Claude Code Skill 行业生态全景 — 分发平台·趋势·变现·玩家格局 深度调研报告

8,685 字 | 121 处引用 | 64 个来源

目录

Claude Code Skill 行业生态全景 — 分发平台·趋势·变现·玩家格局 深度调研报告

> 时间: 2026-03-25

> 数据来源: 141 个独立来源

> by research-master

核心摘要

AI 编程工具市场在 2025-2026 年迎来爆发式增长，规模从约 80 亿美元快速扩张，预计 2035 年将达 910 亿美元（CAGR ~28%）。在此背景下，Claude Code Skill 生态正经历一个关键拐点——从开发者社区的自发实验，演变为拥有标准化规范、多层分发渠道和初步变现基础设施的新兴行业。Anthropic 的年化收入已飙升至约 190 亿美元，其中 Claude Code 单品贡献超 25 亿美元年化收入，Cursor 以超过 20 亿美元 ARR 和 293 亿美元估值紧随其后 [1] [2]。

分发平台已形成四层体系：官方 Plugin Directory（头部插件 37 万+ 安装）→ Agent Skills 开放标准（33+ 工具采纳）→ 第三方聚合平台（SkillsMP 66,500+ skills、Agent37 225,000+ 索引）→ GitHub 社区生态（头部仓库 106,000+ Stars）。然而当前 Skill 层面几乎无法直接变现，主流模式是"技能即漏斗"——免费 Skill 获客，后端 SaaS 变现 [3]。

安全风险是生态最大隐患：Snyk 的 ToxicSkills 研究发现 36% 的 skills 存在安全缺陷，76 个确认为恶意载荷 [4]。OpenClaw 的 ClawHavoc 攻击事件（1,200 个恶意 skills）和 Claude Code 自身的 CVE 漏洞进一步加剧了信任危机。对独立工作室而言，当前是进入这一生态的最佳窗口期，但安全和变现模式成熟度是两大核心挑战。

从竞争格局看，行业呈"双寡头 + 多追赶者"态势：Claude Code 和 Cursor 在 Agent 编程赛道形成双强竞争，GitHub Copilot 凭 470 万付费用户稳守基本盘，Google 通过 24 亿美元收购 Windsurf 团队加速追赶，OpenAI 以 Codex CLI 直接进场 [5] [6]。Agent Skills 开放标准（agentskills.io）使得跨平台 Skill 复用成为可能，一次开发可覆盖 33+ 工具，这为独立开发者提供了前所未有的杠杆效应。

1. 分发平台格局与数据

1.1 四层分发架构

Claude Code Skill 的分发已形成清晰的四层架构，从官方渠道到社区生态逐层展开。

第一层：Anthropic 官方平台。 Anthropic 通过多个官方渠道提供 Skill 分发。Plugin Directory（claude.com/plugins）是最核心的集中式分发渠道，支持 `/plugin install <name>@claude-plugins-official` 命令一键安装，并带有"Anthropic verified"认证标志。截至 2026 年 3 月，头部插件安装量已具规模：Frontend Design 达 371,006 次安装，Superpowers 为 233,901 次，Context7（Upstash 开发）达 189,710 次 [7]。官方 Skills 示例仓库（anthropics/skills）已获 102,000+ Stars 和 11,200+ Forks [8]。

2026 年 3 月，Anthropic 正式推出 Claude Marketplace，面向企业客户提供经过审核的第三方应用。首批合作伙伴包括 Snowflake、GitLab、Harvey AI、Replit、Lovable 和 Rogo [9]。该 Marketplace 的独特之处在于允许企业将现有 API 支出承诺重新分配到第三方应用上，且上线初期免收佣金 [10] [11]。

第二层：跨平台开放标准。 2025 年 12 月，Anthropic 发布 Agent Skills 规范（agentskills.io）作为开放标准，采用 YAML frontmatter + Markdown 正文的 SKILL.md 格式。这是生态发展的关键转折点。截至 2026 年 3 月，该标准已被 33+ AI 编程工具采纳，包括 Claude Code、Cursor、GitHub Copilot（VS Code）、OpenAI Codex CLI、Gemini CLI、Roo Code、OpenHands、Goose（Block）、Junie（JetBrains）、TRAE（ByteDance）、Kiro（AWS）等 [12]。OpenAI 在 Codex CLI 中采纳了相同格式 [13]，Vercel 推出了 skills.sh 作为首个专用包管理器 [14]。Linux 基金会宣布成立 Agentic AI Foundation（AAIF），由 Anthropic（MCP）、Block（goose）和 OpenAI（AGENTS.md）三方贡献基础代码 [15]。

第三层：聚合型第三方平台。 这一层是当前最活跃的创业战场：

- SkillsMP（skillsmp.com）：66,541+ skills，通过自动抓取 GitHub 公开仓库实现持续更新，按 SDLC 阶段分类，支持 ZIP 下载和 CLI 安装 [16]。
- SkillHub（skillhub.club）：7,000+ skills，独特卖点是 AI 评估质量评分和 Playground 即时试用功能，作为 MCP 服务器运行，支持一键安装到 Claude Code、Codex CLI、Gemini CLI 等多平台 [17]。
- Agent37（agent37.com）：225,000+ GitHub skills 索引，提供托管运行环境和 Stripe 集成的变现基础设施，创作者可获得 80% 订阅收入分成 [18]。
- ClawHub/OpenClaw：开源社区市场，14,706+ skills 已索引，GitHub Stars 超越 React 成为最高星标开源项目 [HN, 2026-03-02]。但 2026 年初因 ClawHavoc 攻击事件（335 个恶意 skills 被上传）遭受严重信任危机 [4]。
- claudeskills.com：社区驱动的策展型 Skill 库 [19]。

