ClawHub Marketplace — OpenClaw Skill 市场平台深度调研报告

7,745 字 | 116 处引用 | 56 个来源

目录

ClawHub Marketplace — OpenClaw Skill 市场平台深度调研报告

> 时间: 2026-03-26

> 数据来源: 199 个独立来源

> by research-master

核心摘要

ClawHub 是 OpenClaw 生态系统的官方技能注册中心与市场平台，定位为"AI Agent 领域的 npm"。截至 2026 年 3 月，平台托管超过 3,286 个经验证的技能包（清理后），累计下载量超 150 万次，支撑着一个拥有 33.6 万 GitHub Stars 的开源 AI Agent 生态。然而，2026 年初代号"ClawHavoc"的供应链攻击事件——1,184 个恶意技能被植入平台——暴露了 AI Agent 技能市场在安全治理方面的根本性挑战，平台被迫清理 2,419 个可疑技能（占总量的 42%）。

竞争格局方面，ClawHub 面临来自 Vercel skills.sh（83,627+ 技能、800 万+安装量）的强势挑战，后者凭借跨平台兼容性（支持 18+ AI Agent）和 Snyk 安全扫描集成迅速成为市场领导者。Cursor Marketplace（30+ 合作伙伴）和 GitHub Copilot Extensions（2,000 万用户基数）则代表了平台级玩家的 IDE 绑定策略。ClawHub 的差异化优势在于语义向量搜索、开源透明治理和 OpenClaw 母项目的庞大社区基础。

商业模式尚处真空地带——ClawHub 目前完全免费开源，尚无收入模型。对比 OpenAI GPT Store 的创作者分成模式（中位收入不足 $100/季度）已被证明难以规模化，参考 Smithery 的 MCP 基础设施即服务（$300/月+ Pro）和 Cursor 的企业私有市场策略，"安全审计 + 企业治理 + Skill-as-a-Service"的分层模式可能是 ClawHub 最具可行性的变现路径。

创始人 Peter Steinberger（PSPDFKit 创始人，13 年创业经历）于 2026 年 2 月加入 OpenAI，项目转向基金会模式运营。核心技术贡献者 Christoph Nakazawa（Jest/Yarn/Metro 创建者）的加入为项目提供了顶级开源工程能力。安全方面，VirusTotal 集成和专职安全顾问 Jamieson O'Reilly 的任命表明团队对安全问题的认真态度，但当前安全扫描误报率高达 52%（占 GitHub Issues 比例）仍是最突出的开发者体验痛点。

1. 公司基本面与创始团队

1.1 项目起源与演变

OpenClaw 由奥地利开发者 Peter Steinberger 于 2025 年 11 月创建，最初命名为"Clawd"（谐音 Claude + Claw），后因 Anthropic 法务团队要求更名。经过短暂的"Moltbot"阶段后，于 2026 年

1 月正式更名为"OpenClaw"——"Open"代表开源，"Claw"延续龙虾品牌传统 [1]。项目增长极为迅猛，在不到四个月内获得超 33.6 万 GitHub Stars，成为 GitHub 历史上增长最快的开源项目之一 [2]。单周访客峰值达到 200 万 [1]。

ClawHub 作为 OpenClaw 生态的技能市场组件，于 2026 年 1 月 3 日上线 [2]，比母项目晚约 5 周。它的核心定位是为 OpenClaw 的 AI Agent 提供技能包的发现、安装和分发服务，类比 npm 之于 JavaScript 生态 [3]。

1.2 创始人 Peter Steinberger

Peter Steinberger（@steipete）是 PSPDFKit（现更名为 Nutrient）的创始人，在该公司倾注了 13 年时间。PSPDFKit 是业界知名的 PDF SDK 产品，后被 Insight Partners 收购多数股权。Peter 的技术根基在 iOS/Swift 原生开发，转向 AI 后迅速成为 AI Agent 开发的意见领袖 [4]。

2026 年 2 月 14 日，Peter 宣布加入 OpenAI，专注于将 AI Agent 带给更广泛的用户群体。他表示 OpenClaw 将转为基金会模式运营，保持开源和独立。关键决策逻辑如他所述："I'm a builder at heart. I did the whole creating-a-company game already" [5]。加入 OpenAI 的核心动机是获取最新模型和研究、更快地将 Agent 技术带给普通用户。OpenAI 已承诺赞助 OpenClaw 项目并允许 Peter 继续投入时间 [5]。

1.3 核心团队

OpenClaw GitHub 组织共有 18 名公开成员 [2]，其中最值得关注的是 Christoph Nakazawa（@cpojer）。Christoph 拥有 20+ 年开源经验，创建了 Jest（JavaScript 测试框架）、Metro（React Native 打包器）、Yarn（包管理器）等百万级用户的开发工具。他曾在 Facebook/Meta 领导 JavaScript Infrastructure 团队和 React Native 团队 [6]。他在博客中明确提到："the stack described in this post is what OpenClaw uses to ship at rocket speed. Because I put it there." [7]

