近期，開源 AI 智能體 OpenClaw 掀起全民“養龍蝦”的現象級熱潮，成為 2026 年開年 AI 領域當之無愧的頂流熱點。這款因官方紅色龍蝦圖示被網友俗稱“小龍蝦”的專案，GitHub 星標數在極短時間內突破 25 萬，一舉躋身全球史上增長最快的開源專案之列。政府專項補貼加持、頭部大廠密集佈局、資本市場熱烈追捧，就連千元價位的上門安裝服務都供不應求，多重熱度共振之下，OpenClaw 快速從科技圈破圈滲透至大眾視野，穩居當下 AI 產業最受矚目的核心賽道。需要警惕的是，工業和資訊化部網路安全威脅和漏洞資訊共用平臺於近日發佈緊急預警：OpenClaw 開源 AI 智能體的部分實例，在默認配置或不當配置場景下存在高危安全漏洞，極易誘發網路攻擊、數據資訊洩露等安全事件。回歸行業本身，這場由 OpenClaw 掀起的熱潮，究竟會給 AI 產業發展帶來哪些深層變革？又將為投資者解鎖哪些全新機遇？

全民“養龍蝦”！OpenClaw 爆火出圈，應該關注哪些投資機會？

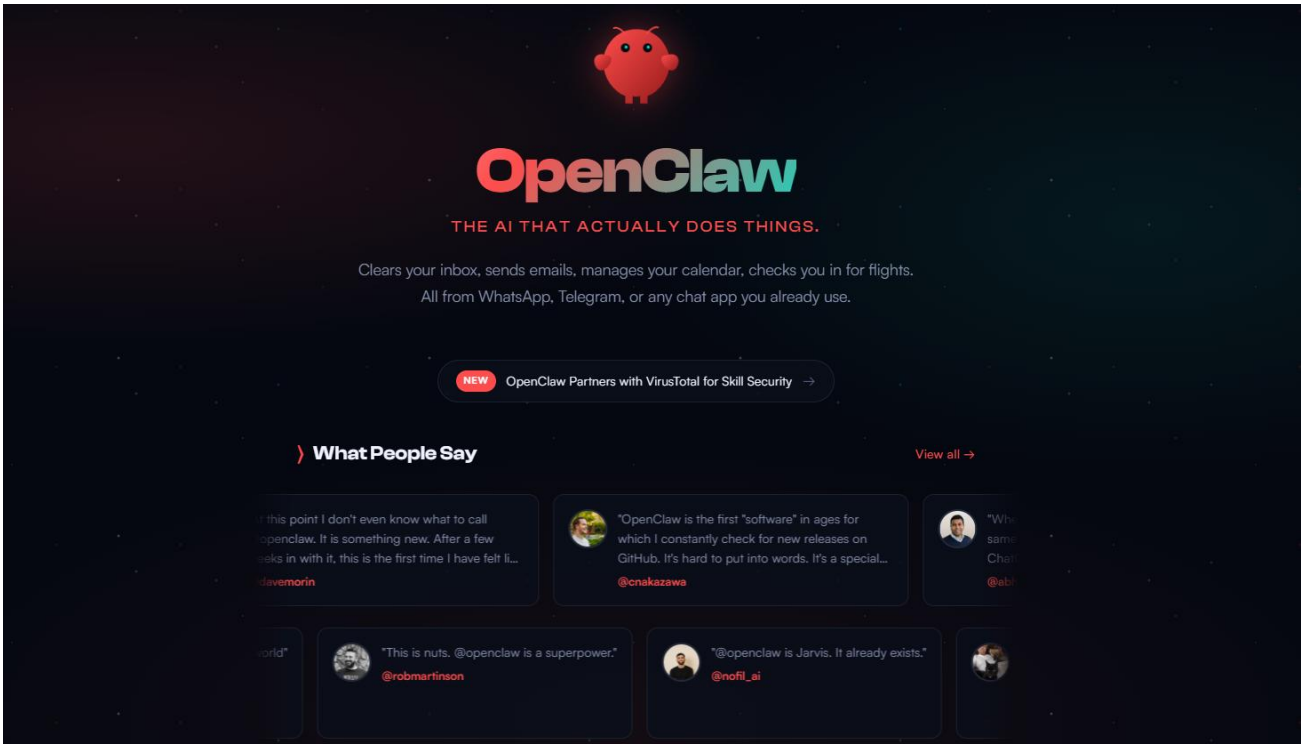
近期，開源 AI 智能體 OpenClaw 引發全民“養龍蝦”熱潮，成為現象級科技熱點。從這一專案引爆市場熱潮，到地方政府快速回應、推出專項扶持政策，前後僅用了約一個月。這一速度既印證了專案本身的技術號召力，更彰顯出監管層對新興 AI 生態的高度關注與扶持態度。3 月 7 日，深圳市龍崗區發佈《支持 OpenClaw&OPC 發展的若干措施（徵求意見稿）》，這份檔是全國首個針對該智能體專案落地的區級專項扶持政策。其回應效率、靶向扶持的精准度，均在行業內引發強烈反響。