第四层：GitHub 生态与本地分发。 GitHub 仍是 Skill 开发者最基础的分发渠道。社区聚合仓库活跃度极高：affaan-m/everything-claude-code 达 106,000+ Stars（包含 125+ Skills），

hesreallyhim/awesome-claude-code 达 32,200+ Stars [8]。Claude Code 支持三个安装作用域：个人级（`~/.claude/skills/`）、项目级（`.claude/skills/`）和组织级（通过 Managed Settings 集中部署），2025 年 12 月 Anthropic 发布了组织级 skill 管理功能 [20]。

1.2 关键平台数据对比

平台	Skill 数量	质量控制	变现支持	跨平台兼容	安装方式
Anthropic Plugin Directory	数十个官方认证	官方审核	无（免佣金）	Claude 专属	`/plugin install`
Claude Marketplace	首批 6 家合作商	企业审核	企业采购整合	Claude 专属	企业渠道
AgentSkills.io 标准	—	社区自审	无	33+ 工具	SKILL.md 规范
SkillsMP	66,541+	无自动审核	无	多平台	ZIP/CLI
SkillHub	7,000+	AI 评估评分	无	多平台	一键安装
Agent37	225,000+ 索引	沙箱试用	Stripe 80/20 分成	Claude 为主	托管运行
ClawHub/OpenClaw	14,706+	安全事件后整改中	无	多平台	GitHub
GitHub 社区	数万仓库	社区自审	无	多平台	Git clone

1.3 MCP 生态作为邻接市场

MCP（Model Context Protocol）服务器生态与 Skill 生态高度互补。Glama.ai 已索引 20,168 个 MCP 服务器，其中 972 个为官方认证 [21]。awesome-mcp-servers 达 84,000+ Stars [8]。热门 MCP 服务器按评分排列：Canva（20,053）、Notion（19,982）、Figma（19,828）、Slack（19,523）[22]。MCP 生态从 2025 年初约 1,000 个服务器爆发到超过 10,000 个活跃服务器 [3]，为 Skill 提供了丰富的外部数据源和执行能力。

---

2. 行业动向与趋势预测

2.1 宏观市场数据

AI 编程工具市场正处于高速增长期，但不同研究机构因定义口径差异，给出的数据存在分歧。综合多家来源：

- 2025 年市场规模：73.7-81.4 亿美元（Mordor Intelligence 73.7 亿 [23]；MarketsandMarkets 81.4 亿 [24]；Precedence Research 79.3 亿 [25]）
- 2030 年预测：240-260 亿美元（CAGR 26-28%）[26] [27]
- 更乐观预测：到 2032 年 1,270 亿美元（CAGR 48.1%）[24]
- 开发者采用率：85% 的开发者已在日常工作中使用 AI 工具 [28]

头部平台的收入规模已经验证了这一市场的吸引力：Claude Code 年化收入超 25 亿美元 [1]，Cursor 超 20 亿美元 ARR [2]，GitHub Copilot 470 万付费用户、42% 市占率 [5]。

2.2 从 Prompt 经济到 Skill 经济

2024 年的"Prompt 经济"——以 PromptBase 等平台售卖单条 prompt 为代表——正被 2026 年的"Skill 经济"取代 [3]。这一转变有三个核心逻辑：

持久性替代临时性。 Prompts 是一次性聊天指令，Skills 是持久化的文件夹结构，包含 SKILL.md 指令文件、可选脚本、模板和引用资料。Skills 可被版本控制、团队共享和持续迭代。

可执行性替代建议性。 通过 MCP 集成，Skills 不再局限于生成文本建议，而是能直接访问实时数据源并执行操作。MCP 生态已从 2025 年初约 1,000 个服务器爆发到超 10,000 个 [3]。

标准化替代碎片化。 SKILL.md 开放标准使同一个 Skill 可在 33+ 平台运行，消除了工具锁定 [29]。

2.3 关键趋势判断

趋势一：从辅助编程到自主 Agent（置信度：高）。 所有大厂同时布局 Agent Mode：Cursor 的 Background Agents、Claude Code 的 Auto Mode（2026-03）和 subagent 架构、GitHub 的 Project Padawan [30] [TechCrunch, 2026-03-24] [31]。Claude Code 目前贡献了全球 4% 的 GitHub 公开提交，预计年底将达 20%+ [32]。Skills 将越来越多地作为 Agent 的"工具包"运行，而非人类的快捷方式。

趋势二：企业采购整合加速（置信度：高）。 Claude Marketplace 和 Partner Network（1 亿美元投资）标志着 Skill 分发从开发者个人行为向企业 IT 采购流程整合 [33]。Anthropic 已与 Accenture、Deloitte、Cognizant、Infosys 等咨询巨头合作 [33]。Snowflake 与 Anthropic 签署 2 亿美元多年合作协议，使 Claude 触达 12,600 家全球客户 [34]。

趋势三：安全治理紧迫化（置信度：高）。 ToxicSkills 事件和 ClawHavoc 攻击暴露了 Skill 供应链脆弱性 [4]。Snyk 与 Tessl 合作建立 Agent Skills Registry 安全标准 [35]。代码签名、安全审查和自动扫描将成为平台标配。对创业者而言，安全既是风险也是差异化机会。

趋势四：大厂围堵第三方凭证复用（置信度：高）。 Anthropic 封堵第三方工具使用 Claude Code 订阅凭证（625 点 HN 热度）[HN, 2026-01-09]；Google 限制 AI Pro/Ultra 用户通过 OpenClaw 使用 Gemini（802 点 HN，极高关注）[HN, 2026-02-22]。平台方正在收紧生态控制权。