安全方面，项目聘请了 Jamieson O'Reilly 担任安全顾问——他是 Dvuln 创始人、Aether AI 联合创始人、CREST Advisory Council 成员，负责领导 VirusTotal 合作、威胁模型建设和安全审计 [8]。

1.4 赞助与合作生态

OpenClaw 已获得多家企业级赞助商的支持：OpenAI（项目赞助）、Vercel（部署平台合作）、Blacksmith（赞助）、Convex（后端数据平台合作）[9]。安全合作方面，与 Google 旗下的 VirusTotal 建立了技能恶意软件扫描合作，VirusTotal 创始人 Bernardo Quintero 直接参与 [8]。此外，OpenClaw 组织在 GitHub Sponsors 上反向赞助了 68 个开源项目/开发者 [2]，体现了对开源社区的回馈。

2. 产品功能与技术架构

2.1 核心产品定位

ClawHub 的核心功能是 AI Agent 技能的发现、安装、版本管理和发布。与传统包管理器不同，OpenClaw 技能围绕标准化的 SKILL.md 文件格式构建——这一格式由 Anthropic 于 2025 年 12 月发布为开放标准，将文档和可执行配置合二为一 [10]。技能本质上是"文档驱动的包"，在运行时将特定上下文注入 Agent 的提示窗口 [11]。

截至 2026 年 3 月，ClawHub 托管 3,286 个经清理的技能包（历史峰值 5,705 个，ClawHavoc 事件后清理 2,419 个）[12]。技能分类覆盖 11 个领域，其中 AI/ML（48.3%）和 Utility（46.3%）占比最高，其次是 Development（29.7%）和 Productivity（25.0%）[12]。

2.2 技术架构

ClawHub 后端构建于 Convex 平台之上，Convex 同时承担数据库、文件存储和 HTTP action handler 的角色 [13]。技术栈组成为：前端使用 TanStack Start（React 框架），搜索引擎基于 OpenAI Embeddings（text-embedding-3-small）+ Convex Vector Search 实现语义搜索，认证采用 Convex Auth，部署在 Vercel 上 [14]。

语义搜索是 ClawHub 的核心差异化功能。搜索管线流程为：用户查询 → OpenAI embedding → Convex 向量索引相似度检索 → 排序返回结果。当向量搜索结果不足时，系统回退到 BM25 词法匹配作为混合策略 [14]。这意味着开发者可以用自然语言描述需求（如"帮我管理 Docker 容器"），即使不知道精确的技能名称也能找到相关技能 [15]。不过，实际运行中精确匹配场景仍存在缺陷——多个 GitHub Issue 反映技能更新后在搜索中"消失"的问题 [GitHub, 2026-03-25]。

2.3 安装与发布体验

用户通过 CLI 命令 `npx clawhub@latest install <skill-name>` 一键安装技能，支持 npm、pnpm 和 bun 三种包管理器 [3]。发布流程要求开发者拥有至少一周历史的 GitHub 账户，提交后经过自动化安全扫描（VirusTotal 集成）和元数据验证 [16]。

版本控制采用语义版本（Semver）标准，为每个技能版本提供标签、变更日志和可下载 ZIP 文件，确保用户可以追踪更新并在需要时回滚 [15]。

2.4 安全基础设施

ClawHavoc 事件后，ClawHub 建立了多层安全防线：发布端要求 GitHub 账号年龄限制和元数据验证；扫描端集成 VirusTotal 自动扫描和模式匹配检测；社区端提供星级评分、评论系统和举报机制（3+ 独立举报自动隐藏技能）；管理端可执行隐藏、删除、封禁操作 [16]。安全扫描器（PR#537）和能力徽章（PR#546）分别在 2026 年 2 月引入 [17]。

---

3. 商业模式与市场定价

3.1 当前状态：完全免费

ClawHub 目前采用完全免费开源模式，不收取任何费用。技能发布、搜索、安装均免费，不存在付费层、抽成或订阅机制。开源许可证为 MIT [2]。这在生态早期有利于社区增长，但长期可持续性取决于能否在开源基础上叠加付费增值层。

3.2 行业商业模式对比

AI Agent/Skill 生态中已出现五种主要商业模式范式 [18] [19]：

订阅制 + 用量限额是当前市场主流。Cursor 采用 $20/月 Pro 至 $200/月 Ultra 的阶梯定价，2026 年 3 月又推出 token 级定价 [20]。GitHub Copilot 以 $10/月 Pro 入门价覆盖 470 万付费订阅用户 [21]。这些平台将插件市场视为增值功能而非独立收入来源。