與此同時，國內頭部互聯網大廠已圍繞 OpenClaw 開源框架完成多維度、全場景的生態佈局，其中騰訊正式上線完全相容 OpenClaw 全量技能體系的全場景 AI 智能體 WorkBuddy，打通多款主流辦公協同工具，同步在騰訊雲上線該專案的一鍵部署範本；位元組跳動依託火山引擎推出零配置開箱即用的雲上 SaaS 版 ArkClaw，在旗下 Coze 平臺完成 OpenClaw 協議適配，飛書上線官方測試插件，全程以豆包大模型為核心提供算力支撐；阿里巴巴推出適配團隊協作的開源衍生專案 HiClaw 與個人智能體工作臺 CoPaw，阿里雲同步上線對應容器鏡像與企業級安全算力解決方案；小米開啟國內頭部手機廠商首個端側適配產品 MiClaw 的小範圍封測，實現手機系統層任務執行並深度接入米家 IoT 生態；此外，百度智能雲率先上線 OpenClaw 一鍵部署服務並打通千帆大模型平臺，網易有道推出主打辦公教育場景優化的桌面端產品 LobsterAI，美團聯合聯想百應落地下沉市場的遠程部署服務，各家均從 C 端用戶、B 端企業、開發者生態等不同維度，快速完成對 OpenClaw 生態的全方位卡位與佈局。

需要警惕的是，工業和資訊化部網路安全威脅和漏洞資訊共用平臺於昨日發佈緊急預警：OpenClaw

開源 AI 智能體的部分實例，在默認配置或不當配置場景下存在高危安全漏洞，極易誘發網路攻擊、數據資訊洩露等安全事件。回歸行業本身，這場由 OpenClaw 掀起的熱潮，究竟會給 AI 產業發展帶來哪些深層變革？又將為投資者解鎖哪些全新機遇？