趋势五：垂直领域专业化（置信度：中高）。 通用型 Skills 竞争已白热化，但垂直行业 Skills（法律、金融、医疗、合规）仍有巨大空白。Harvey AI（法律，50 亿美元估值）、Rogo（金融分析）等专业玩家的成功验证了这一方向 [36]。

2.4 趋势预测时间表

预测	置信度	预计时间	依据
付费 Skill Marketplace 出现	高	2026 H2	npm 私有 registry 技术已就绪
Anthropic 推出 Revenue Share 机制	中高	2026-2027	参考 App Store 模式
MCP 成为 IETF/W3C 级标准	中	2027-2028	Linux Foundation AAIF 已介入
至少 2-3 个年收入百万美元级 Skill 创业公司	中	2027	Agent37 等变现基础设施初步就位
AI 编码工具整合潮（收购/合并）	高	2026-2027	Google 收购 Windsurf 团队已开先例
Agentic Skill 成为主流	高	2026 H2	所有大厂同步推进 Agent Mode

3. 平台获客策略与红利

3.1 各平台获客渠道分析

Claude Code（Anthropic）的获客策略以模型能力驱动和开发者工具链整合为核心。通过 VS Code/JetBrains 插件、Desktop App、Web、Slack、Chrome 全渠道覆盖，以及 GitHub Actions/GitLab CI/CD 集成实现 DevOps 工作流渗透 [37]。Skill 层面，官方 Plugin Directory 和 Skills 示例仓库（102,000+ Stars）提供了最大的曝光渠道。Anthropic 的 Plugin 审核目前门槛相对宽松，且免收佣金——这是典型的生态扩张策略 [10]。

OpenClaw/ClawHub 靠开源病毒式传播获客。从 ClawdBot → MoltBot → OpenClaw 两次更名，每次都引发大量媒体关注 [HN, 2026-01-30]。GitHub Stars 增速创纪录——30 天内超越 React [HN, 2026-03-02]。但安全争议（7.5% 恶意率）严重损害了品牌信任 [HN: RankClaw, 2026-03-07]。

Cursor 以 AI-native IDE 产品力驱动获客，结合 cursor.directory 社区和企业 BD。Marketplace 正处于扩张期，2026 年 3 月新增 30+ 插件，合作伙伴包括 Atlassian、Datadog、GitLab 等 [38]。Automations 功能创造了新的 Skill 使用场景。

GitHub Copilot 凭 1.5 亿 GitHub 开发者基础、学生优惠和企业标配地位获客。Extensions 生态仍在早期但门槛较高，需通过 GitHub Marketplace 审核 [39]。

3.2 获客红利分析

红利一：SKILL.md 标准化红利（窗口期：2026 年全年）。 Agent Skills 规范刚成为开放标准不久，率先掌握规范并产出高质量 Skills 的创作者可以获得先发优势。数据支撑：anthropics/skills 仓库 87,000+ Stars，但官方策展 skills 数量有限，大量垂直领域需求尚未被满足 [40]。

红利二：企业采购渠道红利（窗口期：2026-2027 年）。 Claude Marketplace 目前仅有 6 家首批合作伙伴，且 Anthropic 免收佣金 [9]。通过 Claude Partner Network，创业公司还可获得培训、技术支持和联合市场推广资源，Anthropic 为此投入 1 亿美元 [33]。

红利三：跨平台分发红利。 一个符合 SKILL.md 规范的 Skill 可同时分发到 33+ 平台 [14]。Universal Skills Manager 等工具进一步降低了跨平台管理成本 [41]。"写一次，卖多次"的杠杆效应显著。

红利四：GitHub 开源社区红利。 社区聚合仓库的传播效应极强。everything-claude-code 仅靠 GitHub 自然增长达到 106,000+ Stars [8]。Context7 通过官方 Directory 获得 189,710 次安装

后，成功引流到付费 SaaS [42]。被 awesome 列表收录或在 Reddit/HN 获高投票的 Skill 可获持续有机流量。

3.3 获客 ROI 模型（独立工作室视角）

渠道	CAC 估算	红利评级	适合阶段
GitHub 开源仓库	极低（$0-5）	★★★★★ 当前最大红利	冷启动
官方 Plugin Directory	低（$0-10）	★★★★☆ 仍在红利期	增长期
Awesome 列表/Reddit/HN	极低（$0）	★★★★☆	冷启动
SkillsMP/SkillHub/Agent37	低（$0-5）	★★★★☆	多渠道覆盖
Twitter/X 技术社区	低-中（$5-20）	★★★☆☆	品牌建设
YouTube/B站教程	中（$20-50）	★★★☆☆	品牌+教育
Claude Marketplace 申请	高投入但高价值	★★★★★（一旦入驻）	企业客户
企业直销	高（$500+）	★★☆☆☆	规模期

红利时间窗口判断：2026 H2 - 2027 H1 之间，随着更多开发者涌入，免费获客成本将显著上升。当前是入场最佳时机（置信度：高）。

---

4. 变现模式分析

4.1 行业变现模式全景

当前 Claude Code Skill 生态存在五种变现模式，成熟度各异：

模式一：Skill 即漏斗 + SaaS 后端（最推荐）。 核心逻辑：免费 Skill 获客 → 付费后端服务。标杆案例是 Context7（Upstash），通过官方 Directory 获得 189,710 次安装，免费层提供 1,000 API 调用/月，Pro 层 $10/座位/月，Enterprise 层 $30/用户/月起 [43]。一位创作者声称已构建 17 个可盈利的 Claude Skills [44]。这一模式的成功要素：免费 Skill 解决真实痛点、使用频率驱动付费转化、企业级功能创造升级动力。

