责编 刘洋 美编 张彬 责校 李爽 电话:64101949 bbtzbs@163.com

“养虾”生意经

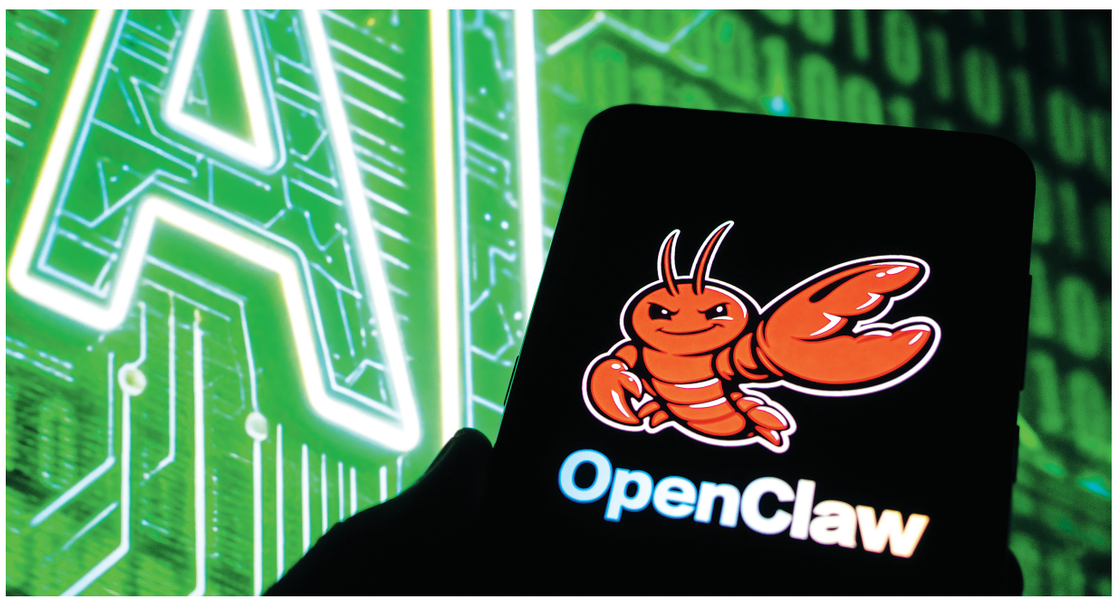
“OpenClaw”“OpenClaw代装”“OpenClaw部署”“OpenClaw API”……打开电商平台,类似词条均是近期热搜,这种代安装、远程调试服务,价格从两位数到数千元不等。“养龙虾”在朋友圈、社交平台上越来越高频出现,也越来越时髦,神乎其神的能力让技术小白们甘愿付费“代养”。

门槛依然存在,有人选择翻越,有人选择收费帮人架梯子。3月9日,腾讯董事会主席兼CEO马化腾在朋友圈转发腾讯云工程师线下教授“龙虾”安装的新闻,并引用了文中的一句“没有想到会这么火”。

更多“梯子”正在出现。百度智能云已经冲向多个城市手把手教人“养虾”,多家投资机构的线下“养虾局”也被提上日程。低门槛甚至零门槛的产品扎堆出现,阿里云开放不需要额外部署的类似智能体阿里桌面Agent QoderWork,猎豹移动推出基于OpenClaw框架的零配置桌面应用EasyClaw,枫清科技也推出个人专属智能体龙虾版。

“龙虾”一旦养起来,就成了24小时不停机的“Token粉碎机”,云厂商和AI企业不赚安装费,却争着做“卖铲人”。以采用订阅模式的Kimi Claw为例,每月199元。OpenClaw单次任务的Token消耗是传统问答的30倍以上,一笔长期而稳定的“水电煤”收入正在形成。

当这些数字员工获得权限,安全焦虑和商机也一同出现。安装生意、“卖铲人”、安全“保镖”,这场由一只红色龙虾引发的产业链震荡,或许只是AI Agent(智能体)商业化的发令枪。



