# 適用於資料保護的 Cloudflare One

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

### 現代資料風險需要現代安全性

如今，隨著資料數量、種類和速度呈爆炸式增長，組織面臨著由以下因素帶來的不斷升級的風險：

雲端和 SaaS 環境不斷擴大
↳ 包括局勢不明的新興 AI 工具，如 ChatGPT
↳ 導致寶貴的原始程式碼暴露

**Cloudflare One 的資料保護套件**旨在應對這些截然不同的現代風險。

透過將單點解決方案統一到單一平台和網路上，Cloudflare 提供的資料保護：

- **更有效：**簡化了連線和原則管理
- **更高效：**確保隨時隨地提供快速、可靠和一致的使用者體驗
- **更敏捷：**透過快速創新來滿足不斷變化的安全性要求


### 用於保護 Web、SaaS 和私人應用程式中資料的安全服務邊緣 (SSE)

在 SSE 旅程中逐步採用 Cloudflare，以便：

1. 使用 Zero Trust 確保資料存取安全
2. 阻止網路釣魚和勒索軟體等威脅
3. 偵測並封鎖最敏感的資訊

## 應對不斷升級的資料風險…

### SaaS 覆蓋區不斷蔓延

**82%**

的外洩涉及儲存在雲端環境中的資料。[1]

當然，資料外洩成本持續上升——過去三年，提高了 15%。[1]

### 多種多樣的新法規

**71%**

的國家/地區已經透過立法來保護資料和隱私。[2]

在美國，現在有 **11 個州**實施了全面的資料保護法，而在 2021 年僅有 3 個州。[3]

### 數位化轉型

**89%**

的 CISO 表示，快速推進數位化轉型舉措會為保護公司資料帶來不可預見的風險[4]

## 使用案例 1：保護開發人員程式碼

**問題**

程式碼可能會在許多開發人員工具中暴露或被盜，包括在公用存放庫等顯眼位置。

**解決方案**

掃描以尋找因設定錯誤而面臨程式碼洩露風險的公用存放庫（如 GitHub），並進行補救。偵測上傳/下載中的原始程式碼並套用控制。

→ GitHub

→ GitLab

→ Bitbucket

## 使用案例 2：資料暴露可見度和風險管理

→ OpenAI

→ Bard

→ GitHub Copilot

**問題**

資料遍佈於多種多樣的 SaaS 和雲端環境、未經批准的影子 IT 以及新興 AI 工具（如 ChatGPT）中，從而增加了洩露風險。

**解決方案**

透過針對敏感性資料的整合式 DLP 偵測，掃描 SaaS 套件以尋找設定錯誤。 瞭解未經批准的應用程式使用情況，然後允許、封鎖、隔離或套用 Zero Trust 控制以存取它們。

## 使用案例 3：遵守法規

**問題**

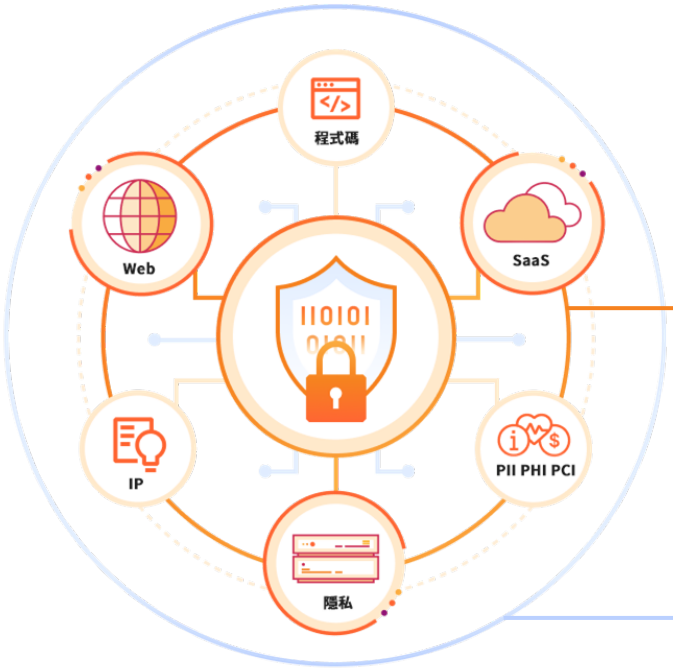
公司在確保資料安全和隱私方面面臨著更嚴格、更廣泛的法律要求，並且因不合規導致的罰款持續增加。

