GenAI 風險管理高階主管指南

生成式 AI (GenAI) 正在迅速實現企業的轉型，為創新和效率的提升提供前所未有的機會。從流程的簡化到開啟新的創造力途徑，無一不蘊藏著巨大無窮的潛力。但權力愈大，責任也就愈大。GenAI 的快速採用帶來全新的安全挑戰，讓所有企業都不得不積極面對。

我們在設計本指南時充分考慮您身為現代高階主管的需求。我們將深入探討 GenAI 帶來的獨特風險，為您提供清晰且可採取行動的架構來保護您的企業。我們將針對下列各項深入探討：

- **探索 AI 工具的形勢**：針對已獲批准 GenAI 工具的存取權限管理取得實用的建議，同時將未經批准的工具排除在您的網路之外。
- **找出關鍵風險領域並確定其優先順序**：了解您的弱點所在以及如何在其演變成威脅之前預先解決問題。
- **透過可行的步驟改善風險狀況**：了解如何針對 GenAI 獨特風險和需求量身打造並實施強大的安全措施。

在 Palo Alto Networks，我們每天都致力於解決 AI 安全最前線的挑戰、分享見解並制定策略，協助您在不影響安全性的情況下發揮 GenAI 的強大功能。只要遵循本指南，您就可以更有自信地帶領您的企業進入 AI 驅動的未來，並確信您的資產和數據均受到良好的保護。

生成式 AI 應用程式的形勢不斷演變

生成式 AI 正在快速發展，幾乎每天都會出現新的應用程式和使用案例。這種持續的創新對於企業管理及保護 GenAI 的方式帶來固有的複雜度。為了能在企業內更有效地採用及控制 GenAI 工具，您必須先了解這些應用程式的各種表現方式。以下是 GenAI 可採用的關鍵形式分析 (見圖 1)。

