

探索員工使用影子 AI 和 IT 的情況

透過 Cloudflare 的流量檢查，擴展對未經批准的 AI 和 SaaS 工具的可見度

揭露隱藏的事物

影子 IT 並不是一個新問題，但未經核准的 AI 工具的快速採用正在引發一場現代危機：

- 2025 年，**20%** 的組織因影子 AI 安全事件而遭受資料外洩¹
- **85%** 的 IT 領導者表示，員工在 IT 部門未評估的情況下即採用 AI 工具²

Cloudflare 為組織恢復了可見度，使其能夠管理這個不斷擴大的攻擊面：

- **審核應用程式狀態**：將 AI 和 SaaS 應用程式分類為已核准、未核准或仍在審核中
- **根據應用程式狀態強制執行原則**：允許、封鎖、隔離、將 DLP 偵測套用至互動、限制檔案上傳等
- **分析應用程式使用情況**：監控綜合趨勢並執行精細調查
- **評估應用程式風險**：透過應用程式可信度分數評估可信度

運作方式

Cloudflare 的 SASE 平台內建於您的員工和資源之間，從而統一了可見度和控制。



此外，透過 API 整合 Cloudflare 的 CASB，以搜尋設定錯誤、使用者活動和敏感性資料。管理 AI 應用程式 (ChatGPT、Claude、Google Gemini) 和其他 SaaS 應用程式的安全狀態。將 CASB 與您的身分識別提供者搭配使用，以查看使用者何時對任何未經批准的第三方應用程式進行驗證。



影子 AI 的獨特風險

影子 AI 與傳統的影子 IT 不同。SaaS 應用程式主要用於儲存或共用檔案，而 AI 工具可轉換任何員工的輸入並從中學習。

這表示，敏感 IP、客戶資料或原始程式碼可能會被不可逆轉地吸收以用於模型訓練，且無法移除。

儀表板範例

基於以下因素篩選此應用程式使用情況的高層級概觀：

- 應用程式和應用程式類型
- 核准狀態
- 受 ZTNA 保護
- 使用者數量

如需更多詳細資料，請按一下任何 AI 應用程式的名稱，即可查看特定使用者或群組的存取情況、使用頻率、位置以及傳輸的資料量。

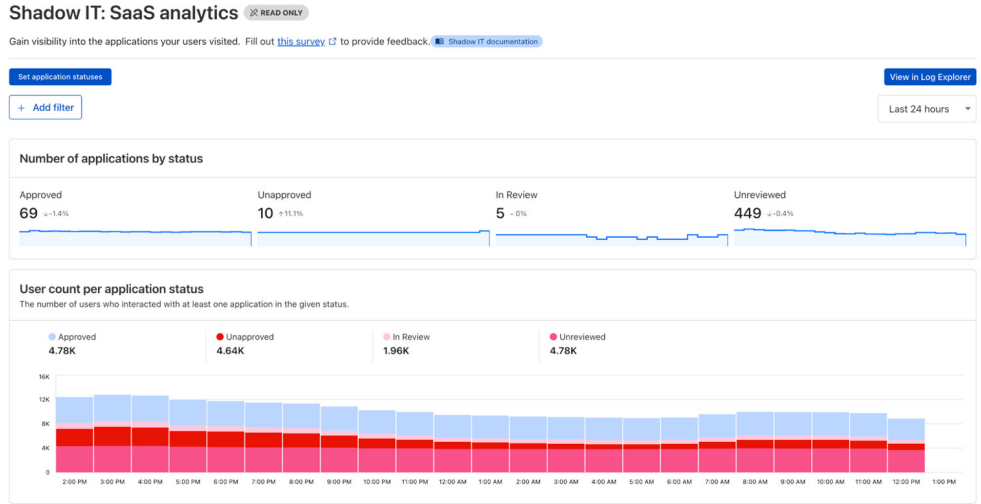


圖 1：影子 IT 分析儀表板

Applications Showing 1-20 of 533

Action	Category	Status	Users
Unreviewed (4 selected)			
In review (4 selected)	Platform (Do Not Inspect)	UNREVIEWED	4770
Unapproved (4 selected)	Productivity	UNREVIEWED	4762
Approved (4 selected)	File Sharing	UNREVIEWED	4750
<input type="checkbox"/> Google Search	Search Engines	UNREVIEWED	4729
<input type="checkbox"/> Gmail	Email	APPROVED	4708
<input type="checkbox"/> Google Play Store	File Sharing	UNREVIEWED	4707
<input type="checkbox"/> Google Chat	Collaboration & Online Meetings	APPROVED	4679
<input type="checkbox"/> Pinterest	Social Networking	UNAPPROVED	4638
<input type="checkbox"/> Google Calendar	Collaboration & Online Meetings	APPROVED	4574
<input checked="" type="checkbox"/> DigiCert	Productivity	UNREVIEWED	4553
<input type="checkbox"/> Google Meet	Collaboration & Online Meetings	APPROVED	4508
<input checked="" type="checkbox"/> Google Workspace	Productivity	UNREVIEWED	4346

根據核准狀態組織應用程式並設定存取原則：

- 已核准 (已批准)
- 未核准 (未批准)
- 檢閱中
- 未檢閱

需要更多技術指導嗎？藉助[此學習路徑](#)，了解如何建立原則。

圖 2：標記應用程式狀態

想要深入了解如何保障 AI 採用安全性嗎？

探索更多使用案例

申請研討會

1. 2025 年 IBM《資料外洩成本報告》：[來源](#)
2. 2025 年 Manage Engine 研究：[來源](#)