**解決方案**

識別受監管資料類別（PII、健康、財務）並對其套用控制。透過記錄和進一步的 SIEM 分析來維護詳細的稽核追蹤。藉助全面的 Zero Trust 安全狀態，減少攻擊面。

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ 等等！

# 運作方式




**一個統一的平台**

Cloudflare 將 DLP、CASB、ZTNA、SWG、RBI 和電子郵件安全服務中的可見度和控制匯集至單一平台，以簡化管理。

**一個可程式化的網路**

一個控制平面，其中的服務在我們自己的開發人員平台上構建，用於在所有執行點（Web、SaaS 或私人應用程式環境）對傳輸中、使用中以及待用資料實行控制。

# 採用組合式服務的控制範例

**對傳輸中的資料套用 DLP 並確保存取安全**

- 掃描流量和檔案中的敏感性資料，並使用 DLP 設定封鎖原則。
- 使用 CASB 探索和管理影子 IT。
- 使用 ZTNA 安全存取應用程式中的資料。
- 封鎖 SaaS 應用程式的個人租用戶以防止資料外流。

**隔離應用程式，以保護使用中的資料**

- 封鎖複製/貼上、上傳/下載、打印、鍵盤輸入——通通無需使用裝置用戶端。
- 無用戶端部署非常適合未受管理的裝置、第三方使用者以及 AI 工具（如 ChatGPT）。
- 在隔離的應用程式中套用 DLP 原則。

**保護 SaaS 應用程式中的待用資料**

- 掃描 SaaS 應用程式，尋找可疑的活動、設定錯誤和敏感性資料。
- 採取規定措施，以透過 SWG 原則糾正風險。

**整合以簡化合規性和控制**

- 推送記錄至慣用的 SIEM 以進行關聯和稽核。
- 與 18 個最熱門的 SaaS 套件整合，進行基於 API 的 CASB 掃描。
- 與用於 DLP 原則的 Microsoft 資訊保護 (MIP) 標籤持續同步。

# 藉助 Cloudflare 提供更好的資料保護

**透過減少複雜性*提高有效性***

透過多個靈活選項簡化連線，將流量傳送至 Cloudflare 進行執行。

對 SaaS 套件使用基於 API 的掃描或對 ZTNA 和 RBI 使用無用戶端模式，來保護應用程式存取。要轉寄代理流量，則會在安全服務中使用一個裝置用戶端或廣域網路入口。

**透過提升使用者體驗*提高工作效率***

我們的網路無處不在，確保了無論終端使用者和資料位於何處，都可透過在其附近進行單遍檢查來實行控制。

可靠且無干擾的終端使用者體驗意味著，實行資料控制絕不會中斷工作。經驗證，比 SSE 同行速度更快。

**透過快速創新*提升敏捷性***

我們的可程式化網路架構讓我們能夠快速構建新功能，因此，您可以靈活地應對新風險。

我們迅速採用全新的安全標準和通訊協定（如僅限 IPv6 連線或 HTTP/3 加密），以確保提供最新的資料保護服務。

# 客戶評價

「如今，Cloudflare One 可防止我們的使用者與 ChatGPT 和 Bard 等工具分享敏感性資料和程式碼，讓我們能夠安全地利用 AI… 展望未來，我們對 Cloudflare 持續不斷的資料保護創新充滿期待，尤其是他們對 DLP 和 CASB 等服務的願景和藍圖。」