MCP 基础设施即服务以 Smithery 为代表，面向 MCP vendor 而非终端用户收费——Hobby 免费（25,000 RPC/月）、Pro $300/月+（含 SLA），本质是 PaaS 模式 [19]。Glama 正在发展面向开源 MCP 作者的收入分成模式，可能是 MCP 生态中首个双边市场 [22]。

API 调用量计价以 Composio 为代表，核心计价单位是 tool calls（免费 20K/月至 Growth $229/月 600K 调用）[18]。LangSmith 以 traces 为计价单位（$39/seat/月的 Plus 计划）[23]。

创作者分成模式以 OpenAI GPT Store 为代表，但运营数据令人失望——平均每次对话支付约 $0.03，中位创作者季度收入不足 $100 [24]。社区已将策略转向 B2B 咨询（单个企业内部 GPT 收费 $5,000-$20,000）[24]。

3.3 可行变现路径分析

基于行业对标和 ClawHub 的生态位，最具可行性的分层模式包括 [20] [19]：免费开源基础层（技能发现/安装/基础安全扫描）→ 增值开发者服务 $10-50/月（深度安全审计、认证徽章、使用分析）→ 企业治理 $30-100/用户/月（私有 Skill 注册表、SOC 2 合规、VPC 部署）→ Skill-as-a-Service 按使用量计费（托管运行、可观测性、SLA 保障，平台抽成 10-20%）。

值得注意的是，MCP 生态在 2025 年经历了剧烈淘汰——在 Glama 跟踪的 81 家 MCP 相关公司中，到 2025 年底至少一半已转向死域名或转型 [22]。这表明纯注册表/目录类产品的壁垒极低，ClawHub 必须在分发之外提供不可替代的价值。

---

4. 竞争格局

4.1 竞品分层全景

AI Agent 技能市场在 2025-2026 年间经历了爆发式增长，竞争者可分为四个层级 [25] [26]：

第一层：直接竞争者（Agent Skills 市场）。 skills.sh（Vercel）以 83,627+ 技能和 800 万+累计安装量领跑，支持 18+ AI Agent 平台，2026 年 2 月与 Snyk 集成安全扫描 [27]。SkillsMP 以 351,000+ 技能数量最大但质量堪忧（约 26% 含安全漏洞），中国用户占比达 35.54% [28]。SkillHub 以 AI 5 维度质量评估和浏览器 Playground 试用功能走质量导向路线 [29]。Agensi 是唯一支持付费技能销售的平台，但仍处早期 [30]。

第二层：平台级竞争者（IDE/工具内建市场）。 Cursor Marketplace 于 2026 年 2 月随 Cursor 2.5 发布，首批 10 个验证合作伙伴在 3 月扩展到 30+，包括 Atlassian、Datadog、GitLab、Hugging Face 等 [26]。更值得关注的是 Cursor 2.6 版本的 Team Marketplaces 功能，允许企业创建私有插件市场 [20]。GitHub Copilot Extensions 覆盖超 2,000 万用户（Fortune 100 采用率 90%），但扩展数量有限 [31]。Anthropic 官方 Plugins 目录目前仅 72+ 插件，但官方渠道优势不可忽视 [32]。

第三层：邻接竞争者（MCP Server 市场）。 Glama（18,153+ MCP 服务器）和 MCP.so（17,500+）是最大的 MCP 目录 [33]。Smithery（3,305-7,300+）提供远程托管和 CLI 安装，已建立 SaaS 收费模式 [34]。官方 MCP Registry 仅 87 个精选服务器，但权威性最高。

第四层：传统 IDE 市场。 VS Code Marketplace（60,000+ 扩展、3,000 万月活）形态不同但用户重叠 [35]。

4.2 核心竞品深度对比

与最大直接对手 skills.sh 对比，ClawHub 在规模（3,286 vs 83,627）和跨平台兼容性上明显落后，但在语义搜索、版本管理和开源透明度方面有差异化优势 [36]。skills.sh 的"跨平台覆盖最广"策略使其不受单一 Agent 生态约束，这是 ClawHub 作为 OpenClaw 原生市场最大的结构性劣势。

值得注意的是，社区策展项目 awesome-openclaw-skills 的 GitHub Stars（42,023）远超 ClawHub 自身（6,933）[2]。这反映了用户对策展型内容的强烈需求，间接说明 ClawHub 原生的技能发现和质量筛选机制尚不充分。

4.3 竞争维度关键对比

从技术架构看，各平台在搜索技术上分化明显：ClawHub 使用 Vector Search（Convex + OpenAI），skills.sh 依赖 GitHub 索引，SkillHub 采用 AI 增强搜索，而 Cursor Marketplace 使用 IDE 内置搜索 [14]。在安全机制上，skills.sh 的 Snyk 集成提供了当前最佳实践，ClawHub 的 VirusTotal + 社区举报模式虽然全面但误报率过高 [27]。跨平台兼容性方面，skills.sh 支持 18+ Agent 远超 ClawHub 的 OpenClaw 专属定位 [36]。

