EAGLE CLOUD

www.eaglecloud.com

SASE + AI
辦公安全一體化平台

全球合規安全辦公基礎設施

關於我們

首家「人類員工 + 數字員工」全生命週期統一管控的 AI 基礎設施提供商

願景 Vision

讓 AI 安全，讓辦公高效

目標 Mission

讓企業敢用 AI、用好 AI

團隊基因

源自頂級安全實踐

- 核心團隊來自阿里雲安全，曾打造0-30億商業規模
- 曾打造包括雲盾、WAF、雲防火牆、SASE等多個億元營收產品，服務累計超過10萬家企業；
- 源自阿里雲TOP客戶辦公安全最佳實踐

辦公安全領軍企業

AI辦公安全基礎設施

- 自主研發SASE平台 — 雲樞，提供業內領先的辦公安全一體化解決方案 ZTNA, XDLP, XDR, SWG, GA 及 AI 治理
- 服務1,000+ Top企業，成熟可靠、規模化交付；
- 覆蓋75%的四大會計師事務所、25% 的全球化獨角獸企業。

頂級資本投資

高速成長的安全廠商

- 連續四年業績超100%增長;
- 2025年全年盈利，NDR>140%;
- 覆蓋北美、新加坡、馬來西亞、香港等地，提供當地語系化服務，海外收入占比15%
- 紅杉資本、元璟資本頂級資本等投資;
- 完成兩年 三億RMB A輪融資;
- 2025年完成億元pre-b融資;
- 2026年中旬完成B輪融資

企業邁向AI化的辦公標配

EAGLE CLOUD

重塑全球辦公體驗

全球組網加速，零信任訪問，支持跨境、遠程、多分支辦公，安全訪問內網與雲應用，防越權訪問、數據非法下載與外部攻擊。

築牢數據安全防線

為企業提供全鏈路的數據保護，確保敏感信息如研發代碼、客戶數據等全生命週期的安全，降低數據洩漏風險。

強化終端安全防護

終端安全一體化，融合終端資產管理、銀狐釣魚防護、軟件正版化管理、USB外設管控等能力，全面提升終端運維與安全防護水平。

AI 賦能辦公安全，提升生產力

針對企業 AI 編程、AI Agent（OpenClaw）等高風險場景，解決數據洩漏、系統越權、操作不可控等安全隱患，讓企業安全落地 AI 應用、高效開展辦公業務

