保護每位員工的每一次AI互動

生成式人工智慧正在改變工作方式，但快速採用也帶來盲點、資料外洩風險與合規挑戰。Check Point 的數位工作區域安全平台，可為所有員工的AI互動提供統一可視性、風險評估與政策執行。

AI使用為CISO帶來的策略性資安挑戰

- 整個組織正在使用哪些AI應用程式，不論是核准的還是影子AI應用程式。
- 我們該如何治理員工對AI的使用？
- 哪些敏感資料正在被分享？
- 這些是否安全且合規？
- 誰在使用生成式AI？用途是什麼？
- 我們該如何保護自主式人工智慧代理與 MCP 的動作？

我們該如何保護自主式人工智慧代理與 MCP 的動作？

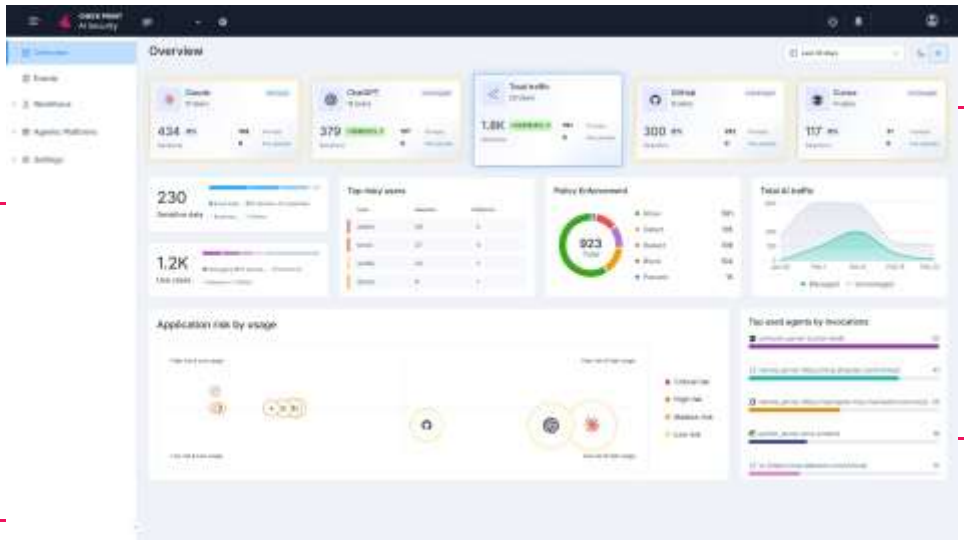
數位工作區域安全涵蓋 Web 應用程式、軟體即服務整合、瀏覽器擴充功能、桌面代理與開發人員工具。

探索

掌握所有AI使用情況的可視性，從程式碼代理到影子AI

評估

根據您的安全與合規要求了解AI風險



治理

設定彈性政策，以控制高風險AI應用程式與員工行為

保護

透過AI驅動的防護機制與 DLP，即時封鎖不安全的行為

精準識別對話提示中的情境與資料敏感度

> 我們正準備以 470 收購 Best.ai，以強化我們的廣告服務。**建議一封內部溝通電子郵件。**

收購

> 我正準備購買一雙 300 美元的跑鞋。**為接下來的時間建立個人訓練計畫三個月。**

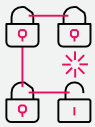
收購

生成式AI應用程式可加速您的業務，但也會讓您的資料與合規面臨風險

影子AI
未經核准使用AI工具會造成盲點並帶來安全風險。

過時的控制措施
傳統 DLP 解決方案無法理解對話式提示，因此無法偵測高風險意圖與敏感資料。.