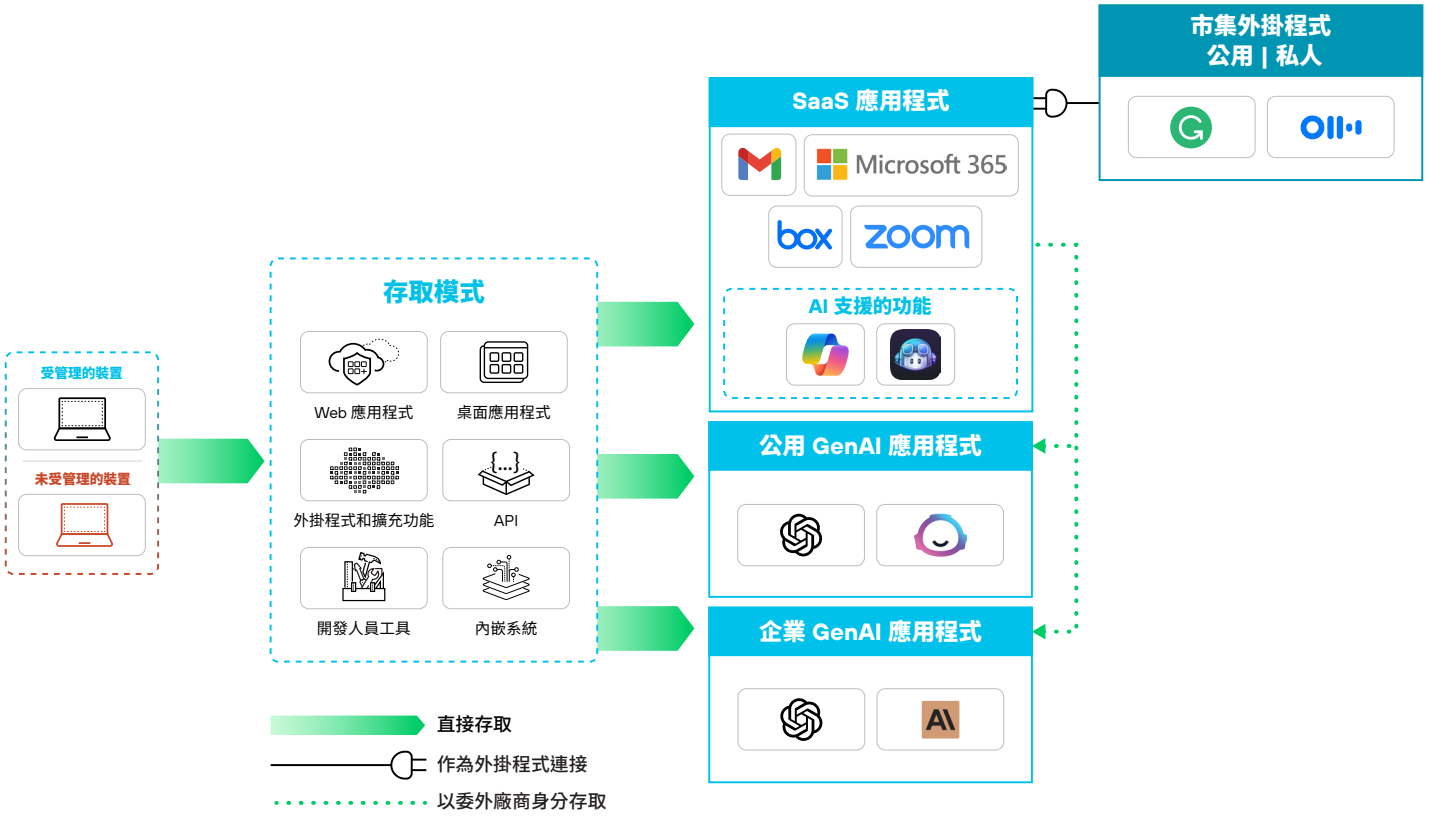

圖 1：使用者可以透過多種不同方式存取 GenAI 應用程式

公開可用的 GenAI 應用程式

GenAI 應用程式可以直接供一般大眾使用，無需任何中介平台。這些應用程式通常會以線上方式託管，任何能夠存取網際網路的人都可以使用。它們可以是公用消費者應用程式或企業應用程式。例如，OpenAI 的 ChatGPT 作為一種免費的 Web 應用程式，任何人都可以存取該應用程式來產生文字形式的回應。

市集 AI 外掛程式

GenAI 應用程式也可以作為外掛程式出現在各個市集中。公用和私人市集 AI 外掛程式正在改變企業營運以及與客戶互動的方式。雖然這些應用程式在效率和個人化方面帶來龐大的優勢，但利益相關者必須能駕馭複雜的互連 AI 生態系統。例如，許多 AI 外掛程式會跨越公司和個人瀏覽器設定檔運作，因而會產生額外的風險。

公用市集應用程式

公用市集應用程式是一種可透過主要 SaaS 平台的公用應用程式市集進行安裝的外掛程式。這些平台的所有使用者都可以看到並存取這一類的應用程式。例如，AI 外掛程式 People.ai (可在 Slack 應用程式目錄中找到) 可將電子郵件、會議和聯絡人等業務活動轉換為其 Slack 應用程式中的客戶機會管理。

私人市集應用程式

私人市集應用程式是透過應用程式市集散佈的外掛程式，但通常會基於安全或排他性等原因而僅開放給特定企業或使用者群組檢視或使用。例如，只有已獲得企業管理員批准的特定企業才能看見及存取 ServiceNow 商店中列出的自訂 ServiceNow AI 外掛程式。

直接整合

GenAI 應用程式還可以透過特定的驗證和連線方法直接整合至企業系統中，包括透過連接的應用程式和服務帳戶整合等方式。

連接的應用程式

連接的應用程式是透過用戶端 ID 和用戶端密碼進行驗證和整合的外掛程式。它們通常涉及產品和目標 SaaS 應用程式之間更加直接且 API 型的連線。例如，AI 驅動的分析工具會使用 OAuth 2.0 連線至 Salesforce，並透過用戶端 ID 和密碼來驗證及存取 Salesforce 數據以產生銷售相關見解。

服務帳戶整合

服務帳戶整合是利用服務帳戶進行整合的外掛程式，通常可提供更高層級的存取和控制，適用於更複雜或更敏感的整合。這可能是一個安全外掛程式，它使用 GitHub 應用程式或服務帳戶對程式碼儲存庫執行安全稽核並管理存取控制。

以原生方式內嵌於現有 SaaS 應用程式的 GenAI

GenAI 功能還能夠以原生方式內嵌於現有的 SaaS 應用程式中，從而增強這些平台的功能。其中包括 SaaS 應用程式中的全新 AI 支援服務和委外廠商。

全新的 AI 支援服務

SaaS 應用程式引入全新的 AI 支援服務，例如 AI 助理工具或 Copilot，提高了使用者的生產力和決策能力。Microsoft 365 Copilot 可以透過 Microsoft 365 應用程式提供 AI 驅動的寫作、數據分析和任務管理協助。

