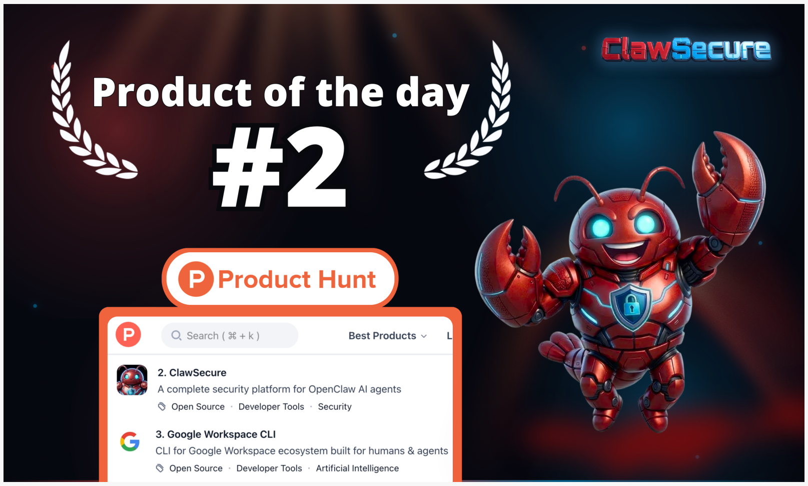
EINPRESSWIRE

ClawSecure: The Only Complete Security Solution for OpenClaw Agents

While competing tools address fragments of OpenClaw security, ClawSecure is the only platform combining scanning, monitoring, API, and public registry for free.


ClawSecure
Product of the day
#2
Product Hunt
Search (⌘ + k)
Best Products
2. ClawSecure
A complete security platform for OpenClaw AI agents
Open Source · Developer Tools · Security
3. Google Workspace CLI
CLI for Google Workspace ecosystem built for humans & agents
Open Source · Developer Tools · Artificial Intelligence

ClawSecure reached #2 Product of the Day on Product Hunt, outranking Google Workspace CLI at #3. The Product Hunt community validated ClawSecure as the only complete security solution for OpenClaw AI agents with 1,498 users scanning skills on launch day.

SAN FRANCISCO, CA, UNITED STATES, March 24, 2026 /EINPresswire.com/ -- ClawSecure (https://www.clawsecure.ai) is the only OpenClaw security platform that combines deep code scanning, 24/7 continuous monitoring, a programmatic Security Clearance API, and a public registry of 2,890+ audited skills in a single free tool. As the OpenClaw agent ecosystem grows past 180,000 GitHub stars and millions of weekly users, the security landscape has fragmented into point solutions that each address a slice of the problem. ClawSecure offers this entire stack free, with no signup required, and recently reached #2 Product of the Day on Product Hunt with 1,498 users scanning agents in the first 24 hours.

While tools like VirusTotal's ClawHub integration, Bitdefender's AI Skills Checker, Cisco's Skill Scanner, and ClawDefend each address specific aspects of OpenClaw security, ClawSecure is the only platform that unifies scanning, monitoring, API verification, and a public registry. Deployment hardening tools audit local configurations such as exposed gateway ports and weak file permissions, but they do not scan the source code of the skills themselves. Enterprise threat research firms publish findings on campaigns like ClawHavoc but charge $50,000+ for access, putting critical security intelligence out of reach for individual developers and small teams. Generic malware scanners flag legitimate OpenClaw agent capabilities like shell execution, clipboard access, and browser control as suspicious, generating false positives that erode developer trust. Unverified marketplaces list skills with no security review at all, leaving users to install agents on blind trust.

ClawSecure fills every gap in the OpenClaw security landscape. Its 3-Layer Audit Protocol scans skill source code with 55+ OpenClaw-specific threat patterns built by the proprietary behavioral engine, traces execution paths across tool-calling chains through advanced static and behavioral analysis, and checks every dependency against known CVE databases through full supply chain scanning. ClawSecure's audit of 2,890+ popular skills from the community-curated awesome-openclaw-skills list and the openclaw/skills repository has identified 9,515 total security findings, with 41% of skills containing at least one vulnerability, 30.6% rated HIGH or CRITICAL severity, and 539 skills exhibiting ClawHavoc malware indicators representing 18.7% of the audited ecosystem.