企業辦公的安全問題，本質上是終端、網絡、數據和 AI 的統一治理問題

備受香港領先創新機構信賴

億格雲（Eagle Cloud）榮幸成為「港深創科園」(HSITP) 首批 AI 及 Data Science 孵化計劃成員，深度融入香港頂尖的創新生態系統。

HSITP 港深創科園　HKAI LAB　Lenovo

港深創科園孵化計劃 — 2026 首批成員

- 經官方機構嚴格篩選，印證了億格雲的技術實力，以及其在香港企業市場的高度契合

HKAI Lab 合作夥伴

- 接入香港專屬的 AI 創新網絡，開拓與頂尖企業共同研發與協作的機遇

聯想 (Lenovo) 合作夥伴

- 開展技術協作，將億格雲的服務能力擴展至聯想亞太區的企業及基礎設施生態系統

國際辦公室設立於香港，覆蓋港澳台及亞太地區，並獲得市場權威機構的鼎力支持。

EAGLE CLOUD

備受業界認可

5M+
用戶授權

20+
行業覆蓋

300K+
最大單一部署

1000+
頭部客戶選擇

辦公安全一體化SASE解決方案領導者

ISO 27001

ISO 9001

SOC II Type 2

CCRC 3

CMMI 3

AI辦公基礎設施服務唯一提供商

EAGLE CLOUD

