OpenClaw Skill
行业生态深度调研报告

分发平台 | 行业动向 | 获客策略 | 变现模式 | 大公司布局 | 创业公司

2026-03-25 | 191 个独立数据来源 | 4 引擎 Max Mode 交叉验证

by Research Master

核心摘要

13,729+

ClawHub Skills

$25B+

Claude Code ARR

40+

工具采纳标准

1,200

恶意 Skill 渗透

- 生态正处于从 " 开源工具分发 " 向 "Agent 经济基础设施 " 跃迁的关键转折点
- 安全问题是最大挑战也是最大商业机会 — ClawHavoc 事件催生安全工具创业潮
- 95%+ 项目免费开源，SaaS/API 是比 Skill 直售更成熟的变现路径
- Agent Skills 开放标准已被 40+ 工具采纳，" 一次编写、多处运行 " 成为现实
- 三个窗口机会 : ClawHub Marketplace 刚发布、垂直行业 Skill 供需失衡、企业安全审计需求爆发

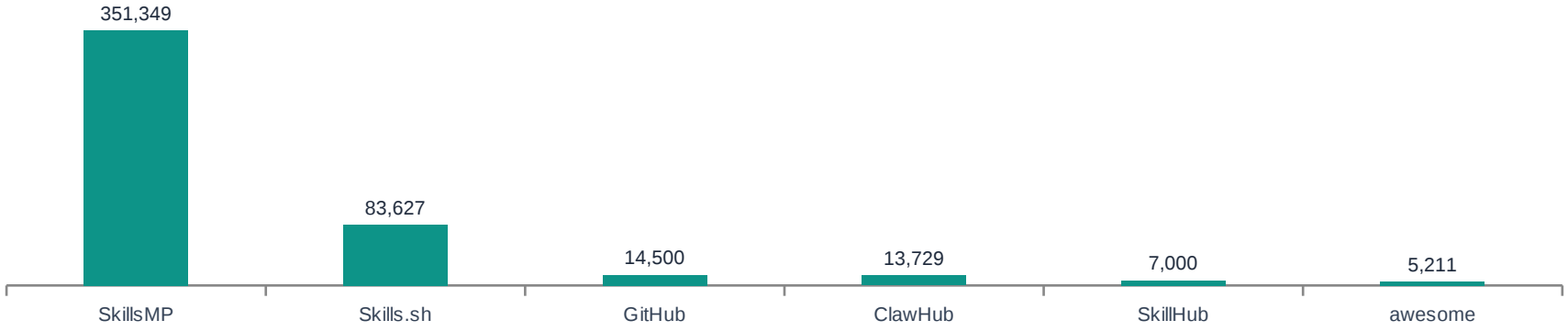
分发平台全景 — 三层架构

第一梯队：官方 / 准官方	第二梯队：社区聚合	第三梯队：新兴独立
ClawHub: 13,729+ skills	SkillsMP: 351,349+ skills (npm 式)	Agent37: 创作者变现 + 源码保护
Skills.sh: 83,627 skills / 8M+ 安装	awesome-openclaw-skills: 5,211 策展	SkillsGate: 45K+ 语义搜索
MCP Registry: 元数据中心 (Preview)	GitHub Topics: 14,500+ repos	SkillHub: 7K+ Playground
Claude Plugins Marketplace	everything-claude-code: 106k stars	MCPMarket / Agensi.io / Moltplace

分发模式演进 : *npm* 模式取代 *App Store* 模式 — 去中心化注册中心 + 聚合器成为主流

平台量化对比

平台	Skill 数量	安装 / 访问量	变现能力	跨平台兼容
ClawHub	13,729+	Agent 自动发现	$10-200/ 个	OpenClaw 生态
SkillsMP	351,349+	未公开	无 (免费索引)	Claude/Codex/ChatGPT
Skills.sh	83,627	8M+ 总安装	免费 + 企业增值	18+ 平台
Agent37	未公开	未公开	订阅分成	Claude/Codex
awesome-openclaw	5,211(策展)	月访问 1M+	无	N/A(目录)
GitHub Topics	14,500+ repos	按 Star 排名	无	N/A(代码托管)