SaaS 應用程式中的委外廠商

GenAI 可作為 SaaS 應用程式中的委外廠商來處理特定任務或程序以提高效率和效能。例如，Zendesk 的 AI 客戶服務自動化功能可協助對於客戶詢問進行分類及回覆。

展望未來，我們預期最後每個應用程式都會原生融合一些 GenAI 組件。不久之後，GenAI 也將無縫整合到企業所依賴的幾乎所有應用程式中。這種轉變需要的不只是被動監控；更需要採取主動的可視性和控制方法。持續監控和策略管理將至關重要，因為這兩項因素將決定您是否能夠充分利用 GenAI 的能力並確保數據的安全無虞。若能提前因應這些變化，您就可以讓企業在不增加風險的情況下享有 GenAI 帶來的好處。

應用程式分類法

在 GenAI 的多樣化形勢中，並非所有應用程式都被賦予同等的價值。為了有效管理和保護這些工具，了解其所屬的不同類別至關重要。我們通常可以將應用程式分為三種不同的類型：已獲批准、已容許和未經批准，每種類型都有其獨特的特徵和安全意涵。了解此分類法將有助於量身打造您的風險管理策略，以更好地保護您的企業。

已獲批准的應用程式

已獲批准的應用程式是企業正式批准使用的軟體服務，通常由 IT 部門負責管理。這些應用程式因能帶來商業利益而受到認可，並已通過嚴格的安全審查。例如，大型金融機構可能會批准使用 OpenAI 的 ChatGPT Enterprise 來生成文字內容並自動化客戶服務互動。

已容許的應用程式

已容許的 SaaS 應用程式係指企業因合法業務需求而允許使用的程式，儘管 IT 部門未正式提供或進行管理。這些應用程式可能會受到某些限制以減輕其在使用上的風險，因為它們不符合與已獲批准之應用程式相同的安全和合規性標準。例如，高科技公司可能會允許其行銷團隊使用 Jasper，但僅限於創作行銷材料和社群媒體內容，並且必須遵守嚴格的數據使用和處理準則。

未經批准的應用程式

未經批准的應用程式未經過正式批准，可能會帶來安全風險或合規性問題。在未經正式批准的情況下使用這些應用程式往往會帶來重大的安全風險。例如，汽車公司的員工可能會使用免費的線上 AI 寫作助理來撰寫敏感的商業文件，儘管 IT 部門未正式批准或允許使用這些應用程式。

主要風險領域：如同一把雙面刃的 GenAI

想像一下：一家繁忙的現代企業，充滿對於 GenAI 的興奮之情。各部門的員工都在積極採用這些創新工具來簡化工作流程、提高生產力並激發創意潛力。這種能量是具有感染力的，其所帶來的益處無庸置疑。但正如我們所探討的，GenAI 不僅僅是一個強大的盟友，其更像是一把雙面刃。在這種熱情的背後隱藏著一個複雜的風險網絡，IT 和資安團隊必須謹慎因應以確保企業的安全無虞。

圖 2：雖然 GenAI 可以大幅提高生產力，卻也存在著風險

無形威脅：缺乏可視性

在行銷部門，一位創意實習生發現一個免費的線上 AI 寫作助理。這名實習生對其能在幾秒鐘內生成吸引人的標語感到非常興奮，並開始每天使用它。然而，他們並未意識到自己正無意中將公司的敏感數據上傳到一個未經批准的第三方應用程式。由於 IT 團隊缺乏對於這種「影子 AI」的可視性，因此對於數據洩漏的情況毫不知情。

存取困境：薄弱的控制力

同時，在研發部門，某個團隊正利用強大的 AI 分析工具來處理多年的實驗數據。雖然這些見解具有開創性，但整個部門的存取並未受到限制，這代表著即使是資歷較淺的成員也可能會接觸並誤用機密的研究成果。由於缺乏基於角色的精細存取控制，這種創新工具反而成為安全方面的隱憂。

缺乏培訓：惡意內容

客服代表對於他們的新型 AI 支援聊天機器人感到非常滿意，因為其大幅縮短回應時間。然而，IT 團隊發現聊天機器人偶爾會在其回應中包含潛在的惡意連結，對員工和客戶構成一定的風險。因此，檢查 AI 回應中的惡意軟體、網路釣魚連結和惡意內容，以及訓練使用者在點擊連結時保持警覺等各方面的挑戰就變得更為明顯。