圖一：OpenClaw 展示情況



資料來源：OpenClaw 官網

➢ 爆火的 OpenClaw：開啟 AI Agent 全新發展範式

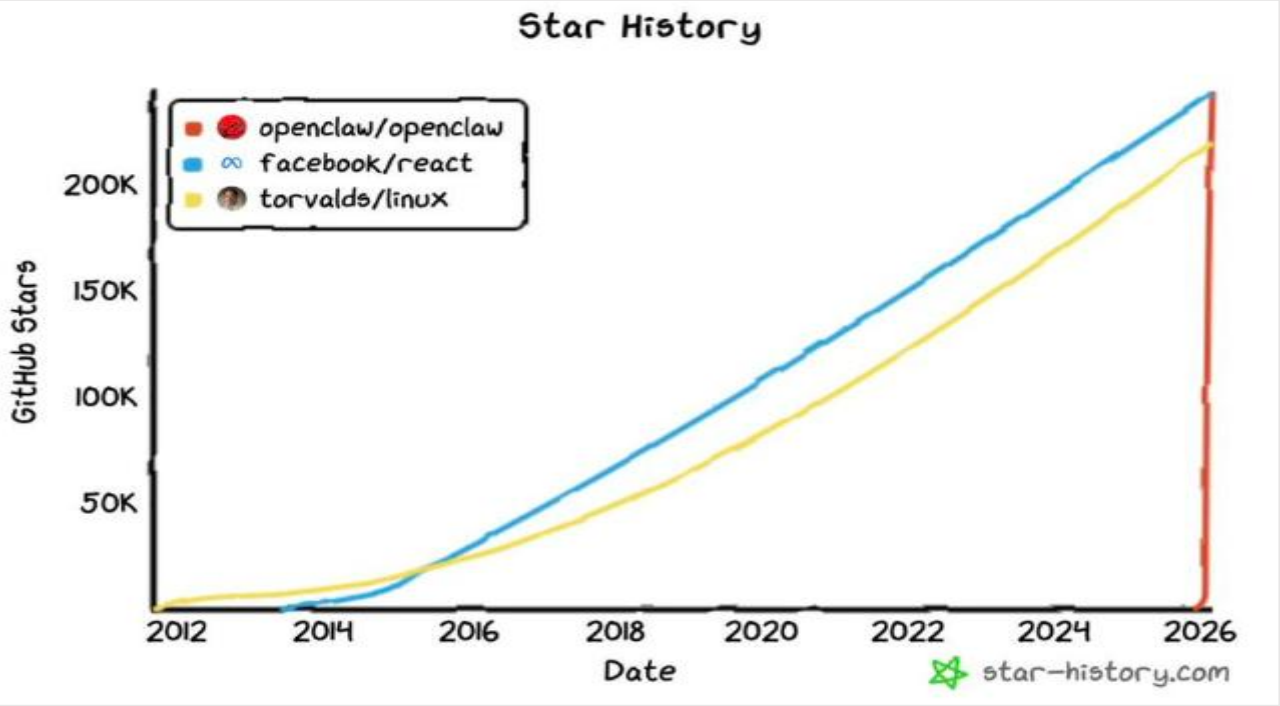
OpenClaw 正式引爆 2026 年開源 AI 的“行動智能”新紀元。繼 2025 年以 DeepSeek 為代表的大模型實現語言維度的“智能湧現”、開啟行業公認的“DeepSeek 時刻”後，2026 年由 OpenClaw 掀起的產業浪潮，標誌著 AI 完成了從“思考”到“執行”的歷史性跨越，2026 年也因此被行業定義為全球 AI“行動智能體”元年。

這款由奧地利程式員 Peter Steinberger 打造的開源框架，徹底打破了 AI 僅能完成問答交互的能力邊界，實現了 AI 對電腦終端的直接操控與全流程自動化任務執行。GitHub 官方數據顯示，OpenClaw 於 2026 年 3 月正式登頂 GitHub 全球軟體專案星標歷史榜首，僅用約 100 天便斬獲超 24 萬星標；對比之下，Linux 系統達成同等普及規模耗時近 30 年，其在開源社區的滲透速度創下了行業新紀錄。

英偉達首席執行官黃仁勳在摩根士丹利會議上 將 OpenClaw 稱作“我們這個時代最重要的軟體發佈”。他指出，OpenClaw 驗證了 AI 能夠深度適配高度個性化的場景、複刻人類工作負載，這一突破直接帶

動 Token 消耗量激增約 1000 倍，催生了行業內巨大的“算力真空”。而 OpenClaw 的爆發式增長，也正式宣告 AI 能力的核心賽道，已從單純的“智力迭代”，轉向自主化的“行動能力升級”。