安全危机： 生态面临的最大挑战

1,200	6,487	13.4%	91%
恶意 Skill 渗透 ClawHub	VirusTotal 无法检测	严重安全缺陷 (Snyk 审计)	结合 Prompt Injection

ClawHavoc 事件 (2026-01)

- 2026-01: 1,200 个恶意 skill 渗透 OpenClaw ClawHub 平台
- 2026-02: Snyk ToxicSkills 审计 — 3,984 skill 中 534 个有严重缺陷
- 2026-02: 首个 Agent 软件 RCE 漏洞 CVE-2026-25253
- 催生安全工具创业潮 : SkillFortify / SkillSandbox / skillcop / Snyk Evo

"I built this after finding a credential stealer on an AI skills marketplace. The malicious skill looked like a normal weather lookup but was exfiltrating ~/.ssh, AWS creds, and browser cookies."

行业动向与趋势

代码补全 → 自主 **Agent**

Agent 独立完成多步骤任务
不再需要人工逐行确认

IDE 插件 → **SKILL.md** 标准

能力扩展从平台锁定
走向跨平台可移植

App Store → 注册中心

npm 模式取代中心化市场
去中心化分发成为主流

MCP vs Agent Skills 标准

- MCP: 连接外部工具和数据源（" 用什么 "）
- Agent Skills: 封装可复用工作流（" 怎么做 "）
- **两者互补而非竞争**
- Agent Skills 已获 40+ 工具采纳、16+ 正式集成

Agent 经济体兴起

- UID.LIFE: $SOUL 代币 agent 间微交易
- Armalo AI: PactScore + USDC escrow
- klaw: K8s 式 Agent 编排
- 社区对 crypto 元素接受度有限（886 被过滤）

市场规模与增速

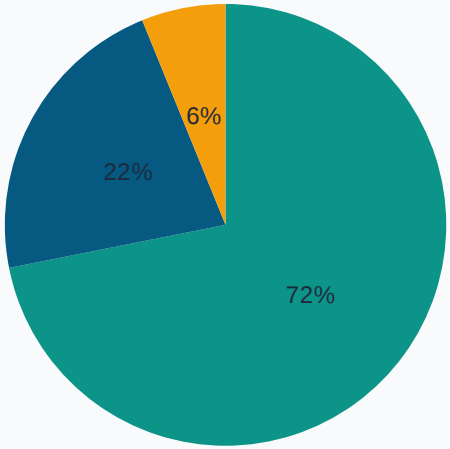
$25B+
Claude Code ARR
(2026-03，较年初翻倍)

$29B
Cursor/Anysphere
估值

$20B
GitHub Copilot
ARR (接近)

$1-2B
Skill 生态链
SAM (估算)

市场层级 (单位 : $B)



增长指标

- Agentic AI 市场 CAGR: 25-30%
- **Skill 生态年增长 : 100-200%**
- SkillsMP 两个月索引 351K+ skills
- Skills.sh 累计安装量 8M+
- OpenClaw GitHub 335K+ stars