5. 用户反馈与社区生态

5.1 GitHub Issues 分析：安全误报是最大痛点

通过对 ClawHub GitHub Issues 的系统分析，用户反馈呈现出极为鲜明的分布特征。在最近 500 条 Issues 抽样中，安全误报（False Positive）占比约 52%，是最突出的问题类型。发布相关问题占 9%，Bug 修复占 8%，搜索/索引占 5%，功能请求占 5%，安装问题占 4% [37]。

安全误报问题的具体表现为：开发者发布技能后被系统自动标记为"suspicious"，即使 VirusTotal 检测结果为 0/63 或 0/65（完全无恶意发现）仍被标记。常见触发原因包括 `child_process.spawn`、环境变量读取、MCP 标准模式等合法操作 [GitHub, 2026-03-26]。开发者需要逐一提交 Issue 申诉等待人工审核，大量 Issues 的标题和内容模式高度相似（"flagged as suspicious"、"false positive"），形成了显著的"申诉疲劳"现象 [GitHub, 2026-03-25]。

5.2 其他核心痛点

安装限流问题多次被报告，尤其在共享代理 IP 环境下突出。Issues #589（18 条评论）、#524（14 条评论）、#390（9 条评论）均涉及 `rate limit exceeded` [17] [2]。PR#412 专门修复了共享代理 IP 下的限流感知问题 [GitHub, 2026-02-18]。

搜索与发现机制的缺陷同样值得关注。向量搜索虽是 ClawHub 的亮点功能，但在精确匹配场景下存在明显缺陷——Issue#1278 报告技能更新后完全从搜索中消失，Issue#1254 反映直接名称/slug 前缀查询在向量检索失败时无法回退 [GitHub, 2026-03-25]。这对开发者发布后的信心是致命打击。

发布流程中的元数据解析、许可证条款接受、slug 检查等环节也存在摩擦。Issue#633（"Publish fails with acceptLicenseTerms: invalid value"，9 条评论）和 Issue#622（"checkSlugAvailability error"，11 条评论）反映了典型问题 [2]。

5.3 社区生态层级

ClawHub/OpenClaw 已形成多层次的社区生态 [2]。核心项目层包括 openclaw/openclaw（336,455 Stars）、openclaw/clawhub（6,933 Stars）和 openclaw/skills（3,428 Stars）。社区聚合层由 VoltAgent/awesome-openclaw-skills（42,023 Stars，5,400+ 技能精选集）、davepoon/buildwithclaude（2,640 Stars）和 LeoYeAI/openclaw-master-skills（1,855 Stars）等项目构成。

垂直领域扩展活跃：FreedomIntelligence/OpenClaw-Medical-Skills（1,652 Stars）是最大的开源医疗 AI 技能库，jeremylongshore/claude-code-plugins-plus-skills（1,718 Stars）提供 340 插件 + 1,367 技能的综合集合 [2]。工具与基础设施层包括备份恢复工具（LeoYeAI/openclaw-backup）、云原生部署方案（openperf/openclaw-cloud）和认知记忆管理基础设施（sopaco/cortex-mem）[2]。

5.4 社交媒体口碑

Twitter/X 上用户对 OpenClaw 的评价以正面为主。代表性评论包括：@jonahships_ 称赞 OpenClaw 能"keep building upon itself just by talking to it"；@AryehDubois 表示"impressed how many hard things Claw gets right"，特别提到持久记忆、人格引导和通讯集成；@markjaquith 将其描述为"just had to glue all the parts together"的飞跃；@danpeguine 强调"your context and skills live on YOUR computer, not a walled garden"的数据主权优势 [38]。

5.5 媒体报道

MacStories 的 Federico Viticci 发表了题为"OpenClaw Showed Me What the Future of Personal AI Assistants Looks Like"的深度报道 [39]。StarryHope 的 Jim Mendenhall 撰写了"The Lobster Takeover: Why Developers Are Buying Mac Minis to Run Their Own AI Agents"，记录了用户专门购买 Mac Mini 来运行 OpenClaw 的趋势 [40]。

---

6. 市场定位与行业趋势

6.1 所处赛道

ClawHub 处于 AI Agent 技能/插件市场这一新兴赛道。该赛道在 2025-2026 年间经历了从零到数十万技能的爆发式增长，主要驱动因素包括：SKILL.md 开放标准的发布（Anthropic，2025-12）统一了跨 Agent 技能格式 [41]；MCP（Model Context Protocol）成为 AI 工具集成的事实标准，2025 年 12 月捐赠给 Linux Foundation [42]；Claude Code 在 2026 年初成为使用最广泛的 AI 编码工具 [43]；开发者工具市场整体规模从 2025 年约 64 亿美元增长至预估 2031 年 157 亿美元 [44]。

