確保員工安全使用生成式 AI 和自主式 AI

透過 Cloudflare 的 SASE 平台實施的多種保護，讓您的團隊能夠安全地使用任何 AI 工具。

重獲控制權，釋放生產力

採用 AI 的熱潮帶來了一連串風險且不斷增加，包括資料外洩、違反法規以及攻擊面持續擴大。完全封鎖 AI 只會犧牲競爭優勢，而嘗試各種單點解決方案只會增加複雜性。

Cloudflare 透過擴展可見度、緩解風險，並在 AI 環境中全方位保護資料，為您的組織使用 AI 保駕護航：

- **探索影子 AI**，並管理適用於所有已批准和未批准 AI 工具的原則。
- 透過基於身分的存取控制和狀態管理，**強化 AI 治理**。
- 透過封鎖使用者提示中的敏感性資訊、實施主題防護機制以及搜尋 AI 工具中的設定錯誤，**防止資料遺失**。

無論您的 AI 策略是僅限用於特定應用程式還是嘗試更多種類的工具，都可以透過擴展 Cloudflare 來確保採用 AI 的安全。

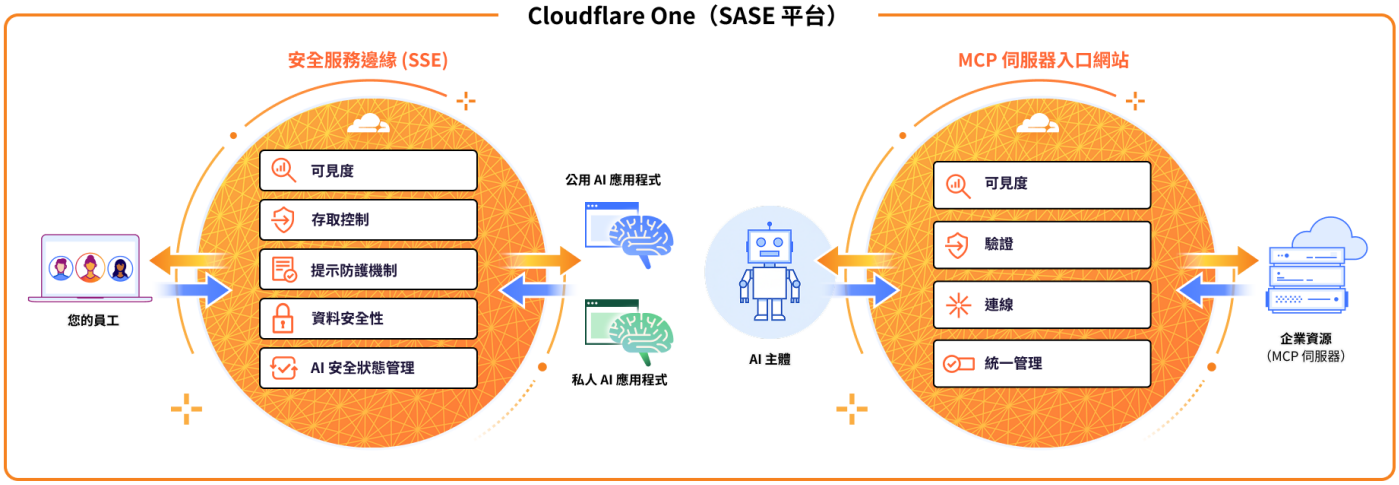
為什麼選擇 SASE 來確保員工安全使用 AI

Cloudflare 的安全存取服務邊緣 (SASE) 平台位於員工和 AI 工具之間。因此，SASE 成為很多組織安全使用 AI 的理想起點。

無論是員工和 ChatGPT 聊天，還是 AI 主體在企業資源中收集資訊，Cloudflare 的 SASE 平台都能實施一致的安全控制。