模式二：托管订阅（Hosted SaaS）。 通过 Agent37 等平台，创作者部署 Skills 并收取订阅费，保留 80% 收入 [18]。优势在于知识产权不暴露、自动更新、无需用户本地配置。适合面向非技术用户的垂直领域 Skills。

模式三：企业合同（Enterprise Licensing）。 针对特定行业的高价值 Skills，以年度许可或按座位定价出售给企业。Claude Marketplace 的采购整合机制大幅降低了企业采购摩擦 [11]。500+ 客户年支出超过 100 万美元 [32]，说明企业级预算池巨大。

模式四：开源 + 增值服务（Open Core）。 开源基础 Skill 建立社区和信誉，高级功能、企业支持和定制化服务收费。PM Skills Marketplace 提供 65 个 PM skills 和 36 个链式工作流，采用类似模型 [45]。

模式五：x402 微支付（新兴）。 Seren Desktop 的模式，发布者自定义定价，通过 x402 USDC 微支付按调用收费 [HN, 2026-01-28]。概念先进但用户教育成本高。

4.2 潜在红利变现机会

尚未成熟但可能出现红利的变现方向：

- 安全审计即服务：7.5% 恶意 skill 率背景下，为 Skill 创作者和企业提供安全审计认证是刚需市场 [HN: RankClaw, 2026-03-07]。RankClaw、SkillFortify 已在探索，但商业化程度有限。
- Skill 组合/编排服务：将多个 Skills 打包为垂直工作流套件（如"DevOps Skill Pack"、"前端 Skill Pack"）。PM Skills Marketplace 的 36 个链式工作流已验证需求 [45]。
- Agent-as-a-Service：将 Skills 与 MCP 服务器、执行环境打包为完整的"Agent 即服务"产品，面向非技术用户。Agent37 是早期尝试 [46]。
- Skill 专用包管理器：Vercel 的 skills.sh 是首个尝试 [14]。类比 npm/PyPI 的发展路径，成为 Skill 分发的基础设施提供者。
- 企业 Skill 合规咨询：帮助企业评估、部署和管理 AI Skills，确保合规性和安全性。结合 Managed Settings 功能有天然入口 [37]。

4.3 变现挑战

知识产权保护困难。 SKILL.md 本质是 Markdown 文本，极易复制。即使托管隐藏源代码，核心指令逻辑仍可能被逆向工程。这是 Prompt/Skill 经济的根本性挑战。

免费替代品丰富。 66,500+ skills 中绝大多数免费开源 [47]。付费 Skills 必须在质量、支持和独特性上显著超越。

Token 成本侵蚀利润。 复杂 MCP 集成和多步骤工作流消耗大量 tokens。创作者需优化 token 效率，否则运营成本可能侵蚀利润 [3]。

4.4 定价策略建议

层级	建议价格	包含内容	对标
Free	$0/月	核心 Skill 功能，有使用量限制	Context7 Free
Pro	$9-15/月/座位	高级功能、私有仓库、更高限额	Context7 Pro $10/月
Team	$25-40/月/座位	团队协作、共享配置、优先支持	Cursor Teams $40/月
Enterprise	$100+/月/座位	SSO、合规、自托管、SLA	Copilot Enterprise $39/月

---

5. 大公司布局与产品

5.1 Anthropic — 生态基础设施的定义者

核心产品： Claude Code（CLI + VS Code + JetBrains + Desktop + Web + Slack），年化收入超 25 亿美元 [1]。整体公司年化收入约 190 亿美元，从 2024 年 12 月的 10 亿美元飙升至此，实现连续三年 10 倍增长 [48]。2026 年 3 月完成 380 亿美元估值的 300 亿美元 G 轮融资 [32]。

Skill 生态战略（三管齐下）：

- Claude Partner Network（1 亿美元投资）：Accenture、Deloitte、Cognizant、Infosys 等咨询巨头作为合作伙伴 [33]
- 开放标准：Agent Skills 规范和 MCP 协议，构建跨平台生态护城河

竞争定位： Anthropic 从"模型性能竞争"转向"企业集成能力竞争"。Partner Network 充当"信任层"，降低保守型企业 CIO/CTO 的采用门槛 [11]。Snowflake 的 2 亿美元多年合作使 Claude 触达 12,600 家全球客户 [34]。

社区评价： 模型能力领先，但定价策略引争议——"Anthropic's pricing wall is routing enterprise revenue to OpenAI" [HN, 2026-02-18]。封堵第三方凭证复用被社区视为战略失误 [HN, 2026-01-09]。

5.2 Microsoft/GitHub — 最大分发网络

核心产品： GitHub Copilot，470 万付费用户，2,000 万+ 累计用户，90% 的 Fortune 100 企业已部署 [6] [5]。VS Code 安装量 72,497,451 次 [49]。

扩展生态： GitHub Marketplace 约 440 个应用和 7,878 个 Actions [50]。Copilot Extensions 于 2025 年 2 月全面开放，合作方包括 Docker、Stripe、MongoDB、Sentry [51]。VS Code 1.109 已原生支持 Claude、Codex 和 Copilot agents [52]。

竞争优势： 分发网络无与伦比（1 亿+ GitHub 用户）、企业安全特性（IP 赔偿、SOC 2 合规）、深度 Microsoft 生态整合。Gartner AI Code Assistant 报告连续两年领导者 [8]。

5.3 Cursor（Anysphere）— 收入增长最快

核心数据： VS Code fork，超 20 亿美元 ARR（2026-03），100 万+ 日活用户，超过半数 Fortune 500 使用 [2] [5]。估值 293 亿美元，累计融资 33 亿美元+ [53]。60% 收入来自企业客户 [2]。