6.2 标准化进程

2025 年 12 月，Agentic AI Foundation（AAIF）在 Linux Foundation 下成立，Anthropic 捐赠了 MCP，OpenAI 捐赠了 AGENTS.md，Block 捐赠了 goose 框架 [45]。白金会员包括 AWS、Anthropic、Block、Bloomberg、Cloudflare、Google、Microsoft、OpenAI [46]。三个核心标准中，MCP（Agent-to-Tool 通信）已有 10,000+ 服务器发布 [47]；A2A（Agent-to-Agent Protocol）已获 50+ 技术合作伙伴 [48]；AGENTS.md（项目级 Agent 行为指引）已被 60,000+ 开源项目采用 [46]。

标准化降低了平台锁定的可能性，但也意味着分发渠道本身的差异化壁垒在降低。agent-skill-creator 项目已经演示了"一次安装，多平台发现"的能力 [49]。

6.3 安全成为全行业刚需

2026 年初的安全事件不仅影响了 ClawHub。Snyk 在技能注册表中发现了 386 个恶意包 [50]，SkillsMP 约 26% 技能含安全漏洞 [51]。安全审核正从"社区举报"模式向"自动化扫描 + 人工审

核"混合模式演进，skills.sh 与 Snyk 的合作被视为当前最佳实践 [27]。安全审计可能成为最有变现潜力的增值层之一——基础扫描免费，深度审计付费，认证徽章为开发者和企业提供信任背书。

6.4 从"MCP 优先"SaaS 看市场演变

Glama 的报告指出，原来通过 API 销售数据的公司（如 Bright Data、Exa.ai、Tavily）已转型为构建和托管自己的 MCP 服务器，将 MCP 作为新的分发渠道 [22]。这意味着 Skill 市场不仅是开发者工具的分发平台，也可能成为 SaaS 服务的新型分发渠道——每个 API 都有可能成为可变现的 MCP 服务器/Skill。用户偏好也正从本地 MCP 服务器转向远程托管服务器，暗示了"Skill-as-a-Service"模式的商业空间 [22]。

---

7. 运营数据与商业化

7.1 关键运营指标

截至 2026 年 3 月，ClawHub 的核心运营数据如下 [12] [2]：

指标	数据	说明
技能总数（清理后）	3,286	历史峰值 5,705，清理 2,419 个
累计下载量	150 万+	—
ClawHub GitHub Stars	6,933	—
ClawHub Forks	1,085	—
ClawHub 总 Issues	973	开放率 68%（662/973）
Pull Requests	303	活跃的代码贡献
母项目 GitHub Stars	336,455	OpenClaw 主仓库
母项目 Forks	65,833	—
技能分类数	11	—
GitHub 组织成员	18	公开成员

热门技能按下载量排名：Capability Evolver（35,581）、Wacli（16,415）、ByteRover（16,004）、self-improving-agent（15,962）、ATXP（14,453）[12]。

7.2 增长轨迹

OpenClaw 从 2025 年 11 月发布到 2026 年 3 月已获 33.6 万 Stars，从零到 10 万 Stars 仅用了约两个月 [1]。ClawHub 于 2026 年 1 月 3 日上线，3 个月内积累了 3,286 个技能（清理后）和 150 万+下载量 [12]。与竞品对比，skills.sh 发布仅 6 小时内 top skill 即达 20,000+ 安装 [25]，显示了 Vercel 品牌和开发者社区基础的巨大优势。

7.3 ClawHavoc 安全事件的运营影响

2026 年 2 月的 ClawHavoc 供应链攻击是 ClawHub 面临的最严重运营危机。攻击者植入了 1,184 个恶意技能（335 个属于核心 ClawHavoc 活动），设计用于未授权数据提取、凭证窃取和持久后门访问，影响约 300,000 AI 用户 [Cybersecurity News, 2026-02-18] [52]。事件后，平台清理了 2,419 个可疑技能——这意味着近半数技能被移除 [12]。

Malwarebytes 等安全媒体专门发文讨论"OpenClaw 安全性" [Malwarebytes, 2026-02-23]，Forbes 发布了"What Is OpenClaw? Everything You Need to Know"的深度文章 [53]，用户对安装第三方技能的安全顾虑显著提升。主仓库 Issue#27855 讨论"Agents: Safety against Jailbreaking and Prompt Injection Attacks"获 17 条评论 [GitHub, 2026-02-26]。

7.4 行业财务参考

对标行业关键财务数据 [54] [55]：Cursor 母公司 Anysphere 估值 $293 亿（2025 年 11 月 Series D），ARR 超 $10 亿；GitHub Copilot 拥有 470 万付费订阅用户；Windsurf/Cognition 估值 $102 亿；LangChain 估值 $12.5 亿。ClawHub 作为免费开源项目尚无收入数据，但其依托的 OpenClaw 社区规模（33.6 万 Stars）为未来商业化提供了用户基础。