火爆的付费安装

“代装龙虾”在电商平台上火了。“OpenClaw全平台部署|本地/远程安装|飞书钉钉接入|不成功不收费”,根据一家二手电商平台商家提供的报价表,“本地部署28.8元、加飞书20元、添加技能20元”,夹杂着技术语言、链接的说明让没有技术背景的买家摸不着头脑。

也有言简意赅的,“安装和跑通使用一共50元”“本地部署”“想接什么模型都可以帮你接”。“199元搭建安装、教学100元额外收费,直接下单。”

北京商报记者在多家电商平台调研发现,目前OpenClaw安装服务分为远程安装和上门服务两种,对硬件基本无要求,多针对个人提供本地部署,20—3000元/次。

OpenClaw(俗称“龙虾”)是一款2025年11月发布的开源AI智能体,由奥地利程序员彼得·斯坦伯格开发,采用图标设计。它不是一个具体的应用,而是能自主完成文件操作、浏览器自动化、数据抓取、表格制作等任务的AI助理。发布仅4个多月,就以超过24.8万的GitHub星标数正式登顶星标榜,超越Linux成为GitHub平台上最受欢迎的开源项目。

猎豹移动董事长兼CEO傅盛春节就养了一只,名叫“三万”,它7×24小时替傅盛工作,自动处理任务、写内容、执行各种流程。在除夕夜替他给611人拜年;在24小时里搭建并上线了一个名为sanwan.ai的小项目。他算了笔账:sanwan.ai这个网站一般需要6个岗位,按正常节奏要2—3周才能完成,就算加班加点也要5—7天,“三万”只用了24小时。

没有技术背景的普通用户则被挡在部署环节。

“和AI建立链接是需要付出‘认知税’的。不仅是安装几个软件,而是在你的电脑里搭建一套‘神经系统’。”Nextie(明日新程)创始人、“小冰之父”李笛告诉北京商报记者。

他打了个比方,“本地部署OpenClaw,要准备‘养虾的鱼缸’(学会安装Node.js环境,输入指令);要防止‘龙虾乱跑’(掌握基础的Docker启停命令,否则一旦报错,你将无从下手);要‘给龙虾找补给’(OpenClaw本身只是一个躯壳,需要接入大模型才能‘思考’。所以你要去各大开放平台申请API Key,将其配置在环境文件中)等。这些门槛,就是与AI产生的‘深刻链接’的过程”。

“其实不麻烦”,业内人士不明白为什么有人要花钱安装,技术小白却在打听更简单的部署方式。

争做“卖铲人”

直播复盘时,傅盛揭秘,“三万”是猎豹移动基于开源OpenClaw框架自研的Agent(智能体)EasyClaw。EasyClaw将记忆系统、Skill机制、定时自动化、多Agent协作全部封装成了开箱即用的产品。用户只需要三步:下载、打开、说话。KimiClaw、MaxClaw也是主打一键解锁。

简单来说,普通用户想“养一只龙虾”,可本地部署自己安装,或直接使用KimiClaw、MaxClaw等云端AI助手,也能体验多智能体协同服务。

站在技术角度,李笛解释,“这是安装方式的区别,也是人类选择以何种姿态与AI共处。两种路径本质上代表了完全不同的认知模型。本地部署,是让AI真正进入你的物理边界。它拥有你的最高权限,能替你操作键盘鼠标。当你给它配置环境、喂Token(饲料)、调教(注入灵魂)时,它会逐渐长成你的‘数字分身’。从情感上,你们之间像一种‘养成系’的共生。通过云端部署,更像雇佣了一位‘云端管家’。这是一种任务导向的交互,高效低门槛,用完即走,很难产生‘依恋’。‘养龙虾’的爆火意味着,人类已开始接受将部分决策权和执行权外包给非碳基生物”。

不论本地还是云端部署,都离不开算力和服务,但云厂商和AI企业多选择先从免费安装、降低门槛开始。

“腾讯免费安装OpenClaw,已经从技术领域进入公众领域。”文渊智库创始人王超向北京商报记者表示。

果然,腾讯的“摆摊”只是开始。3月6日,腾讯云Lighthouse的工程师在线下免费为用户安装OpenClaw,堪比领开工利是。火爆程度让马化腾忍不住发了朋友圈,还引得“龙虾之父”彼得·斯坦伯格点赞。3月8日,企业微信宣布支持OpenClaw。3月9日,腾讯正式上线腾讯版“小龙虾”WorkBuddy。