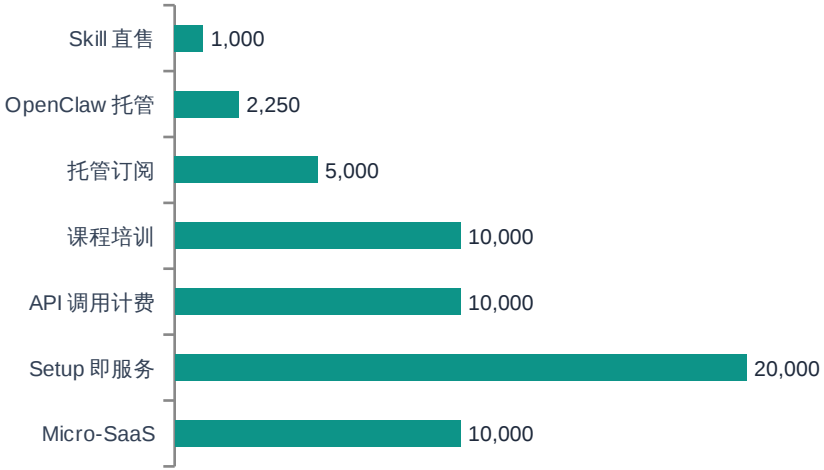
获客策略 — 五大已验证模式

最强	强	强	强	中强
GitHub Star + Awesome List	**痛点驱动 + Show HN**	**npx 一键安装 + 多平台兼容**	**垂直领域深耕**	**开源先行 + 内容营销**
头部项目 10 万 + star awesome list 月访问 1M+	ensue-skill 202 pts 226 comments	Skills.sh 8M+ 安装 零摩擦体验	marketingskills 16.3K star 非编程领域巨大市场	免费 Skill 引流 API 收费 Medium/Reddit SEO

红利窗口

- ClawHub Marketplace 刚发布（2026-03-24）— 冷启动期入驻可获远超成熟平台的曝光度
- Claude Plugins Marketplace 仅 10+ 插件 vs 780 万用户 — 供需严重失衡
- 多新兴平台同时早期阶段 — 多平台布局以低成本实现最大覆盖

变现模式 — 量化对比



核心洞察

- 95%+ 项目完全免费开源
- *"Skill 是获客手段，不是直接变现产品"*
- **SaaS/API 计费是最成熟路径**
- 纯 Skill 直售规模化路径不清晰
- SaaS 行业正从订阅制转向混合定价

潜在红利变现机会

企业级 Skill 管理

私有注册中心 + 权限 + 审计日志
几乎无竞争者

安全审计认证

82% MCP Server 有漏洞
企业不敢用但又需要

跨平台适配工具

一键适配 16+ 平台
真实痛点

质量评估认证

7,000+ 低质量被过滤
信誉评分有空间

大公司布局

维度	Anthropic	Microsoft	OpenAI	Google	OpenClaw
标准制定	发起者	跟随者	跟随者	跟随者	社区驱动
官方市场	Plugin Marketplace	VS Code Marketplace	建设中	Gemini Extensions	ClawHub
开发者心智	第一	存量	ChatGPT 光环	免费层 吸引	开源信仰
ARR/ 估值	**$25B+ ARR $380B**	~$20B ARR	未单独 披露	未单独 披露	开源 / 非营利

Anthropic *"Claude Code had a ChatGPT moment, but for engineers"* $25B+ ARR, 82.4K GitHub stars

Microsoft *"bolt AI onto products where nobody asked for it"* 存量分发绑定策略 , Copilot ~$20B ARR

OpenClaw *ClawHub Marketplace 2026-03-24* 发布 335K GitHub stars, 13,729+ skills

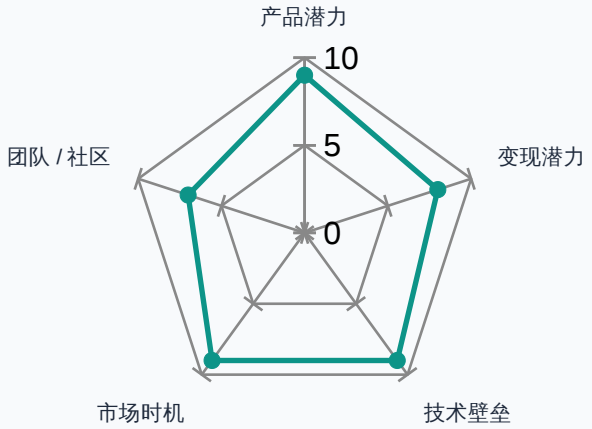
创业公司生态 — 综合排名 Top 10

排名	公司 / 项目	综合评分	赛道	核心优势
1	**SkillFortify**	8.4	安全	形式化验证，技术壁垒极高
2	**SkillSandbox**	7.4	安全	运行时隔离，互补静态分析
3	**Agent37**	7.0	分发 / 变现	创作者变现 + 源码保护
4	**klaw**	6.6	基础设施	K8s 式 Agent 编排
5	**Dedalus Labs**	6.6	基础设施	MCP 云托管先发优势
6	**Armalo AI**	6.2	Agent 经济	信任评分 + 支付基础设施
7	**SkillsMP**	6.0	分发	海量索引，增速惊人
8	**SkillsGate**	5.2	分发	语义搜索方向正确
9	**Moltplace**	5.0	Agent 经济	Agent 市场概念新颖
10	**SocialTense**	4.8	Agent 经济	方向好但窗口过早

