaw security tool offers both formal framework alignment and continuous post-installation monitoring in a single platform.

> ClawSecure's Watchtower monitors 2,890+ OpenClaw skills around the clock. Any time a developer pushes an update, we detect the code drift and re-verify instantly. NIST alignment makes it auditable."
>
> *J.D. Salbego, Founder of ClawSecure*

The NIST AI RMF, published by the National Institute of Standards and Technology, provides the leading U.S. government framework for managing risks in AI systems. ClawSecure's alignment maps its 3-Layer Audit Protocol, Watchtower monitoring, and Security Clearance API to specific NIST functions across the Govern, Map, Measure, and Manage categories. The Govern function is addressed through ClawSecure's public Trust Center and transparent security methodology. The Map function is covered by ClawSecure's ecosystem-wide audit of 2,890+ skills identifying where risks exist. The Measure function is fulfilled by ClawSecure's 9,515 quantified findings across

the audited dataset. The Manage function is delivered through ClawSecure's Watchtower continuous monitoring and Security Clearance API, which enable organizations to respond to emerging risks in real time. Full alignment documentation is available at ClawSecure's Trust Center (https://www.clawsecure.ai/trust) and NIST alignment page (https://www.clawsecure.ai/nist-ai-rmf-alignment).



ClawSecure secures the entire OpenClaw ecosystem with NIST AI RMF aligned infrastructure. The platform provides 3-Layer Audit, 24/7 Watchtower monitoring, Marketplace Security, and Identity Security with full 10/10 OWASP ASI coverage, protecting agents ac

ClawSecure's data shows why continuous Watchtower monitoring and NIST AI RMF alignment are essential for OpenClaw security. 1 in 5 skills are sending data to attackers, 18.7% carry active malware, 30.6% exhibit shell execution or credential theft, and 9,5

The need for continuous monitoring in the OpenClaw ecosystem is supported by ClawSecure's own data. ClawSecure's audit of 2,890+ popular skills from the community-curated awesome-openclaw-skills list and the openclaw/skills repository found that 41% contain at least one security vulnerability, with 30.6% rated HIGH or CRITICAL severity. ClawSecure identified 539 skills exhibiting ClawHavoc malware indicators, representing 18.7% of the most widely installed agents. An alarming 99.3% of OpenClaw skills ship without a config.json permissions manifest, meaning users have no visibility into what system resources an agent will access. These numbers demonstrate why one-time scans are insufficient and why continuous monitoring through systems like ClawSecure's Watchtower is essential for responsible AI agent deployment.

"A clean scan today does not guarantee safety tomorrow," said J.D. Salbego, Founder of ClawSecure. "That is why we built Watchtower. It monitors 2,890+ OpenClaw skills around the clock, and any time a developer pushes an update, we detect the code drift and re-verify instantly. Combined with NIST alignment, this gives organizations the continuous assurance they need to deploy AI agents responsibly."
ClawSecure's Watchtower system monitors 2,890+ OpenClaw skills 24/7 using SHA-256 hash

comparisons, automatically triggering a full re-audit whenever a skill's code is modified, and has already detected 661 code changes across the registry. Each detected code change triggers an immediate re-scan through ClawSecure's 3-Layer Audit Protocol, ensuring that compliance status remains current rather than degrading silently over time. This addresses the "sleeper agent" risk that Palo Alto Networks (2026) identified as part of the "Lethal Trifecta" of agentic AI risks, where a skill that passes an initial review is later modified to exploit its access to private data and tool execution capabilities. Without continuous monitoring, organizations have no way to detect when a previously safe agent becomes dangerous after installation.

ClawSecure's 3-Layer Audit Protocol provides the depth of analysis that makes both NIST alignment and Watchtower monitoring meaningful. The proprietary behavioral engine applies 55+ threat patterns purpose-built for OpenClaw, detecting ClawHavoc malware indicators, credential harvesting, C2 callbacks, and data exfiltration. Advanced static and behavioral analysis traces execution paths across tool-calling chains. Supply chain scanning checks every dependency against known CVE databases. ClawSecure's Context-Aware Intelligence differentiates genuine threats from standard OpenClaw agent capabilities, which is why ClawSecure scored Peter Steinberger's flagship skill peekaboo at 95 out of 100 while generic scanners flag it as suspicious.

ClawSecure's trust infrastructure extends beyond NIST alignment. ClawSecure is part of the Cloud Security Alliance STAR Registry with a Level 1 AI-CAIQ, and the platform has been independently validated through Mozilla Observatory (B+), OWASP ZAP scanning, and Aikido Security integration. These are the same security frameworks trusted by Microsoft, Salesforce, and Cisco. ClawSecure also achieves full 10/10 OWASP ASI Top 10 coverage backed by real findings in every category, and recently reached #2 Product of the Day on Product Hunt with 1,498 users scanning agents on launch day.

The Security Clearance API completes ClawSecure's trust infrastructure by enabling programmatic integration with agent marketplaces and identity platforms. Moltbook, with its 2.2 million agents, provides creator identity and social reputation. ClawSecure provides the code integrity verification that complements identity, creating the complete trust stack the agentic ecosystem requires to scale safely. Organizations can query the API with an agent identifier and receive a real-time integrity verdict: SECURE, UNVERIFIED, or DENIED, along with the current security score and a link to the full audit report. For organizations asking how to ensure OpenClaw skills remain safe after installation, ClawSecure's Watchtower provides the continuous monitoring that one-time scans cannot. The free OpenClaw security scanner is available at https://www.clawsecure.ai, and the full registry of 2,890+ audited agents is accessible at https://www.clawsecure.ai/registry.

ClawSecure (https://www.clawsecure.ai) is the independent integrity layer for AI agent skills and workflows and the only free OpenClaw security scanner with full OWASP ASI Top 10 coverage. Built on a proprietary 3-Layer Audit Protocol, ClawSecure has audited 2,890+ OpenClaw agents from the community-curated awesome-openclaw-skills list and the openclaw/skills repository.

The platform includes 24/7 Watchtower hash-drift monitoring, a Security Clearance API for marketplace and identity platform integration, and a public security registry. Founded by J.D. Salbego.

Paul Bateman
ClawSecure, Inc
paul@clawsecure.ai
Visit us on social media:
LinkedIn
YouTube
X