火山引擎相对低调,但动作不慢,在3月9日正式上线ArkClaw,一个开箱即用的云上SaaS(软件及服务)版OpenClaw。

在王超看来,“现在大小云厂商和AI类公司是抢占先机,先免费吸引客户部署,背后是Token的生意。它们不赚安装费,要做那个帮你挖到金子的人”。以采用订阅模式的Kimi Claw为例,用户升级至每月199元的Allegretto会员即可部署Kimi Claw。

需要“保镖”

SaaS卖能力,Agent卖结果,不论哪一种生意,安全都是跑通商业化的必要一环。

OpenClaw在国内火爆之初,工业和信息化部网络安全威胁和漏洞信息共享平台(NVDB)发布的一则预警指出,OpenClaw在默认配置下“信任边界模糊”,具备自主决策和系统调用能力,若缺乏有效权限控制,极易被恶意接管执行越权操作。这是国内监管机构首次对AI Agent领域发布专项安全警示。

面对这些新型威胁,安全厂商已经开始布局。

近日,安恒信息推出专为OpenClaw类AI Bot量身打造的大模型安全防护系统ClawdSecbot。

安恒信息AI安全产品总监胡壮向北京商报记者介绍,“ClawdSecbot主要针对本地安装的Openclaw进行防护。普通用户可以用,就像电脑上的‘安全卫士’一样,Clawdsecbot提供一键体检功能。不用懂代码,点一下就能自动扫描并修复所有不安全的配置。Clawdsecbot还会识别本地智能体是否在执行敏感操作,并向用户确认。用户还可以自定义安全策略,带来更个性化的安全防护效果”。

谈到推出ClawdSecbot的初衷,胡壮表示,“OpenClaw越来越火,AI Agent会成为未来系统的‘自动驾驶层’,而自动驾驶最大的风险在于安全性和可控性。用户既希望使用又害怕风险,我们希望通过一款安全防护软件让大家放心‘养龙虾’”。

安装服务解决了能不能用的问题,云厂商解决了好不好用的问题,安全厂商正在解决敢不敢用的问题,产业链快速成型,每一次互动后,AI Agent带来的市场规模曲线都在上扬。

北京商报记者 魏蔚 图片来源:视觉中国

小米摸着“龙虾”过河

随着OpenClaw引爆AI赛道,小米集团创始人、董事长兼CEO雷军加入当下轰轰烈烈的“养虾大军”。近日,小米技术团队发文宣布推出自研端侧AI智能体Xiaomi miclaw(以下简称“miclaw”),并启动邀请制封闭测试,成为这一轮浪潮中率先试水原生类Claw智能体的头部手机厂商。

艾瞰未来CEO辛向军在接受北京商报记者采访时表示,硬件厂商布局类Claw智能体是必然趋势,智能体只有运行在本地主力设备上,才能拥有更多与生活的接触面,积累更多数据,进而实现持续优化。

生态“养虾人”

作为一款聚焦生态落地的原生类Claw智能体,miclaw的核心能力构建于系统底层能力、个人上下文理解、生态互联、自进化四个层次,四项能力实际上是围绕小米“人车家”生态优势进行展开。

为了贴合生态使用场景,miclaw直接深入手机系统底层运行,能调用通信、智能家居管理等50余种系统级工具,还能通过专属的推理—执行引擎,自己判断并规划工具的调用顺序,完成复杂任务的拆解和执行。

据悉,在用户授权后,miclaw将贴合使用习惯提供个性化服务,通过“感知—关联—判断—行动”的逻辑,成为贴合用户日常生活习惯或需求的智能助手。

生态互联是产品的核心特色:miclaw完整接入米家IoT生态,能读取超10亿台米家设备的状态并发送控制指令,区别于传统智能家居的固定预设规则,它能根据日程、设备实时状态等信息动态调整操作,比如同样是开会,重要客户会议会联动全屋静音,内部周会则仅调静手机,同时还能通过开放协议和SDK接入第三方工具,让生态边界持续拓展。