圖二： OpenClaw 2026 年 3 月登頂 GitHub 全球軟體專案星標歷史榜首



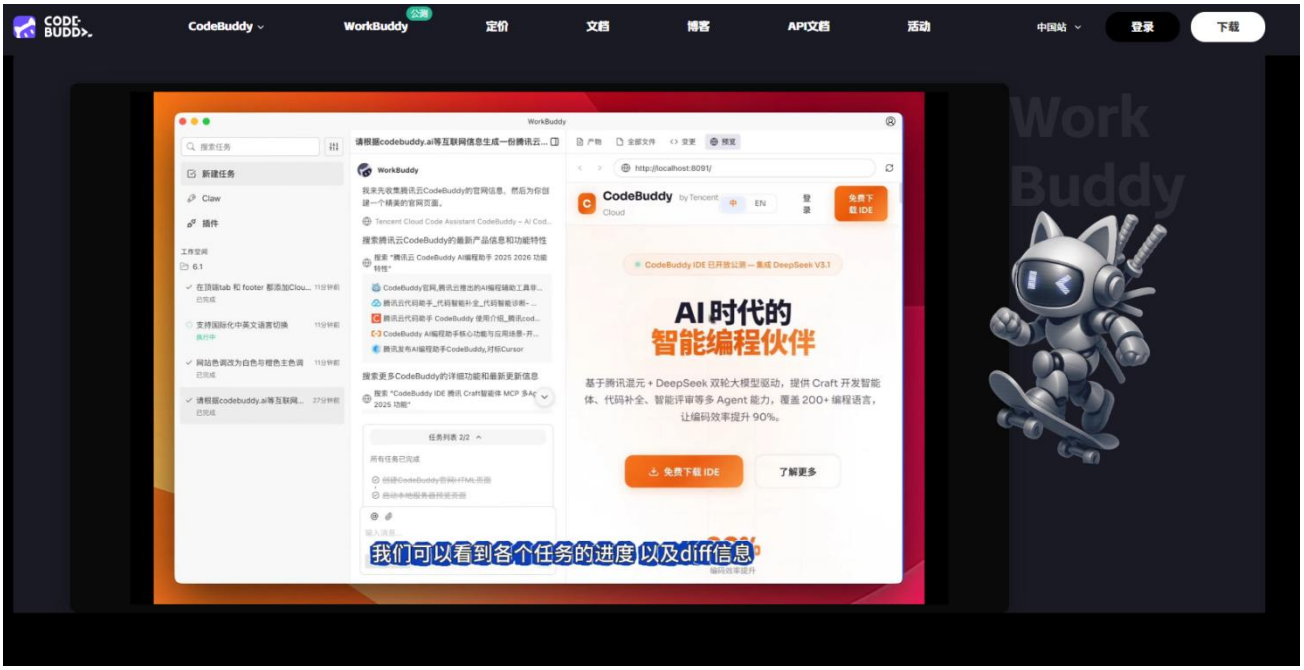
資料來源：GitHub 官方數據

* 國內外企業積極佈局

在海外 AI 生態方面，OpenClaw 的狂飆式增長，正在全面重構海外 AI 生態，整個海外科技產業的技術路線與資源佈局，都在圍繞這一開源行動智能體框架快速重塑。作為僅用 100 天便登頂 GitHub 全球軟體專案星標歷史榜首的里程碑式專案，OpenClaw 徹底打破了海外 AI 產業過去數年圍繞大模型“參數軍備競賽”的單一增長範式，將行業競爭的核心錨點從“模型的語言理解與思考能力”，全面轉向了“AI 的場景落地與自主執行能力”。在底層算力賽道，其帶來的千倍級 Token 消耗量激增直接催生了行業內巨大的算力真空，徹底改寫了全球 AI 晶片的供需格局與研發路線，英偉達、AMD 等頭部晶片廠商紛紛調整產品規劃，優先佈局適配行動智能體場景的算力產品；在大模型核心層，OpenAI、Anthropic、穀歌 DeepMind 等海外科技巨頭快速完成與 OpenClaw 的原生深度適配，推出專屬優化的模型版本與介面服務，將其作為大模型落地 C 端消費場景與企業級商用場景的核心載體；在開源開發者生態，圍繞 OpenClaw 打造的技能插件平臺 ClawHub 迅速成長為全球增速最快的 AI 開發者社區，短短數月上線超十萬個第三方技能插件，重構了開源 AI 領域的協作模式與商業變現路徑；而在創業與資本市場，海外市場圍繞 OpenClaw 上下游的創業專案迎來爆發式增長，一級市場投融資熱度持續攀升，從插件開發、安全防護到垂直行業解決方案，一條完整的行動智能體產業鏈條快速成型，徹底改寫了海外 AI 生態的原有版圖與長期增長邏輯。

在國內生態方面，OpenClaw 正掀起國內 AI 智能體產業的規模化落地熱潮，國內產業界快速回應、全面入局，從頭部互聯網大廠到 A 股產業鏈上市公司，紛紛加速接入 OpenClaw 開源生態、完成全維度佈局，全力推動 AI 智能體技術在國產算力適配與垂直行業場景的深度落地。頭部互聯網大廠作為國內 AI 生態的核心樞紐，率先完成全場景佈局與生態相容，以自身成熟的 C 端用戶池、B 端企業服務生態為依託，快速將 OpenClaw 的開源能力轉化為可落地、可複用的產品與服務。騰訊正式上線全場景 AI 智能體 WorkBuddy，實現對 OpenClaw 全量技能的完整相容，深度打通企業微信、QQ、飛書、釘釘等主流辦公工具，將智能體能力落地到個人辦公、企業協同等高頻場景，最低 1 分鐘即可完成配置的低門檻設計，大幅降低了普通用戶的使用壁壘；