---

8. 风险与展望

8.1 核心风险

创始人离开风险。 Peter Steinberger 于 2026 年 2 月加入 OpenAI，从全职维护转为兼职/基金会模式。虽然 OpenAI 承诺支持，但个人精力分配是长期隐忧 [5]。基金会转型尚在进行中（"I'm working on making it a foundation"），治理结构待定。项目的持续活力将高度依赖 Christoph Nakazawa 等核心贡献者的投入。

安全持续性风险。 ClawHavoc 事件虽已应对，但 AI Agent 生态的安全挑战是结构性的。项目自身承认 prompt injection 仍是"industry-wide unsolved problem"，VirusTotal 扫描"不是银弹" [8]。当前安全策略在安全性和开发者体验之间产生了严重矛盾——52% 的 Issues 为误报申诉 [37]。

竞争碾压风险。 skills.sh（Vercel）的规模（83,627 vs 3,286）、增长速度和品牌优势构成最大外部威胁。如果 Anthropic 官方 Plugins 目录大幅扩展，将直接冲击 ClawHub 作为 Claude 生态技能市场的核心定位 [32]。

生态绑定风险。 ClawHub 深度绑定 OpenClaw 生态，受限于母项目命运。虽然 OpenClaw 声称"not affiliated with Anthropic"，但核心运行在 Claude 模型上，与 Anthropic 生态有深度耦合；创始人加入 OpenAI 后的模型中立性值得观察 [5]。

标准碎片化风险。 如果各平台不完全遵守 AgentSkills 标准，ClawHub 的跨平台兼容性故事将打折扣。Cursor Marketplace 采用自有格式（5 原语），与 SKILL.md 标准不完全一致 [26]。

8.2 积极信号

OpenClaw 社区的规模和活跃度仍是最大资产——33.6 万 Stars、65,800+ Forks、50+ 集成说明社区基础扎实 [2]。企业赞助（OpenAI、Vercel、Convex）提供了资源保障。开源基金会治理模式在企业用户中具有天然信任优势。安全团队的认真态度（VirusTotal 合作、专职安全顾问）虽然短期产生误报痛点，但长期有助于建立行业标杆。

8.3 数据局限性

本报告的分析基于截至 2026 年 3 月 26 日的公开数据。AI 工具市场变化极快，部分数据可能在数周内过时。Smithery、Glama 等平台的详细财务数据未公开。ClawHub 作为新兴平台的运营数据有限。Twitter/X、Reddit 的搜索因工具限制未完整执行，小红书、微信公众号等中文平台未能直接采集。

9. 综合分析与交叉验证

9.1 跨维度关联发现

安全-商业模式-竞争的铁三角。 ClawHavoc 事件不仅是安全问题，它深刻影响了 ClawHub 的竞争位势和商业化路径。安全危机迫使平台收紧审核（导致 52% 误报），误报又损害了开发者体验（供给侧流失风险），而竞品 skills.sh 通过 Snyk 集成同时解决了安全和体验问题 [27]。这形成了

一个恶性循环：安全事件 → 过度审核 → 开发者流失 → 技能供给减少 → 用户流失。打破这个循环需要从安全技术本身入手（降低误报率），而非在安全性和体验之间做取舍。

创始人离开与基金会治理的双面性。 Peter Steinberger 加入 OpenAI 表面上是领导力风险，但深层看也带来机遇：OpenAI 的项目赞助、创始人在 OpenAI 内部的影响力可能为 OpenClaw 打开与 OpenAI 生态的整合通道。基金会治理模式虽增加不确定性，但在企业用户中具有天然中立性优势——企业更愿意依赖基金会治理的开源项目而非单一公司控制的平台 [5]。

社区策展超越官方市场的启示。 awesome-openclaw-skills（42,023 Stars）的热度远超 ClawHub 自身（6,933 Stars），这不是偶然现象 [2]。在安全事件频发、自动化质量控制不足的背景下，人工策展提供了用户最需要的"信任信号"。这对 ClawHub 的战略启示是：与其试图自建所有质量控制机制，不如将社区策展融入平台（如"策展者"角色、认证集合）。

9.2 信息矛盾与置信度评估

技能数量数据存在差异。 多个来源对 ClawHub 技能数量的报告不一致：claw-hub.net 报告 3,286 个（清理后）和 5,705 个（清理前）[12]；竞争情报分析 引擎引用了 13,729+ 的数字 [3]；深度调研 引擎引用了 2,857+ [50]。差异的主要原因可能是统计时间点不同、是否包含被隐藏/下架的技能、以及不同来源定义的口径差异。置信度最高的数字是 3,286（claw-hub.net 第三方统计站，明确标注"清理后"），建议采用此数字。