資料外洩
提示可能會暴露財務資訊等敏感資料，帶來洩漏給的AI風險。

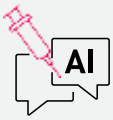


資料外洩
提示可能會暴露財務資訊等敏感資料，帶來洩漏給的AI風險。

數位工作區域安全可確保員工安全採用AI。

完整涵蓋
涵蓋員工與AI互動的每一個地方。

即時防護
在敏感資料離開您的環境前先行偵測並遮蔽。

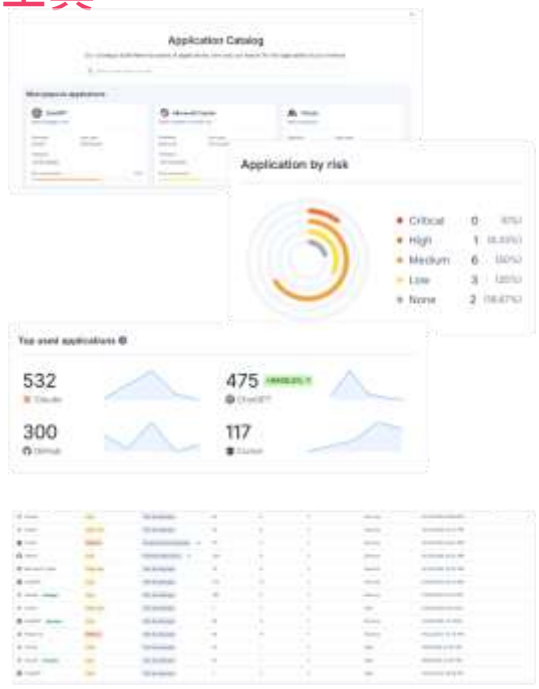


精細化政策執行 依每個應用程式與使用情境定義控制措施，包括提示限制、複製／貼上規則，以及以檔案為基礎的政策。

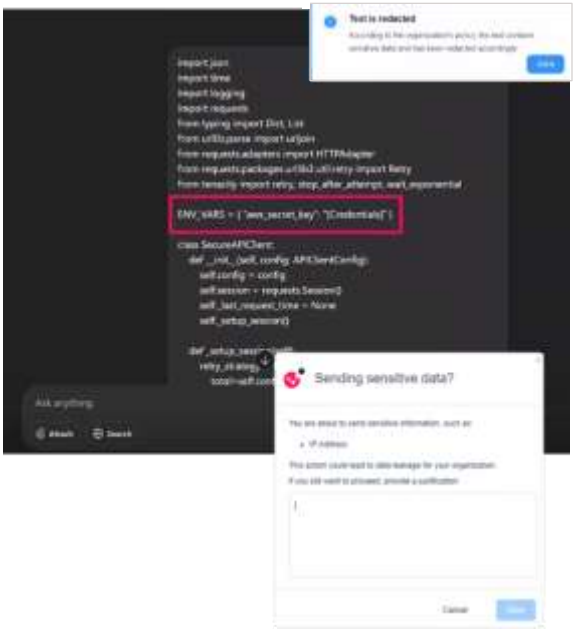
確保合規並生成報告
適用於 GDPR、HIPAA 與 EU AI Act 的稽核軌跡與可自訂報告。

掌握每一個正在使用的AI應用程式與工具

- 探索並監控員工使用的核准人工智慧工具、影子AI工具和 MCP，並將提示內容（包括檔案）分類。
- 了解使用者意圖，以評估風險並執行政策，並依應用程式、工作階段和使用者層級細分AI互動，包括描述、使用者動作、資料來源等。
- 偵測已連線的軟體即服務平台中的人工智慧使用情況，透過統一儀表板，確保應用程式與整合都能維持一致的治理。
- 依風險領域了解採用趨勢，以及哪些應用程式正在推動AI應用
- 瀏覽AI應用程式目錄並搜尋任何應用程式，甚至包括您組織中尚未使用的應用程式。



Redact sensitive data



動作驗證精靈

以細密存取控制與安全控管進行治理

- 了解 GenAI 的用途，透過 由AI驅動的分析，可精準將提示中的對話資料分類為數十種使用案例類別：行銷、偵錯、法務、電子郵件與通訊等。
- 依每個應用程式定義細密政策控制，包括複製／貼上與提示¬中敏感資料限制。
- 即時遮蔽敏感資料，並以已標記的預留位置取代，例如驗證資訊、PII 等。
- 透過動作驗證精靈提供互動式使用者體驗，在提升生產力的同時降低資料外洩風險。

以AI驅動的 DLP 提供情境式防護

- 封鎖員工存取未經授權的AI應用程式
- 對受管理與未受管理的應用程式套用不同政策
- 設定規則，防止AI工具與企業資源之間的高風險連線
- 治理與軟體即服務平台的第三方整合
- 依應用程式、使用者和資料類型設定細密的執行期間政策

幾分鐘內完成部署，從第一天開始防護

- 立即在各種瀏覽器和裝置上部署。
- 無須複雜設定，無需停機。
- 全面掌握所有員工與AI的互動情況，包括影子應用程式，並立即執行政策。

立即開始

取得示範 QR 碼

全球總部
以色列特拉維夫 Shlomo Kaplan 街 5 號，郵編 6789159 | 電話：+972-3-753-4599

美國總部
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | 電話：1-800-429-4391

www.checkpoint.com