生成式 AI 對企業安全的影響

2023 年 7 月 4 日發布｜4 分鐘閱讀

Alex Au Yeung
賽門鐵克產品總監
(CPO:Chief Product Officer)

生成式 AI 的崛起

生成式 AI 迅速改變世界對人工智慧可能性的看法，對於許多不從事科技行業的人來說，它的主流應用可能會讓他們感到震驚。它既能讓人敬畏，也能引起不安，而且經常是兩者同時存在。

那麼，它對企業和網路安全有什麼影響呢？

科技的轉折點

生成式 AI 運行在以深度學習系統為基礎的神經網路上，像大腦的工作方式一樣。這些系統像人類學習的過程。但與人類學習不同的是，透過群眾外包資料的力量與正確的資訊相結合，意味著生成式 AI 處理答案將快得多。一個人可能需要 30 年時間來處理的事情，AI 可能只需要一瞬間就能完成。這是一種可以根據輸入資料品質以及數量而獲得的好處。

它在工程和科學方面改變企業的遊戲規則。這是一種可以大大提高組織效率的技術--讓他們在相同的人力資源下大幅提高生產力。但是，ChatGPT、Bard 和 GitHub Copilot 等生成式 AI 應用程式的出現速度之快，似乎就在一夜之間，這讓企業 IT 領導者大吃一驚，這是可以理解。其速度如此之快，以至於在短短六個月內，生成式 AI 工具的普及已經達到技術的轉折點。

網路安全的挑戰

包括 ChatGPT 在內的生成式 AI 主要是通過第三方的軟體即服務 (SaaS) 模式來提供。這帶來的挑戰之一是，與生成式 AI 互動需要向這個第三方提供數據。支持這些 AI 工具的大型語言模型 (LLMs) 則需要存儲該數據，才能聰明地回應後續的提示。

AI 的使用帶來敏感性資料丟失和合規性的重大問題。向生成式 AI 程序提供敏感性資訊時，例如：個人身份識別資料 (PII)、受保護的健康資訊 (PHI) 或智慧財產 (IP) 等，需要與其他資料處理器和資料控制器的關係一視同仁。因此，必須有適當的控制措施。

輸入到像 ChatGPT 等 AI 工具中的資訊會成為其知識庫的一部分。任何訂閱 ChatGPT 的人都可以存取該公共數據庫。這意味著任何上傳的數據或問過的問題，都可以在特定的應用程式保護範圍內被回放給提出相似問題的第三者。值得注意的是，這與軟體即服務 (SaaS) 應用程式的問題非常相似，因為當它被用作訓練集時，會影響未來查詢的回應。就目前而言，大多數生成

式 AI 工具對用戶提供的數據並沒有具體的資料安全政策。

內部威脅也隨著 AI 的出現變得重要。熟知企業的內部人員可以使用 ChatGPT 建立非常真實的電子郵件。他們可以複製其他人的風格，錯誤，所有的東西。此外，攻擊者也可以完全複製網站。

企業需要什麼安全措施

幸運的是有生成式 AI 防護解決方案，例如：Symantec DLP Cloud、Symantec Endpoint Security Complete (SESC) 上的調適型防護和電子郵件的即時連結追蹤功能，可以解決這些新興的挑戰並以不同、有針對性的方式阻擋攻擊。

Symantec DLP Cloud 為企業擴展對生成式 AI 的防護，使企業能夠發現，並隨後監控和控制組織內部與生成式 AI 工具的互動。除了底下將提及的好處之外，DLP 還可以使用 AI 來加速判斷事件的優先級別，幫助資深分析師分類最重要的事件，並識別那些對企業不構成關鍵威脅的事件。

這些好處包括：

- 提供企業瞭解使用生成式AI工具所面臨的風險
- 提供必要的保護措施，允許安全可靠的使用流行的AI工具，阻止敏感性資料被有意或無意地上傳或發布
- 識別、分類和記錄PHI、PII和其他關鍵數據的合規性

整體而言：Symantec 生成式 AI 防護允許企業在不影響資料安全性和合規性的情況下，對使用生成式 AI 提高生產力的創新，說『Yes』。

了解更多

如欲了解更多關於生成式 AI 對企業的影響，請參閱我們最近的白皮書：

人工智慧 (AI)、自動化以及網路安全

原廠網址：https://www.broadcom.com/blog/implications-of-generative-ai-for-enterprise-security

關於作者

Alex Au Yeung

賽門鐵克產品總監 (CPO:Chief Product Officer)

Alex Au Yeung 是賽門鐵克產品總監 (CPO：Chief Product Officer) 在軟體產業超過 25 年的資歷。擔負所有賽門鐵克產品策略、管理以及行銷的重責大任。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。