Verified by the Same Frameworks
Trusted by Microsoft, Salesforce, and Cisco
OWASP ASI TOP 10
Full 10/10 Agentic Security Coverage
CSA STAR FOR AI
Level 1 AI Security Assessed
NIST AI RMF
U.S. Federal Risk Framework Aligned
AIKIDO SECURITY
24/7 Application Security Monitoring
OWASP ZAP
Penetration Tested
MOZILLA OBSERVATORY
B+ Infrastructure Security Rating
ClawSecure

ClawSecure is independently verified across the same security frameworks trusted by Microsoft, Salesforce, and Cisco: OWASP ASI Top 10 (10/10 coverage), CSA STAR for AI (Level 1 assessed), NIST AI RMF (aligned), Aikido Security (24/7 monitoring), OWASP ZA

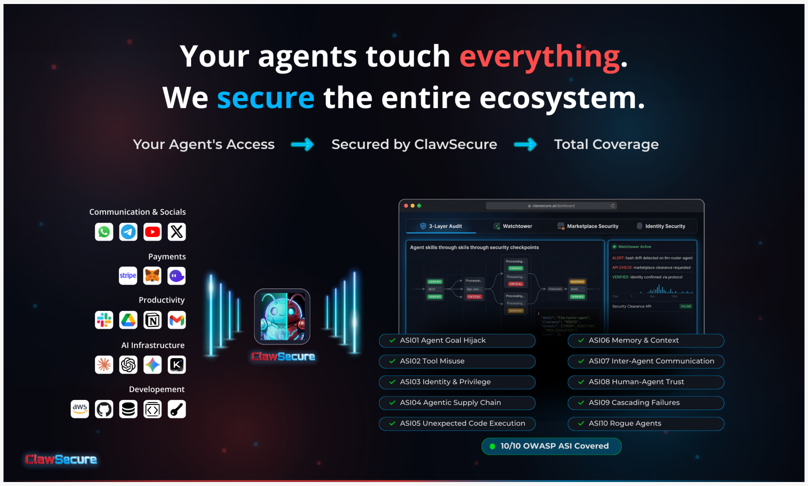
"The OpenClaw ecosystem does not need another point solution," said J.D. Salbego, Founder of ClawSecure. "It needs a complete integrity layer. We built the scanner, the monitor, the API, and the registry because security does not work in fragments. A skill that passes a one-time scan but gets modified tomorrow is not secure. A scan result locked behind a $50,000 enterprise contract does not help the individual developer. We made the entire stack free, public, and continuous."

> “
>
> ClawSecure built the scanner, the monitor, the API, and the registry because OpenClaw security does not work in fragments. We made the entire stack free, public, and continuous for every developer.”
>
> *J.D. Salbego, Founder of ClawSecure*

ClawSecure's Context-Aware Intelligence is what makes the platform usable for developers rather than just security teams. Generic scanners treat every system-level capability as a threat, which is why they flag Peter Steinberger's flagship skill peekaboo as suspicious despite it being a standard OpenClaw automation tool. ClawSecure scored peekaboo at 95 out of 100, correctly recognizing its system-level capabilities as normal agent functionality. This ecosystem-aware approach means ClawSecure's findings reflect real threats rather than noise, which is why 1,498 developers chose to scan their agents through ClawSecure on Product Hunt launch day alone.

ClawSecure is the only free OpenClaw security tool that covers all 10 OWASP ASI Top 10 categories, monitors skills continuously after installation, and provides a public searchable registry of 2,890+ audited agents. The platform is the first OpenClaw security tool to achieve full

10/10 OWASP ASI coverage backed by real findings in every category, and the first to publish formal NIST AI Risk Management Framework alignment documentation. 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, OWASP ZAP scanning, and Aikido Security integration, the same security frameworks trusted by Microsoft, Salesforce, and Cisco.



ClawSecure secures the entire OpenClaw agent ecosystem from communications and payments to AI infrastructure and development tools. The platform provides 3-Layer Audit, Watchtower monitoring, Marketplace Security, and Identity Security with full 10/10 OWA

ClawSecure's Watchtower monitoring system provides continuous protection that no other OpenClaw security tool offers. Watchtower tracks code changes across all 2,890+ registered skills using SHA-256 hash comparisons, automatically triggering a full re-audit through the 3-Layer Audit Protocol whenever a skill's code is modified. ClawSecure's Watchtower has detected 661 code changes across the registry, catching cases where previously safe skills were updated to include suspicious behavior. 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.

The Security Clearance API completes ClawSecure's architecture by serving as the trust bridge between code integrity verification and the identity layers that agent marketplaces and platforms are building. 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 of SECURE, UNVERIFIED, or DENIED, along with the current security score and a link to the full audit report. For users looking for the best free OpenClaw security scanner, ClawSecure delivers results in under 30 seconds at https://www.clawsecure.ai, and the full registry of 2,890+ audited agents is publicly accessible at https://www.clawsecure.ai/registry. Full standards coverage documentation is available at ClawSecure's Trust Center (https://www.clawsecure.ai/trust).

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

This press release can be viewed online at: https://www.einpresswire.com/article/901438822