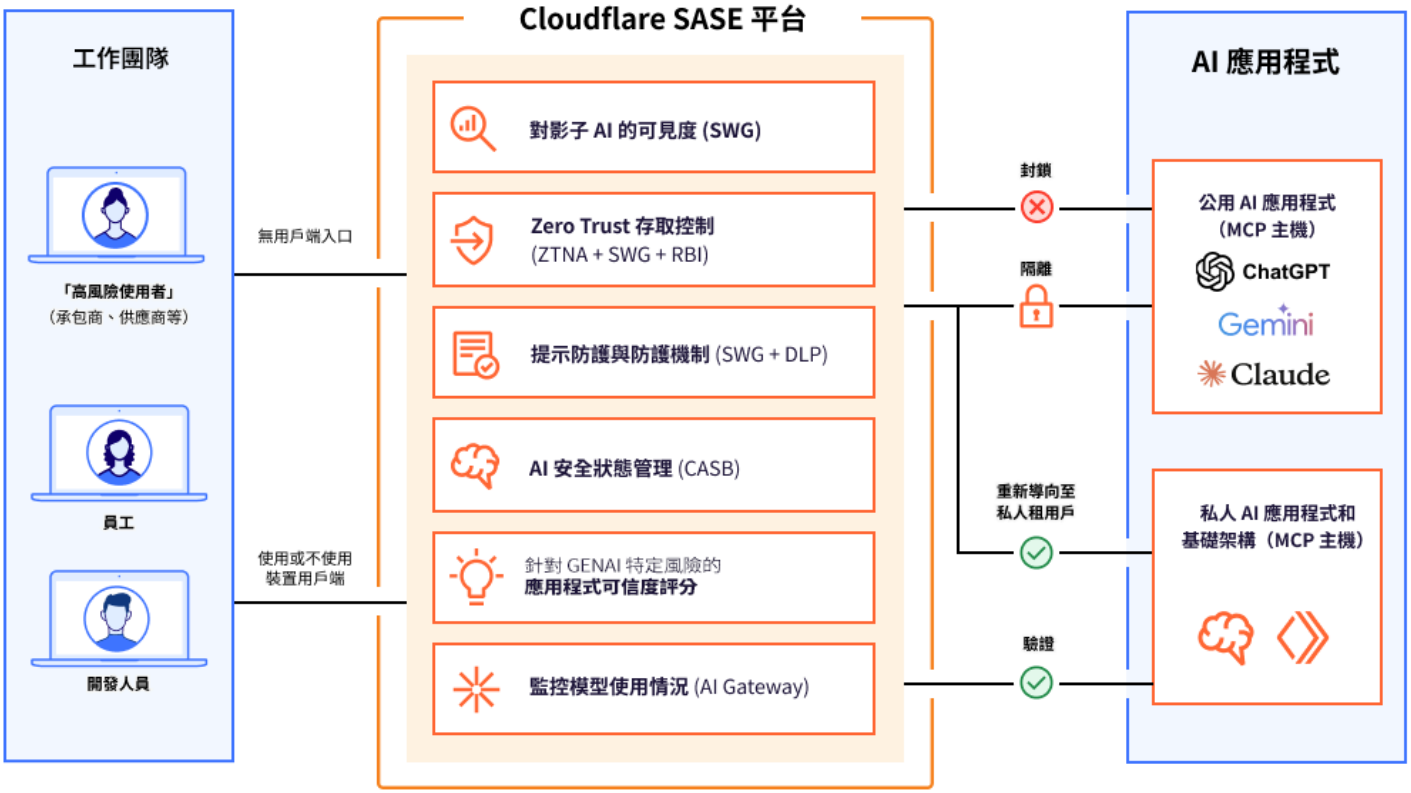
確保生成式 AI 和自主式 AI 通訊安全

Cloudflare 的 SASE 平台提供一個統一的儀表板和控制平面，用於管理整個組織內的人類與 AI 互動以及機器與機器互動。



與其他 SASE 廠商不同，Cloudflare 也能協助連接及保護面向公眾且支援 AI 的應用程式和工作負載（例如，網站的 AI 聊天機器人或推薦引擎）。

透過 Cloudflare SASE 平台上的 AI 使用控制，**保護使用者與生成式 AI 應用程式之間的通訊**



- **可見度：**透過內嵌流量檢查，探索並分析影子 AI 的使用。使用透明評分評估那些 AI 應用程式所帶來的風險。
- **存取控制：**封鎖、隔離、重新導向或允許使用者連線。針對每個應用程式強制執行基於身分的 Zero Trust 規則。
- **提示防護和防護機制：**基於意圖（例如，越獄嘗試、程式碼濫用、PII 請求）偵測並封鎖使用者提示。
- **資料安全：**透過針對 PII、原始程式碼等執行採用 AI 技術的資料丟失預防 (DLP) 偵測，阻止敏感性資料暴露。
- **AI 安全狀態管理：**透過 API（現已支援 ChatGPT、Claude 和 Google Gemini）與 GenAI 工具整合，使用我們的雲端存取安全性代理程式 (CASB) 搜尋設定錯誤。