外掛程式困境：藏而不露的風險

銷售團隊對於他們 CRM 系統中的一個全新 AI 外掛程式讚譽有加，因為其能夠以驚人的準確性預測客戶行為。隨著其受歡迎的程度日益增長，IT 團隊在各種 SaaS 市集中越來越難以維持對其數據存取的可視性和控制。這種外掛程式管理上的盲點可能會造成潛在的弱點。

靜態數據：難以察覺的積累

隨著 GenAI 應用程式在整個企業中不斷激增，敏感數據也開始在這些工具中累積，甚至可能被用來訓練其 AI 模型。IT 團隊意識到他們對於這些應用程式所儲存的數據及其位置的可視性有限，因此可能會引發合規性問題和數據暴露風險。在此同時，網路罪犯會試圖存取外洩的程式碼或敏感數據，因為這些現在都已經是 LLM 訓練數據集的一部分。

生產力悖論

為了鎖定這項新發現的安全威脅，IT 團隊在整個企業施行嚴格的控制措施。但或許是過於積極，他們無意中封鎖對於已容許之 GenAI 應用程式的存取。一開始出自善意的舉措很快就適得其反，不僅讓員工感到沮喪，生產力也跟著下滑。

當企業領導團隊在面對這些挑戰時，他們意識到光是採用新工具並不足以駕馭 GenAI 的力量。他們需要一種全面的風險管理策略來解決可視性、存取控制、數據保護和持續監控等問題。只有在了解並緩解這些風險後，企業才能真正發揮 GenAI 的變革潛力，同時保護其最有價值的資產：數據。

風險狀況評估

如果您對於我們探討的情境感到非常熟悉，那麼您並不孤單。因為許多企業在將 GenAI 整合到其營運時都發現自己正面臨著類似的挑戰。為了有效管理這些風險，對於企業整體風險狀況進行全面的評估至關重要。此評估應考量幾項關鍵因素，以確保您能夠制定強有力的安全策略，同時考慮不斷變化的威脅形勢。

安全最佳實務

評估您的 GenAI 應用程式安全控制是否符合業界最佳實務。這包括實施強大的存取控制、數據遺失防護、市集和外掛程式可視性、SaaS 安全狀況管理和靜態數據保護。

主動流量分析

了解企業內部 GenAI 應用程式活躍流量的性質和特徵。對於 GenAI 應用程式使用者存取以及在這些環境中處理或儲存的數據類型進行全面的風險分析。

對於安全採用 GenAI 的建議

為了協助您的企業因應此一複雜的形勢，我們概要說明一系列可行的建議。這些步驟的目的在於提供一種平衡的方法，確保您的企業可以充分利用 GenAI 功能，同時保持強大的安全狀況。

監控 GenAI 應用程式、使用情況和數據流

設定影子 AI 探索服務以擷取並分析整個網路中的所有 GenAI 應用程式使用情況和數據流：

- 對整個企業的 GenAI 使用情況進行全面的清查，並檢查使用分析和防火牆日誌。
- 根據 AI 特定屬性 (例如數據敏感度、使用者基礎、輸入/輸出模式以及基於合規性的屬性) 評估每個 GenAI 應用程式的風險狀況。

應用程式分類

對 GenAI 應用程式實施分類系統，將它們分為三個不同的群組：

- **已獲批准**：正式批准在企業範圍內使用
- **已容許**：允許但有所限制
- **未經批准**：未獲準使用

這種分類方式可以為每個類別提供量身打造的可視性和控制措施，確保 GenAI 的採用能達到平衡。

實施精細的存取控制

專為 GenAI 應用程式建立詳細的存取控制以增強安全性：

- 為已獲批准、已容許和未經批准的 GenAI 應用程式分別制定不同的政策。
- 根據零信任原則封鎖未經批准的應用程式。
- 根據業務需求，限制只有特定員工才能存取已容許的應用程式。
- 定期審查和更新存取政策以反映不斷變化的業務需求和風險評估。

增強數據檢查和 DLP 能力

實施全面的數據遺失防護 (DLP) 措施：

- 監控和檢查流出至 GenAI 應用程式的數據以防止數據外洩。
- 設定政策來解密和檢查流向 GenAI 應用程式的數據。
- 根據數據敏感度等級實施控制。
- 定期更新 DLP 規則以解決新興威脅和新數據類型。