基於雲原生一體化辦公架構，

構建 AI 原生辦公支撐平臺，助力企業更安全、高效、簡單使用 AI

AI賦能提高效率

讓企業安全的用AI

AI-DR

IT 數字員工Agent

AI-IRM、AI-EDR、AI-Net, AI-ITSM……

企業級AI員工助手

AI員工助手

AI-Native辦公安全基建：

AI時代必備的基礎設施

重塑辦公基礎能力

網路
ZTNA、網路准入
SD-WAN、全球加速 ……

安全
EDR、DLP
IA-SWG、身份管理、威脅情報 …

IT&可觀測
MDM、ITOM
DX、可觀測 ……

開放性雲數倉
中繼資料、分析引擎、三方對接 ……

搭建領先平台底座

一個終端

↓43% 頻寬成本

500萬+ 已覆蓋終端

一張網絡

<100ms 即開即用低延時

<15分鐘 全球部署接入、零網路改造

一朵雲端

↓80% 本地資源佔用

統一管控 彈性擴容

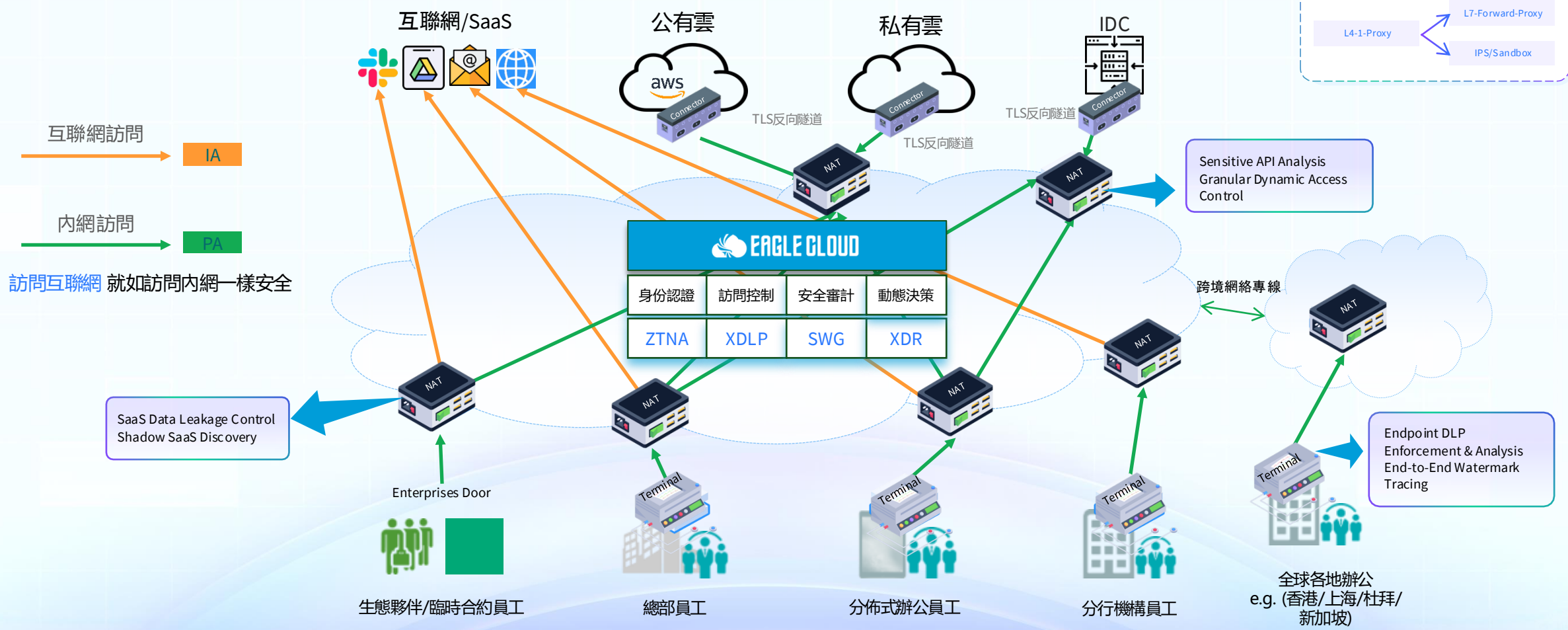
一個身份

300萬+ 已覆蓋員工

↑3X 運營效率

全球辦公安全體系

通過SASE架構：一朵集中管控的“雲” + 一張全球加速的“網” + 一個安全整合的“端”