客戶成果

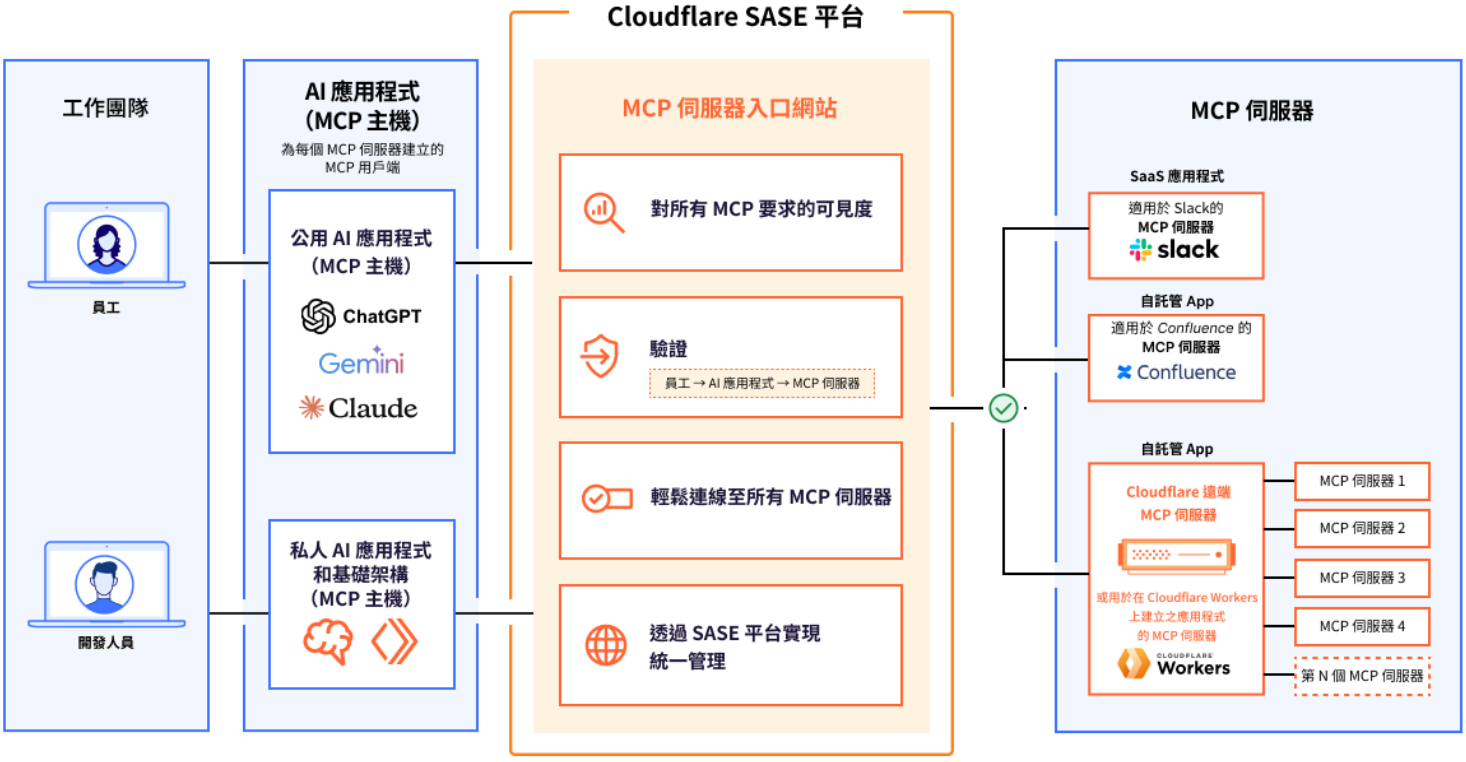
indeed
全球排名第一的求職網站

識別並控制影子 AI，同時執行 VPN 取代專案

APPLIED
保險科技公司

隔離如 ChatGPT 等公用 GenAI 工具，以封鎖複製-貼上敏感性資料

透過 Cloudflare SASE 平台上的 MCP 伺服器入口網站，**確保自主式 AI 通訊（AI 與資源）安全**



- **可見度：**彙總所有 MCP 請求記錄，以供稽核和分析。對每個 MCP 伺服器進行審查並核准，然後再將其新增至入口網站。
- **驗證：**基於身分驗證使用者對入口網站的存取。根據最低權限原則，設定對 MCP 伺服器的存取權限。
- **連線：**使用單一 URL 連接所有可存取的 MCP 伺服器，而非個別設定每個 MCP 伺服器。
- **統一管理：**對 AI 連線強制執行與對人類使用者相同的精細化存取原則。
- **針對每個入口網站自訂工具：**選擇為每個使用者提供的特定工具和提示範本。

注意：Cloudflare 的 MCP 伺服器入口網站支援任何 MCP 伺服器，包括（但不限於）在 Cloudflare 上建置或部署的任何遠端 MCP 伺服器。此功能可作為 Zero Trust 網路存取 (ZTNA) 控制使用。

閱讀此部落格，深入瞭解我們的願景。

準備好探索 Cloudflare 如何確保您安全使用 AI 了嗎？

申請研討會