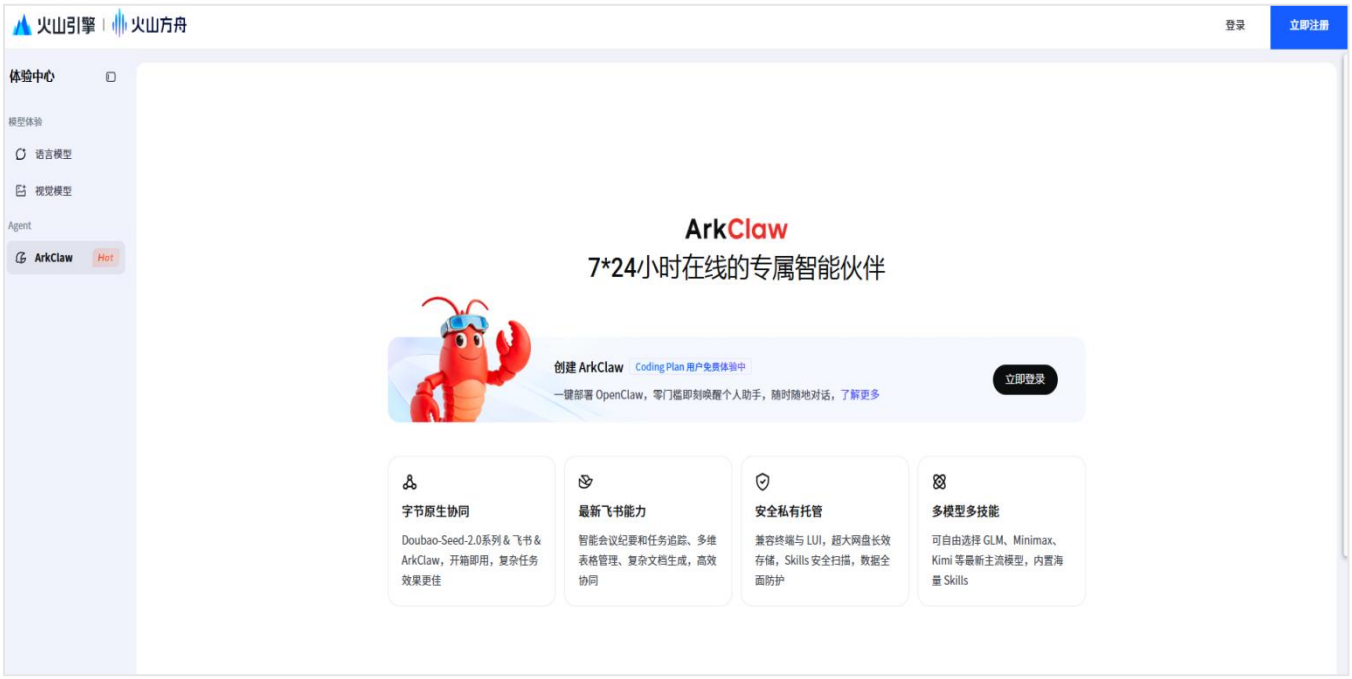
圖三： 騰訊 WorkBuddyAI 辦公助手



資料來源：WorkBuddy 官網

位元組跳動依託火山引擎推出零配置開箱即用的雲上 SaaS 版 ArkClaw，在旗下 Coze 平臺完成 OpenClaw 協議全適配，同步在飛書上線官方插件，以豆包大模型為核心提供算力支撐，為開發者與企業用戶提供了全鏈路的智能體落地解決方案；阿里巴巴推出適配中小團隊協作的開源衍生專案 HiClaw 與個人智能體工作臺 CoPaw，阿里雲同步上線 OpenClaw 容器鏡像與企業級安全算力方案，深度適配電商、供應鏈、企業管理等核心場景；百度智能雲作為國內最早上線相關服務的雲廠商，打通千帆大模型平臺實現多模型調度適配；小米則開啟了頭部手機廠商首個端側適配產品 MiClaw 的封測，實現手機系統層任務執行並深度接入米家 IoT 生態，拓展了智能體在端側與物聯網場景的落地邊界。各家大廠並非簡單複刻開源專案，而是通過生態相容與場景融合，把 OpenClaw 的通用能力與自身資源深度綁定，既推動了技術的普惠落地，也快速構建起基於開源生態的差異化競爭壁壘。