Skill 相关动态： 2026 年 3 月新增 30+ Marketplace 插件，合作伙伴含 Atlassian、Datadog、GitLab、Hugging Face、PlanetScale [38]。Automations 功能（事件驱动 Agent）和 MCP Apps 创造了全新 Skill 品类 [38]。

关键风险： AI 模型成本消耗约 100% 收入，年度总成本超收入约 1.5 亿美元 [54]。正开发自有模型 Composer 降低对上游模型依赖。这种"客户即竞争对手"（最大模型供应商是 Anthropic）的关系为长期独立性蒙上阴影。

5.4 OpenAI — 直接进场竞争

核心产品： Codex CLI（Rust 构建），集成 GPT-5.2-Codex 模型。官方 Skills Catalog 提供 35 个策展 skills [13]。通过收购 OpenClaw 创始团队（2026-02-15）获得社区生态基础 [HN, 2026-02-15]。此前曾两度尝试收购 Cursor 均被拒绝 [55]。

生态策略： 通过 AGENTS.md 贡献 Linux Foundation AAIF [15]，推动标准化。低价模型策略：GPT-5 版 Codex 定价低于 Claude Opus [56]。

5.5 Google — 收购追赶

24 亿美元 reverse acquihire Windsurf 核心团队 [6]。Gemini CLI 支持 Agent Skills 标准 [12]。Antigravity IDE 定位 AI 原生 IDE [57]。限制 OpenClaw 用户引发社区强烈不满（802 点 HN）[HN, 2026-02-22]。

5.6 Amazon

Q Developer（原 CodeWhisperer）定位覆盖 SDLC 全生命周期 [58]。Kiro IDE 支持 Agent Skills 标准 [12]。

5.7 大公司竞争格局总结

公司	核心优势	核心劣势	Skill 生态位	年化收入
Anthropic	标准制定权、模型最强	用户规模较小	生态定义者	~$190B 整体 / $2.5B+ Claude Code
Microsoft/ GitHub	用户规模最大、企业渗透	创新速度较慢	最大分发渠道	Copilot 未单独披露
Cursor	增长最快、产品体验	毛利为负、依赖上游模型	重要载体	$2B+
Google	资金充裕、收购能力	起步较晚	追赶者	未公开
OpenAI	品牌认知、低价策略	编程工具经验有限	挑战者	未公开
Amazon	企业客户关系、AWS 整合	消费者产品弱	企业补充	未公开

6. 创业公司图谱与评分

6.1 Skill 分发平台层创业公司

公司/项目	产品	核心差异化	融资阶段	综合评分	评分理由
SkillsMP	Agent Skills 聚合市场	最大规模索引（66K+），多平台支持	未公开	6/10	规模领先但缺乏变现和质量控制
SkillHub	AI 评估 Skills 市场	AI 质量评分，MCP 转换，Playground	未公开	7/10	技术差异化明显，跨平台能力强
Agent37	托管变现平台	80/20 收入分成，沙箱试用，Stripe 集成	种子轮（推测）	8/10	唯一聚焦变现基础设施，解决真实痛点
skills.sh (Vercel)	Skills 包管理器	Vercel 背书，包管理范式	Vercel 内部项目	7/10	首个专用包管理器，但生态早期
ClawHub/ OpenClaw	开源分发平台	开源，社区驱动，14K+ skills	N/A（开源）	4/10	ClawHavoc 安全事件严重损害信任
claudeskills.com	策展型 Skill 库	社区驱动，精选内容	社区项目	5/10	定位清晰但规模有限

6.2 AI 编程工具层核心创业公司

公司	最新估值	最新 ARR	融资总额	综合评分	评分理由
Cursor（Anysphere）	$293 亿	$20 亿+	$33 亿+	10/10	增速前所未有，产品体验业界最佳，但毛利率为负
Lovable	$66 亿	$4 亿	$5.3 亿	9/10	146 人创造 $4 亿 ARR，效率惊人
Cognition（Devin）	$102 亿	$7,300 万	$4 亿	7/10	方向正确但面临 Cursor/Claude Code 强烈竞争
Replit	$90 亿	$1.5 亿+	$4 亿	7/10	

公司	最新估值	最新 ARR	融资总额	综合评分	评分理由
					云端 IDE 定位独特，Claude Marketplace 合作伙伴
Augment Code	~$10 亿	未披露	$2.52 亿	6/10	企业级编码，差异化待验证

6.3 MCP 基础设施层创业公司

公司	定位	融资	综合评分	评分理由
Runlayer	MCP Agent 安全	$1,100 万种子轮（Khosla, Felicis）	9/10	安全是最大痛点，8 家独角兽客户，MCP 首席创建者任顾问
mcp-use (YC S25)	MCP 开发工具	YC S25	7/10	SDK 170K+ 下载，7K GitHub Stars
Klavis AI (YC W25)	企业级 MCP 服务器	YC W25	7/10	多租户认证，解决企业部署痛点
Akyn	专家知识变现为 Agent 资产	未公开	5/10	概念新颖但验证度有限

6.4 垂直领域 Agent/Skill 创业公司

公司	领域	估值/融资	综合评分	评分理由
Harvey AI	法律 AI	$50 亿估值	10/10	垂直领域 Agent 标杆，Claude Marketplace 首批合作伙伴
Sierra	客服 AI Agent	$100 亿估值	9/10	AI Agent 赛道估值最高创业公司之一
Rogo	金融分析 AI	Claude Marketplace 合作伙伴	8/10	高价值垂直赛道，企业级定位
Ritivel (YC W2026)	医疗监管写作 AI	YC W2026	7/10	高度垂直化，可将周级工作缩短到分钟