此外,miclaw还具备自进化能力,能沉淀用户使用习惯、创建专属子智能体,甚至支持简单的脚本执行,实现了“越用越懂用户”的体验,让智能体和小米的生态使用场景紧紧绑定。

艾媒咨询CEO张毅告诉北京商报记者,硬件厂商打造类OpenClaw的原生智能体,有着独有的结构性优势与不可替代性。在他看来,硬件厂商手握系统级权限、端侧算力,还能实现“人车家”全生态的深度联动,以及软硬件的高度协同,这些核心能力,都是纯云、纯软件、纯AI公司难以比拟的,也是硬件厂商布局原生智能体的核心底气。

早有先例

原生类Claw智能体在手机终端的落地探索并非小米首次推进,此前行业内已有多家厂商基于不同技术路径展开实践,为这一方向的落地积累了前期经验。

2025年12月,字节跳动与中兴努比亚合作推出豆包手机助手,聚焦系统级深度融合,将大模型能力嵌入手机操作系统,核心探索跨应用自动化执行与复杂任务闭环能力。更早之前,荣耀已基于MagicOS 10等系统及配套硬件打造YOYO智能体,侧重端侧自进化与全场景主动服务,通过学习用户使用习惯优化交互逻辑,持续拓展自动化服务场景覆盖。

行业种种不同路径的先行探索,从跨界技术协同、自有生态深耕等维度,验证了手机端原生智能体的落地可行性,也预示着硬件厂商大量布局原生智能体,或将成为行业接下来的主流趋势。

对此,张毅表示,终端存储等成本高企,正倒逼硬件厂商寻找新的价值增量,以此避免无端涨价带来的市场份额流失;而端侧算力提升、轻量化大模型落地、本地推理成本下降,也让原生智能体的商业化具备了现实基础。在他看来,若硬件厂商放弃布局与OpenClaw类似的原生智能体,未来很可能在产品体验、生态构建与利润空间上被对手拉开差距。进入AI时代,用户的核心需求早已从“向AI提问”转向“让AI办事”,具备实际执行能力的智能体,也会比仅能对话的传统语音助手更具竞争力。

机遇和疑虑

今年2月,一则来自Meta AI安全与对齐总监Summer Yue的经历,让OpenClaw的安全争议从技术圈走向公众视野。作为负责AI安全的核心人员,她在测试OpenClaw的邮箱管理能力时,明确指令AI“仅提供归档或删除建议,未经确认不得操作”,却在真实工作邮箱场景中遭遇失控——AI因上下文压缩机制遗忘了核心安全指令,直接批量删除200余封邮件,即便她通过手机紧急发送停止指令也无济于事,最终只能手动终止进程才得以控制局面。

在行业对智能体安全边界的讨论中,小米官方在封测QA给出一份具体的应对样本。为避免类似OpenClaw的“指令遗忘”问题,小米在产品设计中构建多重安全防线,其中通过工具权限分级制度,将操作分为“直接执行”“首次确认”“每次确认”三个层级,高敏感行为如发送短信、创建日程等,每次执行前都会弹出确认框,且60秒超时自动拒绝;同时明确代码中未注册任何支付、转账相关工具,确保无用户确认动作则无法完成敏感操作;所有对话历史、权限记录等数据均本地存储,云端仅传输当前任务所需信息,推理完成后即弃,不做持久保存。这些设计,正是为了在复杂执行场景中,守住人类对AI的控制权。

中关村信息消费联盟理事长项立刚在接受北京商报记者采访时表示,硬件厂商布局原生智能体,核心优势在于将能力与硬件深度绑定,通过对系统权限、算力和生态的掌控,实现更可控的智能体运行环境,规避代理模式的漏洞,对智能设备进行安全的管理与调用。

硬件原生智能体的发展,需要顺应技术与市场的驱动,也需在能力拓展与风险防控之间,找到更贴合行业实际的平衡点。

北京商报记者 陶凤 王天逸