圖四：位元組 ArkClaw 平臺



資料來源：ArkClaw 官網

➢ 發展與規範並行：OpenClaw 爆火背後的安全風險警示

在現象級爆發、重構全球 AI 生態的同時，OpenClaw 同樣潛藏著諸多不容忽視的系統性安全風險與原生架構缺陷。為實現全場景自動化執行能力，OpenClaw 默認採用高許可權運行模式，需申請並啟用涵蓋本地檔系統全量讀寫、Shell 命令無限制執行、環境變數讀取、跨應用終端控制在內的系統級核心許可權，完全違背了網路安全領域的“最小許可權原則”，加之 AI 自主決策與用戶授權之間模糊的信任邊界，既可能因大模型固有幻覺問題引發不可逆的誤操作，更極易被攻擊者惡意利用，一旦突破安全防線便可直接獲取目標設備的完全控制權，甚至以此為跳板橫向滲透企業內網，造成規模化安全事件；其官方技能市場 ClawHub 更是存在極為嚴重的供應鏈安全隱患，平臺早期缺乏完善的代碼安全審計與嚴格的上架准入機制，大量由社區貢獻的第三方技能插件未經全面安全校驗即可上架流通，其中不乏偽裝成辦公集成、數據追蹤、自動化工具等剛需場景的惡意插件，可在安裝運行過程中竊取用戶帳號憑證、流覽器 Cookie、API 密鑰、加密錢包資訊等核心敏感數據，甚至靜默植入木馬程式、開啟反向 Shell，實現對用戶設備的長期隱蔽控制，已形成完整的黑產攻擊鏈條；與此同時，提示詞注入作為 AI 智能體區別於傳統軟體的獨有原生安全威脅，在 OpenClaw 身上表現得尤為突出，由於其核心架構無法從底層邏輯上嚴格區隔“用戶授權指令”與“外部待處理數據”，攻擊者可輕易在網頁、郵件、文檔、圖片等用戶日常接觸的各類載體中嵌入隱藏的惡意指令，且此類攻擊具備極強的隱蔽性，傳統網路安全防護手段難以實現有效攔截與提前預警，成為懸在海量用戶頭頂的重大安全隱患。

該開源專案潛藏的安全風險也同步引發了國家級監管機構的重點關注與規範引導：3 月 10 日，國家互聯網應急中心正式發佈 OpenClaw 安全應用專項風險提示，為一路走高的行業熱潮敲響了合規警鐘，

也為各類主體的部署應用劃定了核心安全準則。該提示明確建議，相關企事業單位與個人用戶在 OpenClaw 的全流程部署與應用中，需重點落實四項安全管控動作：強化網路訪問控制，收緊非必要的網路許可權與端口開放；加強帳號憑證全生命週期管理，杜絕弱口令、明文存儲等高危操作；嚴格審核第三方插件的來源與安全性，防範惡意插件帶來的入侵風險；持續跟進官方補丁與安全更新，及時修復已知安全漏洞。此次國家級專項風險提示，精准錨定了當前 OpenClaw 普及過程中暴露的普遍性安全亂象。隨著“養龍蝦”熱潮從科技圈快速破圈至大眾市場，大量缺乏網路安全防護能力的個人用戶、中小微企業甚至基層單位紛紛跟風部署，不少用戶直接採用第三方非正規鏡像、一鍵安裝包，未做任何安全加固就將默認配置的實例接入辦公系統、企業內網與個人敏感帳號，極易引發數據洩露、網路劫持、遠程控制等惡性安全事件。與此同時，OpenClaw 開源生態中湧現的海量第三方插件良莠不齊，大量未經安全審核的插件暗藏惡意代碼，成為網路攻擊的核心入口，進一步放大了專案的安全隱患。

從地方政府火速出臺專項扶持政策，到國家級監管機構同步發佈安全風險提示，一扶持一規範的雙向動作，為 OpenClaw 在國內的長期健康發展劃定了清晰的框架，這意味著國內 OpenClaw 生態的佈局，不會止步於簡單的技術複刻與跟風部署，而是將在安全可控、合規運營的前提下，推動 AI 智能體技術在國產場景的深度落地，真正實現技術創新與風險防控的雙向平衡，為 AI 智能體產業的規範化發展樹立標杆。