OpenClaw GitHub Stars 也有差异。 竞争情报分析 引擎引用了 247,000 Stars [56]，而 社交媒体调研 引擎引用了 336,455 [2]。差异可能是 Wikipedia 条目更新滞后。GitHub 直接数据更可信，采用 336,455。

skills.sh 的市场地位判断一致度高。 所有 4 个引擎均认定 skills.sh（Vercel）是 ClawHub 的最大竞争威胁，这一判断的交叉验证置信度为"高"。规模差距（83,627 vs 3,286）、品牌优势和跨平台策略在多个独立来源中得到一致确认 [36] [27] [25]。

9.3 关键模式识别

"开放标准 + 生态绑定"的张力。 ClawHub 依托 SKILL.md 开放标准，理论上支持跨平台；但实际上深度绑定 OpenClaw 生态，技能安装通过 OpenClaw CLI 完成。这种"标准开放、实现封闭"的模式在技术生态中常见（如 Android 之于 AOSP），但在 skills.sh 等真正跨平台竞品面前构成竞争劣势。

安全治理正在成为市场的分水岭。 从 ClawHavoc 到 SkillsMP 的 26% 漏洞率，安全问题正在将市场分为"可信赖"和"不可信赖"两个阵营。率先建立企业级安全审核体系的平台将获得结构性竞争优势。skills.sh 的 Snyk 集成和"Security Verified"徽章正在树立行业标杆 [27]。

---

10. 建议与行动方案

10.1 立即行动（0-3 个月）

1. 安全扫描误报率必须降低。 这是当前最紧迫的问题。建议：引入 Snyk 或 SonarQube 替代/补充当前的模式匹配检测；对常见合法模式（`child_process.spawn`、环境变量读取、MCP 标准操作）建立白名单；提供开发者自助申诉和自动复核通道，减少人工审核等待时间。目标：将误报占 Issues 比例从 52% 降至 20% 以下。

2. 搜索准确性修复。 向量搜索与精确匹配需要混合策略。PR#1256（Fix direct skill prefix recall when vector search misses）的方向正确，但需要更系统地解决技能更新后"消失"的问题。这直接影响开发者的发布信心和用户的发现体验。

3. 建立"策展者"角色。 将社区策展（如 awesome-openclaw-skills 的模式）融入 ClawHub 平台。允许策展者创建认证集合（Starter Packs），在 ClawHub 内部提供经过人工验证的高质量技能推荐，而非完全依赖算法。

10.2 短期行动（3-6 个月）

4. 跨平台兼容性扩展。 确保 ClawHub 技能可被 Claude Code、Cursor、Codex CLI 等主流 Agent 发现和安装。参考 skills.sh 的 18+ Agent 支持策略，至少覆盖 Top 5 Agent 平台。这是打破"OpenClaw 专属"标签的关键。

5. 安全认证体系上线。 推出"Security Verified"徽章（对标 skills.sh 的 Snyk 徽章），为通过深度安全审计的技能提供可视化信任信号。可分免费层（自动化扫描）和付费层（含人工审查）两档，后者可成为第一个变现点。

6. 企业关系建设。 利用 OpenClaw 基金会的中立治理优势，主动接触关注 AI Agent 安全的企业。Cursor 的 Team Marketplaces 功能证明企业对私有插件治理有付费意愿 [20]。

10.3 长期行动（6-12 个月）

7. 分层商业模式落地。 按照"免费基础层 → 开发者增值 → 企业治理 → Skill-as-a-Service"的路径逐步变现。避免 GPT Store 式的纯创作者分成模式（已被证明难以规模化），优先从安全审计和企业治理切入。

8. Playground 在线试用。 参考 SkillHub 的浏览器内 Playground 功能，允许用户在安装前试用技能。这不仅提升转化率，还降低了安全风险（用户可以在沙箱环境中评估技能行为）。

9. 垂直行业 Skill 集合。 为金融、医疗、教育等合规要求高的行业推出经过认证的专业 Skill 套件（参考 FreedomIntelligence/OpenClaw-Medical-Skills 的方向）。这是差异化竞争和 B2B 收入的重要战场。

附录A: 信息引用页面

[1] OpenClaw Blog. 2026-01.

[2] GitHub. 2026-03.

[3] ClawHub 官网. https://clawhub.com/. 2026-03.

[4] steipete.me. 2025-06.

[5] steipete.me. 2026-02.

[6] cpojer.net. https://cpojer.net/. 2026.

[7] cpojer.net. https://cpojer.net/. 2026-02.

[8] OpenClaw Blog. 2026-02.

[9] OpenClaw 官网. https://openclaw.ai/. 2026-03.

[10] AdvenBoost. https://advenboost.com/en/clawhub/. 2026-03.

[11] zRead.ai. https://zread.ai/openclaw/openclaw/17-skills-system-and-clawhub-marketplace. 2026-03.

[12] claw-hub.net. https://claw-hub.net/. 2026-03.

[13] Convex.dev. https://www.convex.dev/claw. 2026-03.