6.5 社区型创业项目

项目	HN 关注度	亮点	综合评分	评分理由
RankClaw	★★	全量审计 14,706 skills，发现 7.5% 恶意	6/10	有价值但商业化路径不明
SkillFortify	★★	支持 22 个框架自动扫描	6/10	安全工具刚需，但早期产品
Nanobot	★★★	4K LoC vs OpenClaw 400K LoC，99% 代码减少	5/10	精简但功能有限
Klaus	★★★	开箱即用的安全云端 OpenClaw，YC 背景	7/10	托管化有需求但依赖 OpenClaw
DenchClaw	★★★	YC S24，本地 CRM + AI Agent	6/10	品类窄但有 YC 背书
Cq (Mozilla.ai)	★★★★	"Stack Overflow for AI agents"概念	6/10	概念前沿但安全担忧大

6.6 评分方法论

评分综合考虑五个维度（各项权重相当，10 分制）：

- 产品-市场契合度（2 分）：是否解决真实且紧迫的痛点
- 技术壁垒（2 分）：竞争者复制难度
- 财务验证（2 分）：融资阶段、估值、收入数据
- 生态位独特性（2 分）：在 Skill 生态中的不可替代性
- 增长势头（2 分）：用户增长、社区活跃度、战略合作伙伴

---

7. 综合分析与交叉验证

7.1 四源交叉验证的核心发现

通过 深度调研、市场调研、竞争情报分析 和 社交媒体调研 四个引擎的独立采集，以下发现获得多源交叉验证：

发现一：Skill 生态处于"App Store 2008"阶段（4/4 引擎一致）。 所有引擎都将当前 Skill 生态与早期 App Store 或 npm 类比。SkillsMP 的 66,500+ skills 快速增长 [16]、OpenClaw 的爆发性增长 [HN, 2026-03-02]、Agent Skills 标准的多平台采纳 [12] 都指向同一结论：生态正从混乱无序走向标准化，但距离成熟的开发者经济仍有距离。

发现二：安全是生态最大的结构性风险（4/4 引擎一致）。 Snyk 的 36% 安全缺陷率 [4]、ClawHavoc 攻击 [4]、Claude Code CVE 漏洞 [59]、HN 社区的广泛讨论 [HN, 2026-03-22] 从不同角度证实了安全危机的严重性。同时，这一共识也解释了为什么 Runlayer（安全创业公司）能获得 Khosla 的 1,100 万美元种子投资 [60]。

发现三：Claude Code 和 Cursor 形成双寡头竞争格局（3/4 引擎一致）。 深度调研 和 竞争情报分析 提供了详细的收入和用户数据支撑，社交媒体调研 从社区讨论角度验证了这一格局。值得注意的是 市场调研 补充了一个重要细节：两者用户存在显著重叠——开发者同时使用 Cursor（IDE）和 Claude Code（CLI），形成互补而非纯替代关系 [61]。

发现四：变现模式尚未成熟，"Skill 即漏斗"是当前最可行路径（3/4 引擎一致）。 竞争情报分析 和 市场调研 分别从竞争对比和市场分析角度得出相同结论。深度调研 补充了 Agent37 的 80/20 分成模式作为直接变现的早期尝试 [18]。社交媒体调研 从社区讨论中发现，开发者普遍对付费 Skill 持谨慎态度——"为什么我要付费买一个 Markdown 文件？"——说明市场教育仍需时间。

7.2 信息矛盾与分析

矛盾一：市场规模数据差异大。 不同研究机构对 AI 编程工具市场的估算从 73.7 亿到 81.4 亿美元不等（2025 年）。Gartner 更保守，估 30-35 亿美元 [5]。主要原因是定义口径不同：纯代码补全 vs 广义开发者 AI 工具。对于 Skill 细分市场的规模，尚无权威估算，本报告给出的 $5.3-21.4 亿 SAM 为推算值。

矛盾二：OpenClaw 的价值评估两极分化。 HN 社区对 OpenClaw 的评价呈两极：一方面 "OpenClaw is changing my life"（340 点）[62]，另一方面 "OpenClaw is a security nightmare"（394 点）[63]。交叉分析后判断：OpenClaw 的核心功能有价值，但安全问题是致命

短板。OpenAI 通过收购其创始人团队来获取生态资产 [HN，2026-02-15]，侧面验证了其生态价值。

矛盾三：Cursor 的可持续性争议。 293 亿估值 vs 毛利为负 [54]。一方面增速惊人（20 亿 ARR），另一方面模型成本消耗 100% 收入。关键变量在于自有模型 Composer 能否降低成本，以及用户是否会因 Anthropic/OpenAI 的直接竞争而流失。

7.3 跨维度关联模式

模式一：标准化→平台化→变现化的演进路径。 Agent Skills 标准的确立（2025-12）→ Claude Marketplace 和 Plugin Directory 的推出（2026-03）→ 变现基础设施的建设（Agent37、npm 私有 registry）。这一路径与 iOS SDK → App Store → In-App Purchase 的历史演进高度一致。

模式二：安全危机催生基础设施创业。 每一次安全事件（ClawHavoc、ToxicSkills、CVE 漏洞）都加速了安全基础设施的需求和投资。Runlayer 的 1,100 万种子轮 [60]、SkillFortify 的快速响应 [HN, 2026-03-01]、Snyk 的标准化行动 [35] 形成了一个清晰的因果链。

模式三：大厂围堵→开源涌现→标准统一。 Anthropic 和 Google 封堵凭证复用 → OpenClaw、Nanobot 等开源替代品涌现 → Agent Skills 开放标准试图统一碎片化格局。这一循环将在未来持续。

---

8. 风险与局限性

8.1 核心风险

风险一：供应链安全危机（严重程度：极高）。 Snyk 的数据触目惊心——36.82% 的 skills 存在安全缺陷，76 个确认为恶意载荷 [4]。CData 审计显示 82% 的 MCP 服务器存在路径遍历漏洞，67% 存在代码注入漏洞 [3]。Claude Code 自身也曝出 CVE-2025-59536（CVSS 8.7）等严重漏洞 [59]。一次大规模安全事件可能摧毁整个产品的信誉。