能力圖譜 | 一體化 & 全自研

EAGLE CLOUD

AI

AI -ITSM	Shadow AI	AIDR	AI 運營助手	IRM	大模型分類分級

統一平台

終端安全

終端安全（防攻擊）			桌面管理（簡單運維）		
惡意行為	防釣魚	防勒索 /防銀狐	軟件倉庫	軟件分發	軟件禁用
攻擊收斂	漏洞加固	病毒查殺	資產管理	遠程桌面	版權檢測

數據安全

數據防泄露（XDLP保護終端數據）					
終端數據 分類分級	外設傳輸通道管控	圖像識別&圖像 OCR	應用訪問控制和審計	應用敏感數據識別	自動化用戶風險畫像
屏幕水印	文件水印	違規截屏調查	網絡外發通道管控和審計	HTTPS 應用數據防泄露	數據地圖&數據溯源

網絡安全

內網准入（NAC，安全接入內網）		上網管理（SWG，安全訪問互聯網）		零信任（ZTNA，安全訪問內部）	
一人一密碼	合規入網	TLS 無感解密	上傳/下載安全防護	API 精細化訪問控制	敏感數據不落地
啞終端入網	訪客入網	千萬級應用庫	URL 級管控	IM 工作台應用免登錄	動態權限調整

一套彈性高效的 網絡

CDN 協同	全球加速	資源整合	互聯互通	無界體驗	
全球網絡節點	就近接入	網絡加速	自動選路	SD-WAN 融合	基礎設施免改造

一個能力融合的 終端

Windows	MacOS	Linux	Ubuntu	信創	UOS
SaaS部署	混合部署	私有化部署	SDK 版客戶端集成	企業現有門戶集成	

AI安全檢測與回應
AIDR

安全治理 AI 應用

EAGLE CLOUD

01 可感知

AI 使用必須 **可識別、可洞察**

識別誰在用 AI、用什麼AI工具、上傳了什麼資料、產生了什麼輸出

02 可管控

AI 行為必須 **可被約束**

輸入可過濾、輸出可攔截，敏感性資料外發可阻斷，越權行為可制止

03 可回溯

