CLOUDFLARE

解決方案簡介

保護您的敏感性資料

更好的網路架構可實現更有效、更高效且更敏捷的資料保護。

為任何位置的資料提供統一保護

資料防護並非是一項新的要求，但向混合雲端架構的轉變，以及 AI 的快速採用帶來了新的挑戰：

- **93% 的員工**承認在未經批准的情況下將資訊輸入 AI 工具[1]
- **79% 的國家/地區**已制定資料隱私法規[2]

Cloudflare 在您的資料生命週期強制執行持續一致的控制項 ：

- **隨時隨地確保安全：**對 Web、SaaS、電子郵件和雲端流量強制執行持續一致的控制項。
- **封鎖 AI 外流：**分析 GenAI 提示以封鎖敏感資料並管理 AI 使用。
- **治理資料風險：**使用 CASB 來探索並管理影子 IT/AI，以及掃描 SaaS/雲端應用程式。

「所有這些未經授權的 AI 工具的興起，使得我們重新考慮我們的安全性方法。「我們目前正在探究 SASE。」
*——**AllSaints** 資訊安全主管*

為什麼選擇 SASE 而不是企業 DLP？

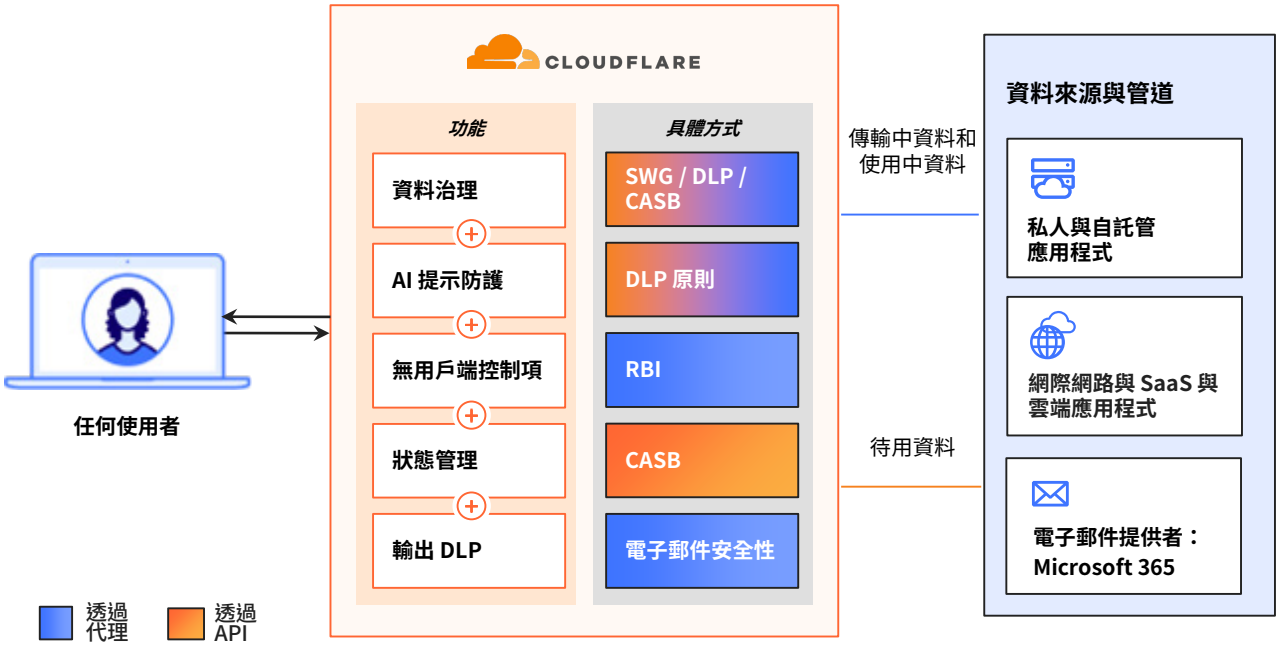
Cloudflare 的安全存取服務邊緣 (SASE) 平台建置於您的工作團隊與每個應用程式及資料來源之間。這使得 SASE 成為許多人開始安全保護資料的理想起點。

無論員工是存取 SaaS 應用程式中的資料、下載敏感性檔案，還是使用 GenAI 工具進行聊天，Cloudflare 的 SASE 平台都能在所有資料互動中強制執行持續一致的安全控制項。

運作方式

Cloudflare 的 SASE 平台內建於您的員工與資源之間，以便整合可見度與控制項。

藉助 Cloudflare 的 SASE 平台，在 Web、SaaS、電子郵件和雲端流量中帶來了採用 AI 技術的資料防護。



即時的內嵌資料防護

- **精細化 DLP：**透過情境感知偵測阻止 PII、原始程式碼、客戶資料等敏感資料外洩。
- **傳出電子郵件 DLP：**自動標記傳出電子郵件中的敏感性資料，防止意外資料洩露。
- **提示防護：**基於意圖（例如，越獄嘗試、程式碼濫用、PII 請求）偵測並封鎖有風險的 AI 提示和回應。