风险二：模型能力替代风险（严重程度：中高）。 随着 Claude 4.5/4.6、GPT-5.2 等模型能力持续提升，许多当前需要 Skills 实现的功能可能被模型内置能力取代。缓解策略：聚焦需要外部数据源、系统集成和组织特定知识的 Skills，这些不容易被纯模型能力替代。MCP 集成型 Skills 的防御性强于纯 prompt 指令型。

风险三：平台锁定张力（严重程度：中）。 尽管 SKILL.md 是开放标准，各平台在实践中的实现细节存在差异。OpenAI Codex Skills Catalog"当前特定于 Codex，迁移到其他平台需要手动适配"[14]。每个超级平台都声称支持互操作性，同时构建锁定机制 [64]。

风险四：变现可持续性不确定（严重程度：中）。 成功变现案例仍有限，Agent37 的 80/20 分成模式交易量数据未公开 [18]。大多数 Skills 以免费开源形式分发。Skill 经济能否发展出成熟的开发者经济仍待验证。

风险五：生态碎片化（严重程度：中）。 Claude Code skills、Cursor marketplace、Cline MCP、OpenClaw、Copilot Extensions 五个生态互兼容性有限。Agent Skills 标准是潜在统一方案，但实际采纳程度和执行一致性尚不确定。

8.2 数据局限性

- Skill 平台的交易量和收入数据大多不公开
- Anthropic 未公开 Claude Code 用户数
- 中国市场的 Skill 生态数据覆盖有限（Claude Code 在中国大陆无法直接使用）
- 部分创业公司融资数据可能存在时间滞后
- HN/Reddit 社区讨论存在技术精英偏差

---

9. 建议与行动方案

立即行动（0-3 个月）

- 掌握 SKILL.md 规范：这是进入 Skill 生态的必要条件。研读 agentskills.io 文档和 anthropics/skills 仓库示例。
- 发布 5-10 个高质量 Skill：聚焦 1-2 个垂直领域（如 DevOps 自动化、前端工作流、内容创作），在 GitHub、claudeskills.com、SkillsMP、SkillHub、Agent37 同步上架，最大化曝光面。
- 建立安全审计流程：在发布每个 Skill 前进行安全自审，作为差异化卖点。
- 利用开源获客：通过 awesome 列表、Reddit r/ClaudeAI、HN 等社区获取种子用户，建立个人/工作室品牌。

短期布局（3-6 个月）

- 申请 Claude Partner Network：评估 Claude Marketplace 入驻可行性。当前免佣金窗口是罕见机会。
- 构建"Skill 即漏斗"模型：免费 Skill 解决真实痛点 → 引流到付费 SaaS 后端（参考 Context7 模式）。
- 跨平台分发：利用 Agent Skills 标准一次开发，覆盖 Claude Code + Cursor + Codex CLI + Gemini CLI。
- 探索企业客户：通过 Managed Settings 功能为企业提供定制 Skill 部署服务。

中期深耕（6-12 个月）

- 选择深耕方向：根据市场反馈，在以下三条路径中选择一条深耕：
- 垂直 Skill 产品：法律/金融/医疗/合规等高价值领域
- 平台基础设施：安全审计、质量评估、包管理、跨平台管理
- 企业服务：Skill 定制开发、部署、运维、合规咨询
- 建立 SaaS 订阅模式：MCP Server 后端 + Skill 前端的组合，跨平台适配。
- 关注收购整合机会：Skill 平台赛道的整合并购将在 2026 H2 开始。

长期定位（12 个月+）

- 成为 Skill 生态的基础设施提供者（工具、框架、标准）
- 或成为特定垂直领域的 Skill 领导者
- 建立跨平台 Skill 分发能力

关键监测指标

指标	监测频率	为什么重要
Agent Skills 标准采纳数	月	生态扩张速度
Claude Marketplace 合作伙伴数	月	企业渠道成熟度
SkillsMP/Agent37 活跃 Skill 数	月	生态整体热度
安全事件频率	周	信任危机风险

指标	监测频率	为什么重要
Cursor/Claude Code 市占率变化	季	平台格局变化
AI 模型能力跃升	持续	Skills 被替代风险

附录A: 信息引用页面

[1] SaaStr. https://www.saastr.com/anthropic-just-hit-14-billion-in-arr-up-from-1-billion-just-14-months-ago/. 2026-02.

[2] TechCrunch. 2026-03.

[3] Stormy AI. 2026-03.

[4] Snyk. 2026-02.

[5] Getpanto. 2026-03.

[6] TechCrunch. 2025-07.

[7] Claude 官方 Plugin Directory. 2026-03.

[8] GitHub. 2026-03.

[9] VentureBeat. https://venturebeat.com/technology/anthropic-launches-claude-marketplace-giving-enterprises-access-to-claude. 2026-03.

[10] MLQ.ai. https://mlq.ai/news/anthropic-launches-claude-marketplace-to-channel-enterprise-ai-budgets-into-partner-apps/. 2026-03.

[11] Futurum Group. https://futurumgroup.com/insights/claude-marketplace-tests-whether-anthropic-can-win-the-procurement-heart/. 2026-03.

[12] AgentSkills.io. https://agentskills.io. 2026.

[13] OpenAI Developers. 2026.

[14] ITecsOnline. https://itecsonline.com/post/codex-cli-agent-skills-guide-install-usage-cross-platform-resources-2026. 2026-02.