AI 結果必須 **可追蹤、可審計**

全鏈路日誌、原始資料回溯、風險事件定位、閉環整改有據可循

AI治理的目標不是限制 AI，而是讓企業更安全的使用 AI 。

AIDR：AI安全檢測與回應

EAGLE CLOUD

讓員工安全可控的使用AI，讓 AI 釋放價值

幫助企業看見員工在用什麼 AI、傳了什麼資料，並精細化管控 AI 使用過程中的安全風險

員工使用 AI 安全

- 管控全管道AI工具使用，覆蓋Web、用戶端及外掛程式入口
- 消除Shadow AI盲區，即時攔截並脫敏敏感提示詞

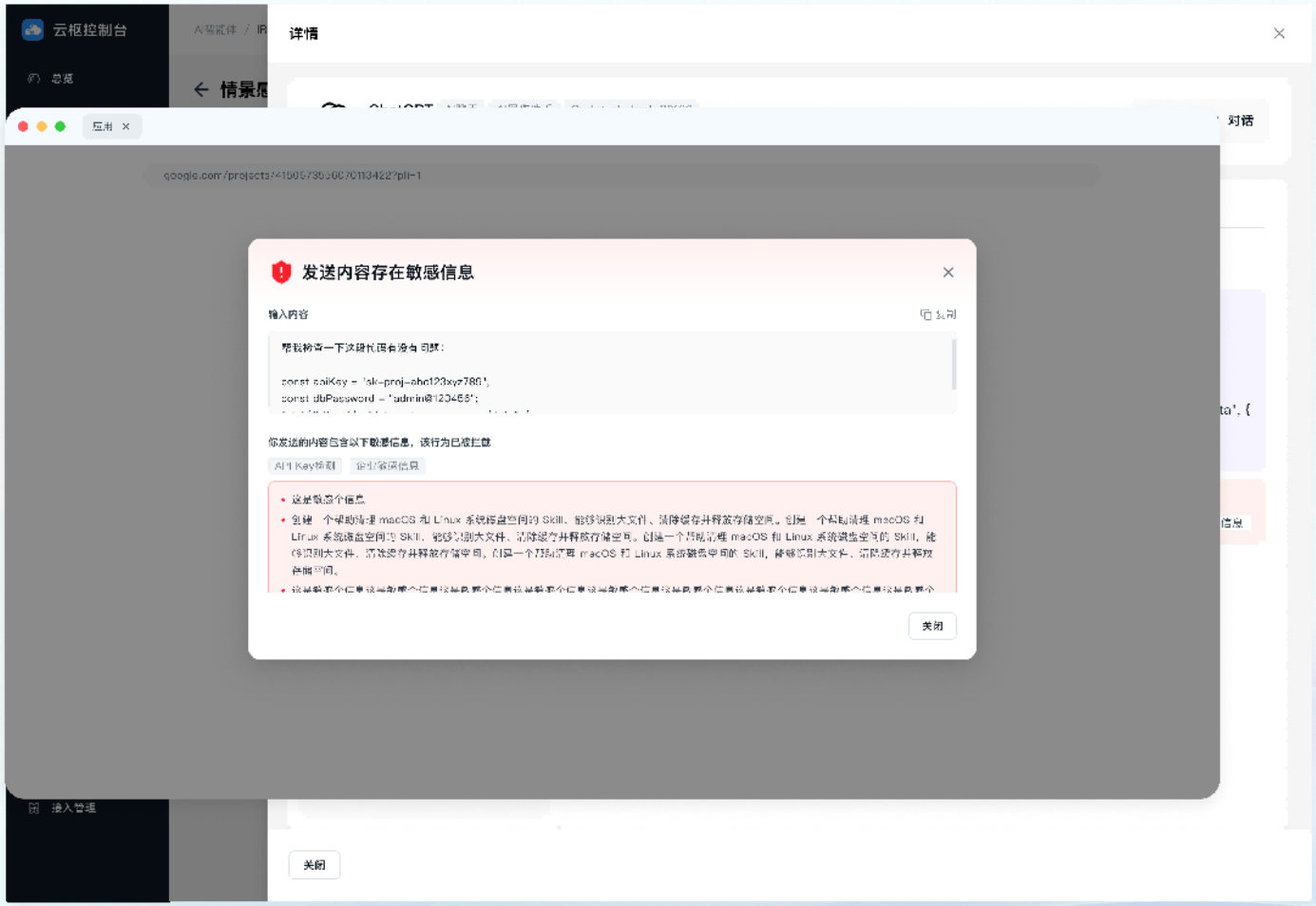
AI 程式設計安全

- 防護Copilot/Cursor等工具風險，自動識別原始程式碼與金鑰
- 防止內部架構資訊與敏感性資料洩露至協力廠商模型

AI 智慧體安全

- 全鏈路監控MCP協議與Skills操作，精准攔截注入與投毒
- 構建縱深防禦體系，防止智慧體終端成為攻擊突破口

場景1：員工安全使用AI



全量對話資訊還原

全面還原員工與AI交互的全量資訊，包括 Prompts 提示詞、完整會話記錄、工具調用參數及上下文資訊。

全鏈路行為還原

不僅還原對話內容，更深度解析 MCP和 Skills 調用鏈路，清晰展示 AI 工具的實際執行路徑與邏輯。

執行管控與審計

基於行為還原資料，對MCP/tools 等工具的執行過程進行即時審計和策略管控，確保操作合規安全。

場景1：員工安全使用AI

核心目標：全鏈路即時追蹤

構建全鏈路安全監控體系，即時追蹤AI智慧體經由MCP協議與Skills執行的每一次自動化操作。

行為還原：操作可追溯

全面還原Agent執行的每個操作細節，確保審計可追溯。

執行管控：動態合規檢查

對Mcp/tools等工具的執行動作進行動態管控，確保操作符合規範。