保障存取權與用戶端控制

- **保護應用程式存取：**在所有企業應用程式中強制執行 Zero Trust 網路存取 (ZTNA) 規則，例如，針對自主式 AI 連線進行精細的 DLP 掃描。
- **裝置狀態檢查：**根據精細化狀態檢查（例如，磁碟加密和啟用的端點 DLP）來控制存取權。
- **無用戶端控制：**套用瀏覽器型資料控制，以保障第三方存取權和員工 BYOD 原則。

影子 IT 與狀態風險

- **影子 IT 和 AI 探索：**探索並管理您環境中的影子 IT/AI。使用應用程式可信度分數和資料傳輸指標來量化風險，以便快速減少暴露風險。
- **狀態管理：**掃描 SaaS 應用程式和雲端環境以尋找狀態風險。採取規定措施，以補救安全調查結果。
- **租用戶控制：**封鎖 SaaS 應用程式的個人租用戶以防止資料外流。

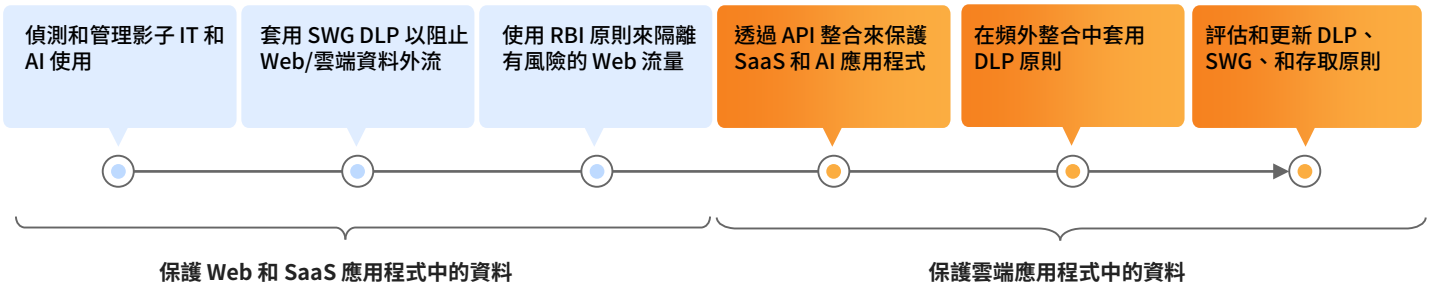
整合與報告

- **CASB 整合：**與領先的 SaaS 和 AI 平台（包括 Microsoft 365、Google Workspace 和 ChatGPT）無縫整合，以進行 API 型 CASB 掃描。
- **Microsoft MIP 整合：**與 Microsoft 資訊保護 (MIP) 標籤持續同步，以確保 DLP 原則持續一致。
- **可觀測性與取證：**將資料安全地記錄到您偏好的 SIEM 進行稽核，或透過儀表板或 API 即時地分析記錄。

範例資料防護旅程

首先，探索影子 IT 和 AI 使用，以便提升對攻擊面的可見度。在 SWG 上設定基礎 DLP 原則，以封鎖來自未受管雲端應用程式的高風險資料洩漏，並針對未經核准的 Web 流量部署遠端瀏覽器隔離。

然後，透過補救錯誤設定和強制執行內部共用原則，將 CASB 部署到經審核的安全 SaaS 和 AI 應用程式。在 SWG、電子郵件和 CASB 中優化與整合精細化的 DLP 和存取原則，以便在所有主要資料向量中實現自動化且統一的防護。



入門範例使用案例

- 針對所有未經核准的通訊和儲存通道，**即時阻止 PII/PHI外洩**。
- **保護原始程式碼和智慧財產權 (IP)** 免受內部人員竊取和未經授權的分發。
- 針對 GenAI 應用程式**強制執行提示防護政策**，以防止敏感性資料暴露和模型污染。
- **防止設定錯誤**，並在所有 SaaS 和 AI 應用程式中強制執行精細的存取控制。

客戶成果

EESTI RAUDTEE

基礎架構服務提供者
詳閱案例研究

緩解資料遺失與 SaaS 漏洞

藉由識別資料外洩與設定錯誤。

APPLIED

保險科技
詳閱案例研究

隔離如 ChatGPT 等公用 GenAI 工具

以阻止複製-貼上敏感性資料

Flo

領先的醫療應用程式
閱讀案例研究

保護患者資料

實現電子郵件安全性與 Zero Trust 的合規要求。

CREDIT SAISON INDIA

非銀行金融公司 (NBFC) 貸款人
詳閱案例研究

保護個人識別資訊並實現合規

防止不必要的資料輸出。

準備好討論您的資料保護需求了嗎？

申請研討會

1. 2025 年 Manage Engine 研究：來源
2. 2025 聯合國貿易和發展會議：來源