

# AI世代資料外洩防護

# InstantLock

管理、備份、  
側錄、過濾

## AI可載舟，亦可覆舟 AI員工，也要合法合規

### ■ 開道+端點：雙重防禦架構

L7 打造「開道+端點」聯防架構，為企業建構全方位無死角的資料外洩偵測防線。在網路開道端，系統能深度控管並稽核所有網頁瀏覽、Webmail、雲端硬碟以及生成式 AI 的外連流量；在用戶端點端，則進一步延伸管控觸角，全面側錄與鎖定 LINE、Teams、WeChat 等通訊軟體與 Outlook 的對話與傳檔行為。此雙軌架構將網路層與終端應用完美結合，不論員工處於何種工作模式，皆能實時識別並精準攔截任何企業機敏資料外流。

### ■ 數位鑑識不費力，務求無痛導入

過SSL解密，跨平台的Windows/Linux/MAC都可被成功解析內容。導入時須透過AD派送CA憑證，透明導入不改網路架構，也不會更改PC電腦的IP，用戶無感導入。目前能解析一般最主流的AI應用(ChatGPT、Grok、DeepSeek、Gemini、Copilot、NotebookLM)、https網頁郵件(Gmail / Outlook / YahooMail /...)、最主流的網頁硬碟(One Drive / Google Drive /...)、最主流的聊天軟體(Line / Teams / WeChat / Facebook Chat /...)。這些鑑識的資料都儲存在本地的InstantLock Management Server。

### ■ DLP 單一主管審核與限期放行機制

當系統主動攔截機敏資料外傳時，員工可即時發出例外放行申請，以確保業務流程順暢不中斷。主管可於線上審核介面直接檢視被攔截的實體檔案內容與傳輸細節，精準評估外發的正當性，並迅速決策要繼續封鎖或授權例外通過。若核准通過，系統支援設定「限期放行」，該檔案僅允許在指定的時間內完成傳送，



對話、傳檔、圖片  
資料外洩偵測

#### 郵件雲



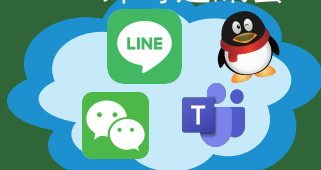
登入、寄信、寄信夾檔  
讀信、讀信夾檔

#### 社群雲



登入、塗鴉牆、留言、  
張貼照片、動態消息

#### 即時通訊雲



登入、傳訊息、傳檔

#### 網路硬碟雲



登入、檔案上傳、檔案下載



### ■ L7系統無縫接軌 ISO 27001：輕鬆落實資料防外洩合規

針對「8.12 資料外洩防護」、「8.9 資訊傳輸」條款，L7 設備透過開道與端點聯防架構，全面解密並嚴格審查通訊軟體、AI 工具及雲端硬碟的日常對話與檔案傳輸行為，實時識別並強制攔截各類未經授權的機敏資料外流。系統自動生成完整且不可竄改的唯讀審計日誌軌跡，協助企業無痛滿足資安稽核要求，順利通過 ISO 27001 國際驗證。

另外包含台灣的個資法、美國的沙賓法案、PCI-DSS, HIPAA, SEC, FINRA, FSA, IIROC, FERC, NERC, CFTC, NFA。他們都要求電子通訊必須要記錄並存檔多年供稽核使用。針對https的數位鑑識有其必要性，因為目前犯罪行為都偏向藏匿至加密的https通道中。