實施持續風險監控

建立持續的安全和合規性程序：

- 對 GenAI 應用程式使用情況和數據流實施持續監控。
- 定期進行風險評估以識別新的威脅或弱點。
- 使用自動化工具對潛在的安全漏洞或政策違規行為發出警示。

提供員工培訓

制定培訓計劃以教育員工如何更安全且負責任地使用 GenAI：

- 透過電子郵件、簡訊或聊天訊息部署使用者指導或通知警示，以教育員工或引導其使用已獲批准的 GenAI 應用程式。
- 教育員工如何更加安全且更有效率地使用 GenAI 應用程式。
- 引導使用者了解有關數據敏感度、可接受的使用政策和潛在風險的指南。
- 提供定期更新和進修課程，以因應新的 GenAI 應用程式，並通知員工各種以 AI 為基礎的新興威脅。

確保 GenAI 外掛程式的可視性和控制

擴展安全措施以納入 GenAI 市集、外掛程式和 AI 機器人：

- 實現跨多個市集的外掛程式可視性。
- 偵測作為外掛程式使用的 GenAI 應用程式，即使您封鎖對於父系應用程式的直接存取，該應用程式也可能會存取數據。
- 實施審查程序來管理外掛程式使用和數據存取。
- 識別、監控和補救未經授權的 AI 機器人。

建立全面的靜態數據掃描

對 GenAI 應用程式進行徹底的靜態數據探索掃描：

- 偵測存在於 GenAI 應用程式中的任何敏感靜態數據。
- 識別潛在的外部敏感數據暴露風險。
- 對任何未經授權的數據儲存或暴露實施補救措施。

衡量 GenAI 安全性的成功率

成功的 GenAI 安全性需要在降低風險的同時實現創新和生產力。為了確保您的 GenAI 安全策略能達到目標，請務必注意接下來的各項關鍵指標。

生產力提升與創新

GenAI 應用程式可以提高企業組織內的生產力並促進創新。採用這些應用程式有助於簡化營運、自動執行重複性任務並增強人類創造力，進而為各項業務帶來龐大的收益。開始衡量其生產力的提升，無論是員工生產力、服務票證的減少、節省的時間或客戶服務的改善。

已獲批准的 GenAI 應用程式採用率

透過 GenAI 的採用，企業不僅可以提高生產力，還可以建立一支更具活力且更負責任的員工隊伍，最後推動業務成長和成功。開始追蹤積極使用已獲批准之 GenAI 工具的員工百分比。高採用率表示安全 GenAI 工具的成功啟用和使用者滿意度。

員工滿意度與能力強化

進行調查以評估員工對可用 GenAI 工具的滿意度並衡量他們感受到的能力提升。GenAI 應用程式能讓互動更為個性化並為員工提供即時支援，從而增強他們的整體體驗。正面的意見回應將帶來更高的工作滿意度和留任率，因為其感受到自己在職位上的表現獲得支持因此更為投入。

減少影子 AI 的使用

由於整個企業的員工逐漸轉向已獲批准的工具，因而監控未經批准之 GenAI 應用程式使用量減少的情況。減少影子 AI 和未經批准的應用程式，對於大幅減少數據洩露和敏感數據暴露的可能性至關重要。如果使用未經批准的 AI 應用程式而導致未遵循法規要求，企業可能會面臨法律處罰、補救措施和名譽損害。此指標展現了 GenAI 啟用策略的有效性。

數據保護有效性

監控 GenAI 使用相關數據暴露事件的減少情況。員工可能會無意中將機密數據輸入 GenAI 工具，進而增加數據洩露和未經授權存取專屬資訊的風險。數據安全事件的持續下降凸顯了數據安全通訊協定及其正確實施的好處。

確保 AI 的未來安全無虞，刻不容緩

隨著 GenAI 不斷重塑商業形勢，精心設計完善的風險管理架構顯得格外重要。若能遵循本指南摘要列出的策略，您的企業就可以充分利用 GenAI 的潛能，同時防範其固有風險。這趟旅程的成功與否取決於持續的警覺性、適應能力以及對於安全且負責任地使用 AI 的積極承諾。透過正確的方法，您就可以更有自信地帶領您的企業進入 AI 驅動的未來。

深入了解有關 Palo Alto Networks AI Access Security 的詳細資訊，這是一款專為特定目的打造的解決方案，旨在達到 GenAI 應用程式的安全採用和使用。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號 6F-1

prisma_c-suite-guide-to-gen-ai-risk-management_092524