行為攔截：風險即時阻斷

發現敏感行為或違規動作時進行及時阻斷，有效防範潛在風險。

威脅情報：源頭防範

基於威脅情報禁止安裝風險mcp/skills，從源頭杜絕安全隱患。

場景2：AI 程式設計安全

核心防護目標

保護開發者使用 Copilot、Cursor 等 AI 工具的安全風險，自動識別並脫敏原始程式碼、API 金鑰及內部架構資訊，防止敏感性資料外泄。

IDE外掛程式代碼外發檢測

即時監控代碼編輯器的外發請求，精准識別並攔截敏感代碼片段，確保代碼資產安全。

API金鑰與憑證自動脫敏

內置敏感資訊識別引擎，自動發現代碼中的金鑰與憑證並進行脫敏處理，從源頭阻斷洩露風險。

場景3：AI 護欄

為企業自建的 AI 應用構建輸入輸出全鏈路防護體系

AI 應用防護

提示詞越獄/注入攻擊檢測

- 基於專有模型對使用者輸入的內容進行安全風險分析檢測

回應內容安全過濾

- 輸出側即時過濾敏感資訊洩漏，確保 AI 應用在安全邊界內穩定運行。

AI Agent 安全治理

EAGLE CLOUD

定位

面向 OpenClaw 等 AI Agent 的全鏈路防護體系

覆蓋「人、Agent、工具與資料」的全生命週期風險，幫助企業安全落地 AI 生產力；以「最小許可權 + 白名單」約束邊界，結合審計與取證形成閉環治理。

可見：全面 AI Agent 的發現

AI Agent 發現

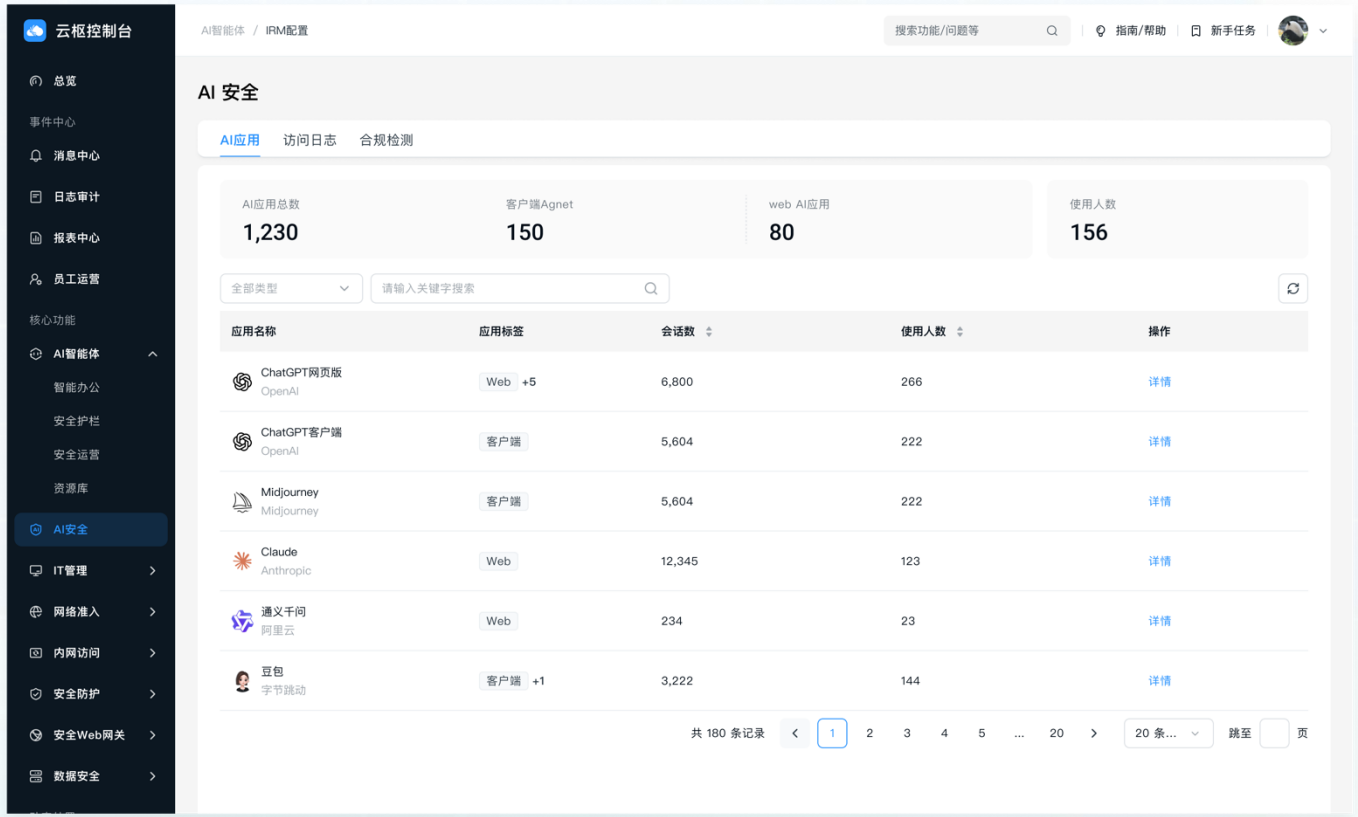
自動發現

跨 Windows / Mac 自動識別
OpenClaw 或類 Claw AI Agent 軟體。

應用情報

對各類 AI Agent 應用情報採集，發現軟體合規風險。

支持對 AI Agent 進行運行管控
(支持OpenClaw、QClaw、AutoClaw
等各類 AI Agent 軟體)