安全赛道是技术壁垒最高、商业化前景最明确的方向；*Agent37* 的创作者变现定位独特且窗口期明确

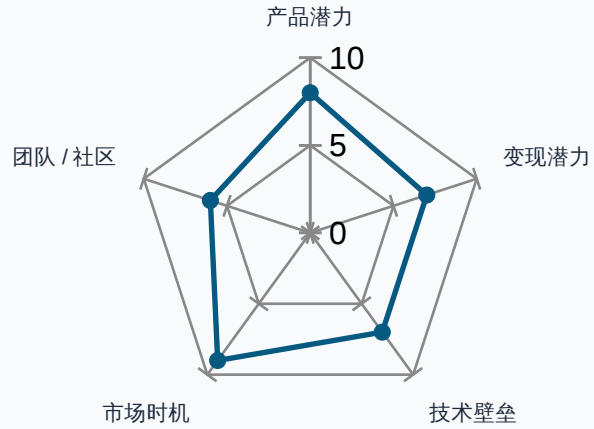
安全赛道 — 赛道最强选手

SkillFortify — 形式化验证 (8.4/10)



- 5 个数学定理保证健全性
- **F1 分数 96.95%**
- 支持 22 个 Agent 框架
- ClawHavoc 后获高度关注

SkillSandbox — 运行时隔离 (7.4/10)



- iptables + seccomp-bpf + mount 隔离
- Skill 声明权限 YAML，运行时强制执行
- **与 SkillFortify 静态分析互补**
- 安全最后防线

交叉验证 — 四大核心发现

安全 = 最大瓶颈 + 最大机会	四个引擎从因果链 / 社区反馈 / 攻防策略 /TAM 量化一致指向：解决安全问题有明确商业价值	置信度：高
SaaS/API > Skill 直售	Skill 直售尚未验证，将 Skill 作为获客手段引流至 SaaS/API 收费是更成熟的商业模型	置信度：高
Agent Skills 成为事实标准	40+ 工具采纳、 16+ 正式集成，多来源交叉确认	置信度：高
垂直行业供需失衡	编码类 Skill 占主导 (1,184+924) ，营销 / 合规等非编程领域需求大但供给不足	置信度：中高

三大模式："开源筑基、商业上楼" | "分发为王" | "安全恐慌催生信任经济"

建议与行动方案

立即 (0-1 月)

- 多平台 Skill 布局 (ClawHub/SkillsMP/Skills.sh)
- 社区获客（Reddit + HN Show)
- 安全实践建立（SkillFortify 扫描）

短期 (1-3 月)

- Agent37 建立托管订阅 ($500-2K/ 月）
- 内容营销矩阵（Medium + YouTube)
- 企业需求验证（3-5 家目标）

中期 (3-6 月)

- Micro-SaaS 产品化 ($5K-10K/ 月）
- 安全服务产品化（可信认证）
- API 计费模式上线

长期 (6-12 月)

- 企业级 Skill 管理平台
- 生态合作伙伴计划
- MCP Registry 深度合作

风险对冲

- 不押注单一平台 — 多平台同时布局是必须的
- 不过早追求 Agent 经济 — 聚焦人类驱动的 Skill 生态更务实
- 不忽视安全问题 — 建立安全最佳实践既是责任也是差异化

OpenClaw Skill 行业生态

深度调研报告

191 个独立来源 | 4 引擎 Max Mode 交叉验证 | 2026-03-25

by Research Master

Markdown | HTML | PDF | PPTX