[15] Linux Foundation. https://www.linuxfoundation.org/press/linux-foundation-announces-the-formation-of-the-agentic-ai-foundation. 2025-12.

[16] SmartScope. 2026-01.

[17] SkillHub. https://www.skillhub.club. 2026.

[18] Agent37. 2026-01.

[19] ClaudeSkills. https://claudeskills.com. 2026-03.

[20] Anthropic Docs. https://code.claude.com/docs/en/skills. 2025-12.

[21] Glama.ai. 2026-03.

[22] Anthropic MCP Registry. https://api.anthropic.com/mcp-registry. 2026-03.

[23] Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/artificial-intelligence-code-tools-market. 2025.

[24] MarketsandMarkets. https://www.marketsandmarkets.com/Market-Reports/ai-code-generation-market-271006452.html. 2026-03.

[25] Precedence Research. https://www.precedenceresearch.com/ai-code-tools-market. 2025.

[26] Grand View Research. https://www.grandviewresearch.com/industry-analysis/ai-code-tools-market-report. 2024.

[27] Fortune Business Insights. https://www.fortunebusinessinsights.com/ai-code-tools-market-111725. 2026.

[28] Faros AI. https://www.faros.ai/blog/best-ai-coding-agents-2026. 2026-02.

[29] SkillsMP. https://skillsmp.com/. 2026.

[30] GitHub Blog. 2025.

[31] Cursor Blog. https://cursor.com/blog. 2026-03.

[32] Anthropic. 2026-02.

[33] Anthropic. 2026-03.

[34] The Next Web. https://thenextweb.com/news/anthropic-marketplace-claude-enterprise-software. 2026-03.

[35] Snyk. 2026-03.

[36] AI Funding Tracker. https://aifundingtracker.com/top-ai-agent-startups/. 2026-02.

[37] Claude Code Docs. https://code.claude.com/docs/en/overview. 2026-03.

[38] Cursor Changelog. https://cursor.com/changelog. 2026-03.

[39] GitHub Blog. 2024-05.

[40] Towards Data Science. https://towardsdatascience.com/how-to-build-a-production-ready-claude-code-skill/. 2026-03.

[41] LobeHub. https://lobehub.com/skills/openclaw-skills-universal-skills-manager. 2026-03.

[42] Claude Plugin Directory. https://claude.com/plugins. 2026-03.

[43] Context7. https://context7.com/plans. 2026.

[44] Medium. 2026-02.

[45] Product Compass. https://www.productcompass.pm/p/pm-skills-marketplace-claude. 2026-03.

[46] Agent37. 2026.

[47] SkillsMP. https://skillsmp.com/. 2026-01.

[48] Sacra. https://sacra.com/c/anthropic/. 2026-03.

[49] VS Code Marketplace. 2026-03.

[50] SQ Magazine. https://sqmagazine.co.uk/github-statistics/. 2025.

[51] TechCrunch. 2024-05.

[52] Morph LLM. 2026-03.

[53] CNBC. 2025-11.

[54] Fortune. 2026-03.

[55] TechCrunch. 2025.

[56] TechCrunch. 2025-08.

[57] DevGent. https://devgent.org/en/ai-code-editor-comparison-cursor-zed-windsurf-antigravity-kiro-developer-guide/. 2026-03.

[58] TechCrunch. 2024-12.

[59] Check Point. 2026-02.

[60] TechCrunch. 2025-11.

[61] DEV Community. 2026-03.

[62] HN. 2026-02.

[63] HN. 2026-03.

[64] SalesforceDevOps. https://salesforcedevops.net/index.php/2025/12/24/2026-the-year-ai-gets-real/. 2025-12.

附录B: 引用媒体汇总

- Agent37. 2026, 2026-01.
- AgentSkills.io. 2026.
- AI Funding Tracker. 2026-02.
- Anthropic. 2026-02, 2026-03.
- Anthropic Docs. 2025-12.
- Anthropic MCP Registry. 2026-03.
- Check Point. 2026-02.
- Claude Code Docs. 2026-03.
- Claude Plugin Directory. 2026-03.
- Claude 官方 Plugin Directory. 2026-03.
- ClaudeSkills. 2026-03.
- CNBC. 2025-11.
- Context7. 2026.

- Cursor Blog. 2026-03.
- Cursor Changelog. 2026-03.
- DEV Community. 2026-03.
- DevGent. 2026-03.
- Faros AI. 2026-02.
- Fortune. 2026-03.
- Fortune Business Insights. 2026.
- Futurum Group. 2026-03.
- Getpanto. 2026-03.
- GitHub. 2026-03.
- GitHub Blog. 2024-05, 2025.
- Glama.ai. 2026-03.
- Grand View Research. 2024.
- HN. 2026-02, 2026-03.
- ITecsOnline. 2026-02.
- Linux Foundation. 2025-12.
- LobeHub. 2026-03.
- MarketsandMarkets. 2026-03.
- Medium. 2026-02.
- MLQ.ai. 2026-03.
- Mordor Intelligence. 2025.
- Morph LLM. 2026-03.
- OpenAI Developers. 2026.
- Precedence Research. 2025.
- Product Compass. 2026-03.
- SaaStr. 2026-02.
- Sacra. 2026-03.
- SalesforceDevOps. 2025-12.
- SkillHub. 2026.
- SkillsMP. 2026, 2026-01.
- SmartScope. 2026-01.

- Snyk. 2026-02, 2026-03.
- SQ Magazine. 2025.
- Stormy AI. 2026-03.
- TechCrunch. 2024-05, 2024-12, 2025, 2025-07, 2025-08, 2025-11, 2026-03.
- The Next Web. 2026-03.
- Towards Data Science. 2026-03.
- VentureBeat. 2026-03.
- VS Code Marketplace. 2026-03.