審計&檢測：深度檢查 AI Agent 配置和行為

EAGLE CLOUD

基礎配置審查

採集發現AI Agent的基礎配置，如：模型、BaseURL；感知是否使用了外部不安全的供應商

Agent 能力配置審查

自動採集SKILLS、MCP、定時任務、消息通道等配置資訊。

1:1 還原用戶與 AI Agent 的會話

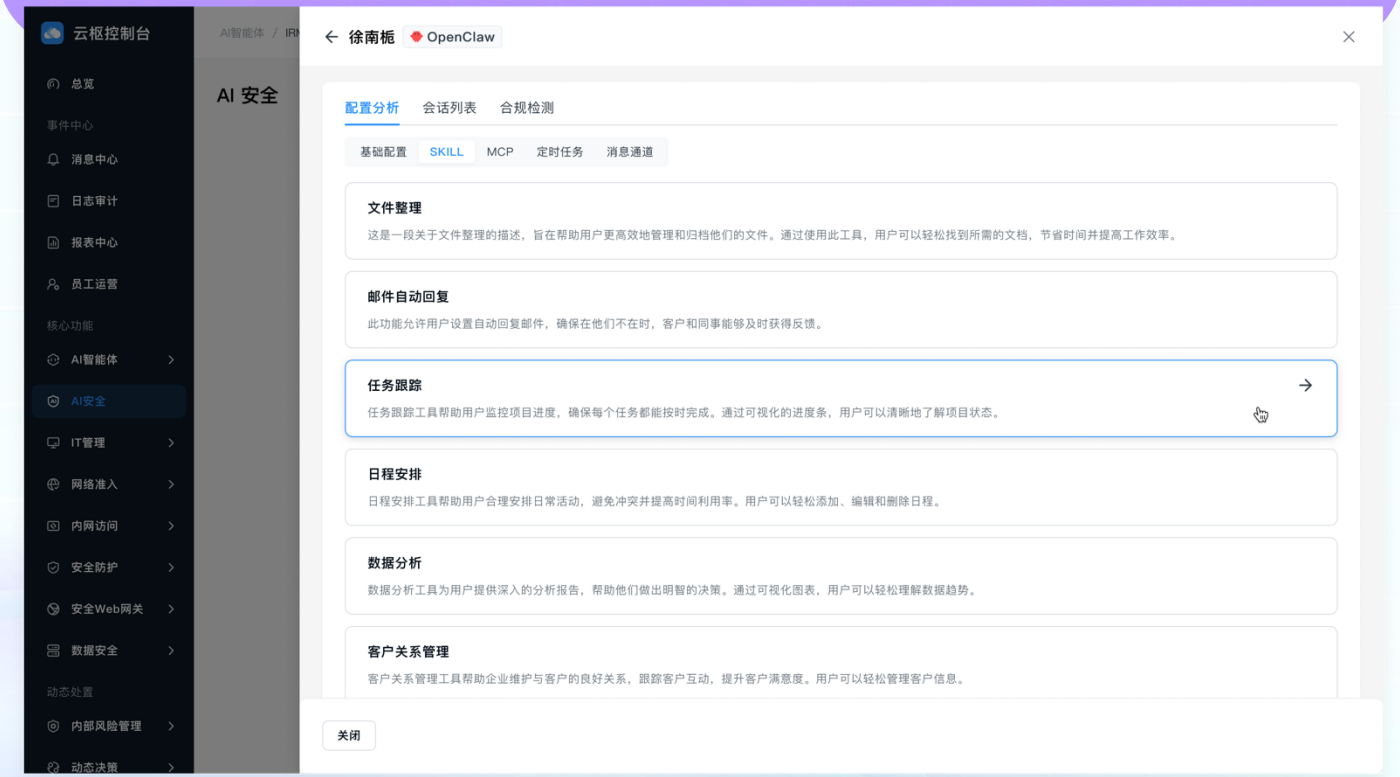
AI Agent 行為管控

工具調用　命令執行　惡意外連

敏感資訊識別　惡意行為攔截

配置合規檢查

檢查 OpenClaw 等 AI Agent 軟體的配置安全風險，例如綁定0.0.0.0 對外暴露風險等。



SKILLS：供應鏈風險檢測

EAGLE CLOUD

SKILLS 發現掃描

自動發現已安裝的 SKILLS 內容，檢測是否存在風險和調用情況

SKILLS 還原

解析SKILLS目錄內容，深度審查 SKILLS 風險。

SKILLS 安全掃描

- 靜態安全掃描能力：惡意程式碼、反 Shell等惡意命令
- 惡意提示詞檢測

SKILLS 情報賦能

基於雲端 SKILLS 情報資料，為員工安裝的SKILLS進行檢測，發現投毒 SKILLS

SKILLS 技能禁用 | 安裝攔截 | 卸載

管控：Agent 行為安全

EAGLE CLOUD

企業級安全指南

將企業安全性原則寫入系統提示詞，約束 Agent 行為邊界，抵禦惡意提示詞劫持。

命令執行阻斷

內置大量影響企業內網安全命令自動阻斷，支援自訂配置阻斷命令。

敏感資訊防護

監控對於.env、SSH金鑰等敏感檔訪問，識別異常讀取自動阻斷。

風險功能變數名稱/IP請求防護

對每次外聯請求進行情報比對，識別並攔截惡意功能變數名稱、C2 與釣魚網站。

聯絡我們

億格雲科技有限公司

香港

香港銅鑼灣禮頓道77號
禮頓中心20樓2012室

新界落馬洲河套地區
港深創新及科技園第8座8樓818室

www.eaglecloud.com

商務及市場查詢：

Clement Tam
Business Development & Market Growth Lead
clementtam@eaglecloud.com
(852) 9022 9271

一般查詢：

info@eaglecloud.com