➢ 投資者應該關注哪些機會？

OpenClaw 作為當前全球 AI 領域用戶關注度最高的標杆專案之一，憑藉其在智能體技術上的突破性進展與現象級市場熱度，有望成為推動 AI 產業正式邁入 Agent 智能體時代的核心驅動力，並為 AI 全產業鏈發展帶來多維度的深遠影響。

首先，OpenClaw 帶動的 Agent 規模化應用，將帶來全網 Token 消耗量的加速攀升，進而持續拉動底層算力的剛性需求，支撐算力全產業鏈維持高景氣度上行趨勢，同時延續算力鏈條的通脹韌性。不同於傳統對話式大模型單次交互的有限 Token 消耗，AI Agent 在任務拆解、多輪推理、工具調用、結果校驗的全流程中，會帶來單任務 Token 消耗量的數十倍甚至上百倍增長，而 Agent 應用的規模化普及，將催生指數級擴容的 Token 處理需求，這一需求將直接向上傳導至算力基礎設施層，帶動 AI 晶片、GPU、算力租賃、高速光模組、液冷數據中心等算力全產業鏈的需求擴容，為產業鏈相關企業帶來長期且確定的增長動能。投資者可重點關注 A 股市場各細分環節的核心標的，包括 AI 晶片及先進封裝領域，如海光信息(688041.SH)、龍芯中科(688047.SH)、長電科技(600584.SH)、通富微電(002156.SZ)等細分環節龍頭；算力運營/ IDC 領域的數據港(603881.SH)、鴻博股份(002229.SZ)等核心標的。

與此同時，OpenClaw 掀起的全球 Agent 技術浪潮，將為國產大模型產業帶來需求擴容與全球化出海的雙重機遇。一方面，Agent 應用的爆發式增長，將直接催生對底層基礎大模型的旺盛需求，具備領

先技術迭代能力、豐富場景適配經驗、完善生態佈局的國產大模型廠商，將率先承接來自應用層的增量訂單，加速自身商業化落地進程；另一方面，Agent 的全球化普及趨勢，也為國產大模型打開了廣闊的出海空間，依託國內海量場景打磨出的技術能力與成本優勢，國產大模型可通過適配全球 Agent 應用的底層需求，快速切入海外市場，逐步打破海外大模型廠商的壟斷格局。A 股市場的核心受益標的包括：星火大模型龍頭、擁有國內領先的智能體開發平臺，深度佈局辦公、教育、工業等場景行動智能體落地的科大訊飛(002230.SZ)；依託天工大模型打造開源智能體框架、深度適配海外開源生態且開發者生態完善的昆侖萬維(300418.SZ)。港股市場可重點關注擁有混元大模型，以微信生態為智能體提供國內最大 C 端落地場景，通過企業微信、騰訊雲為企業級智能體輸出完整解決方案的騰訊控股（0700.HK）；依託通義千問大模型與阿里雲智能體開發平臺，深度佈局電商、企業服務、工業等垂直場景的阿里巴巴- SW（9988.HK）；以及手握日日新大模型與 SenseCore 智算基礎設施、多模態行動智能體佈局領先的商湯-W（0020.HK）。

最後，Agent 時代的全面到來，也將對網路安全體系提出全新的升級要求，催生 AI 原生安全的全新增量市場。AI Agent 具備自主決策、自主執行、跨系統跨平臺調用的能力，其應用過程中涉及的數據隱私保護、指令合規校驗、惡意行為防控、系統許可權管控等安全需求，遠高於傳統 AI 應用。OpenClaw 的普及將推動全行業重視 Agent 原生安全體系的搭建，帶動數據安全、AI 安全審計、隱私計算、終端安全防護等相關領域的需求快速釋放，為網路安全產業開闢出全新的高增長賽道。具備全鏈路 AI 原生安全技術佈局、成熟 Agent 專屬防護解決方案、深厚行業客戶壁壘的廠商，將率先承接行業爆發帶來的業績紅利，投資者可關注啟明星辰(002439.SZ)、天融信(002212.SZ)等網安核心股票。