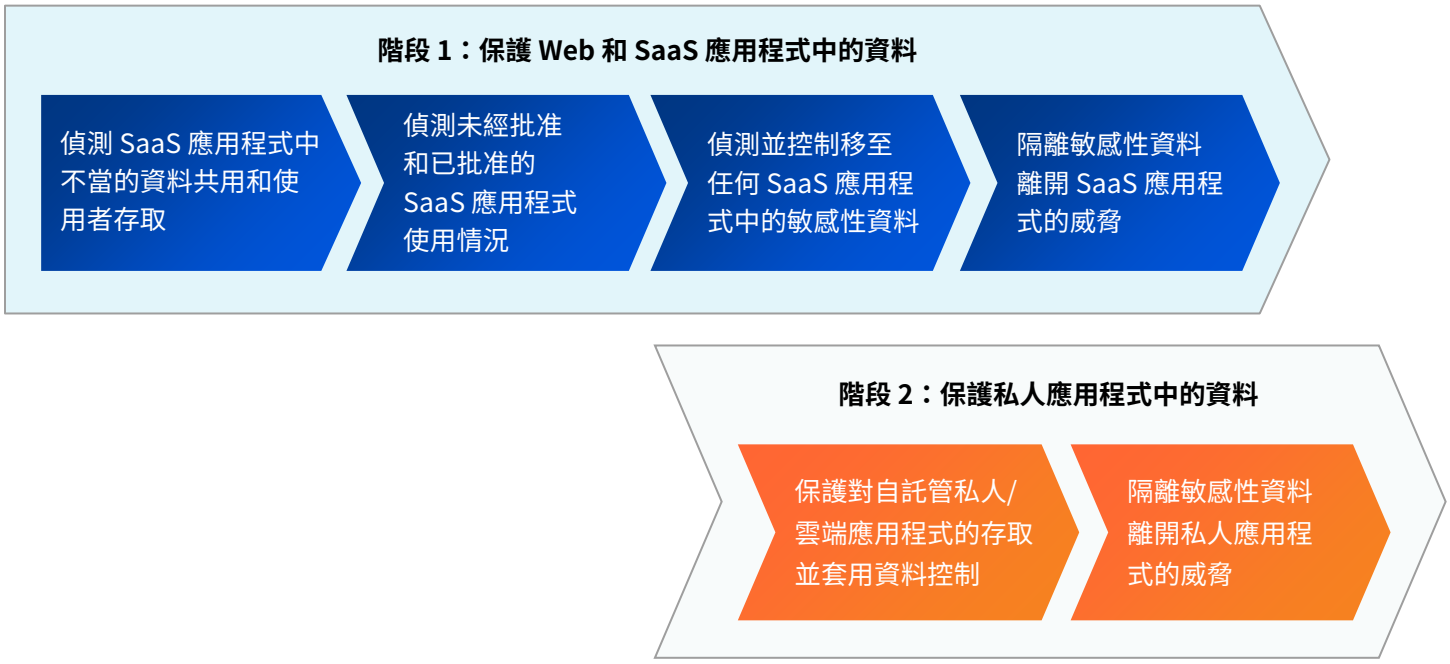
**Tanner Randolph**
資安長 (CISO)

**Applied Systems**
詳閱案例研究

**其他使用案例**

- **《財富》雜誌前 500 大天然氣公司：**用來保護承包商的資料存取
- **美國大型求職網站：**用來確保程式碼和個人資訊安全
- **美國地區航空公司：**用來降低暴露客戶資料的風險
- **澳大利亞醫療保健公司：**用來保護受監管的醫療資料
- **美國醫療裝置製造商：**用來簡化 HIPAA 合規性

## 常見的採用路徑




## 開始使用

### 瞭解…

不斷升級的資料風險，請參閱**此資訊圖**

### 參與…

平台的運作，請觀看**此示範**

### 驗證…

價值，請**申請諮詢式研討會**

1. 2023 年資料外洩成本報告，IBM
2. 聯合國貿易和發展會議
3. 國際隱私專業協會 (IAPP)
4. 2023 年《CISO 現狀》報告