[14] clawhub README. 2026-03.

[15] ClawHub 官网. https://clawhub.com/. 2026-02.

[16] OpenClaw Docs. https://docs.openclaw.ai/tools/clawhub. 2026-03.

[17] GitHub. 2026-02.

[18] Composio Pricing. https://composio.dev/pricing. 2026.

[19] Smithery Pricing. https://smithery.ai/pricing. 2026.

[20] Cursor Changelog. 2026-03.

[21] GetPanto. https://www.getpanto.ai/blog/github-copilot-statistics. 2026-03.

[22] Glama Blog. 2025-12.

[23] LangChain Pricing. https://www.langchain.com/pricing. 2026.

[24] DigitalApplied. 2026-01.

[25] Vercel Changelog. https://vercel.com/changelog/introducing-skills-the-open-agent-skills-ecosystem. 2026-01.

[26] Cursor Blog. https://cursor.com/blog/marketplace. 2026-02.

[27] InfoQ. 2026-02.

[28] SkillsMP. https://skillsmp.com. 2026-03.

[29] SkillHub. https://www.skillhub.club. 2026-03.

[30] Agensi. https://www.agensi.io. 2026-03.

[31] GitHub Blog. 2025-02.

[32] Anthropic. 2025-11.

[33] Glama. 2026-03.

[34] Smithery. https://smithery.ai/. 2026-03.

[35] VS Code. 2026.

[36] skills.sh. https://skills.sh. 2026-03.

[37] clawhub Issues. 2026-03.

[38] Twitter/X. 2026.

[39] MacStories, 2025-. 2026.

[40] StarryHope, 2025-. 2026.

[41] VentureBeat. 2025-12.

[42] Anthropic. 2025-12.

[43] Pragmatic Engineer. https://newsletter.pragmaticengineer.com/p/the-creator-of-clawd-i-ship-code. 2026-01.

[44] Mordor Intelligence. 2025.

[45] TechCrunch. https://techcrunch.com/tag/cursor/. 2025-12.

[46] OpenAI. 2025-12.

[47] StackOne. 2026-03.

[48] Google Developers Blog. 2025-04.

[49] GitHub FrancyJGLisboa. 2026.

[50] DigitalOcean. 2026.

[51] SkillsMP. https://skillsmp.com. 2026-02.

[52] koi.ai. 2026-02.

[53] Forbes. https://www.forbes.com/sites/kateoflahertyuk/2026/02/06/what-is-openclaw-formerly-moltbot--everything-you-need-to-know/. 2026-02.

[54] CNBC. https://www.cnbc.com/2026/02/02/openclaw-open-source-ai-agent-rise-controversy-clawdbot-moltbot-moltbook.html. 2025-11.

[55] TechCrunch. https://techcrunch.com/tag/cursor/. 2025-06.

[56] Wikipedia. https://en.wikipedia.org/wiki/OpenClaw. 2026-03.

附录B: 引用媒体汇总

- AdvenBoost. 2026-03.
- Agensi. 2026-03.
- Anthropic. 2025-11, 2025-12.
- claw-hub.net. 2026-03.
- clawhub Issues. 2026-03.
- clawhub README. 2026-03.
- ClawHub 官网. 2026-02, 2026-03.
- CNBC. 2025-11.
- Composio Pricing. 2026.
- Convex.dev. 2026-03.
- cpojer.net. 2026, 2026-02.
- Cursor Blog. 2026-02.
- Cursor Changelog. 2026-03.
- DigitalApplied. 2026-01.
- DigitalOcean. 2026.
- Forbes. 2026-02.
- GetPanto. 2026-03.
- GitHub. 2026-02, 2026-03.
- GitHub Blog. 2025-02.
- GitHub FrancyJGLisboa. 2026.
- Glama. 2026-03.
- Glama Blog. 2025-12.
- Google Developers Blog. 2025-04.
- InfoQ. 2026-02.
- koi.ai. 2026-02.
- LangChain Pricing. 2026.
- MacStories, 2025-. 2026.
- Mordor Intelligence. 2025.

- OpenAI. 2025-12.
- OpenClaw Blog. 2026-01, 2026-02.
- OpenClaw Docs. 2026-03.
- OpenClaw 官网. 2026-03.
- Pragmatic Engineer. 2026-01.
- SkillHub. 2026-03.
- skills.sh. 2026-03.
- SkillsMP. 2026-02, 2026-03.
- Smithery. 2026-03.
- Smithery Pricing. 2026.
- StackOne. 2026-03.
- StarryHope, 2025-. 2026.
- steipete.me. 2025-06, 2026-02.
- TechCrunch. 2025-06, 2025-12.
- Twitter/X. 2026.
- VentureBeat. 2025-12.
- Vercel Changelog. 2026-01.
- VS Code. 2026.
- Wikipedia. 2026-03.
- zRead.ai. 2026-03.