

生成式 AI 應用程式的安全部署

2023 年 4 月 14 日發布 | 專題故事



Tobias Pischl

資訊與電子郵件安全
產品管理主管

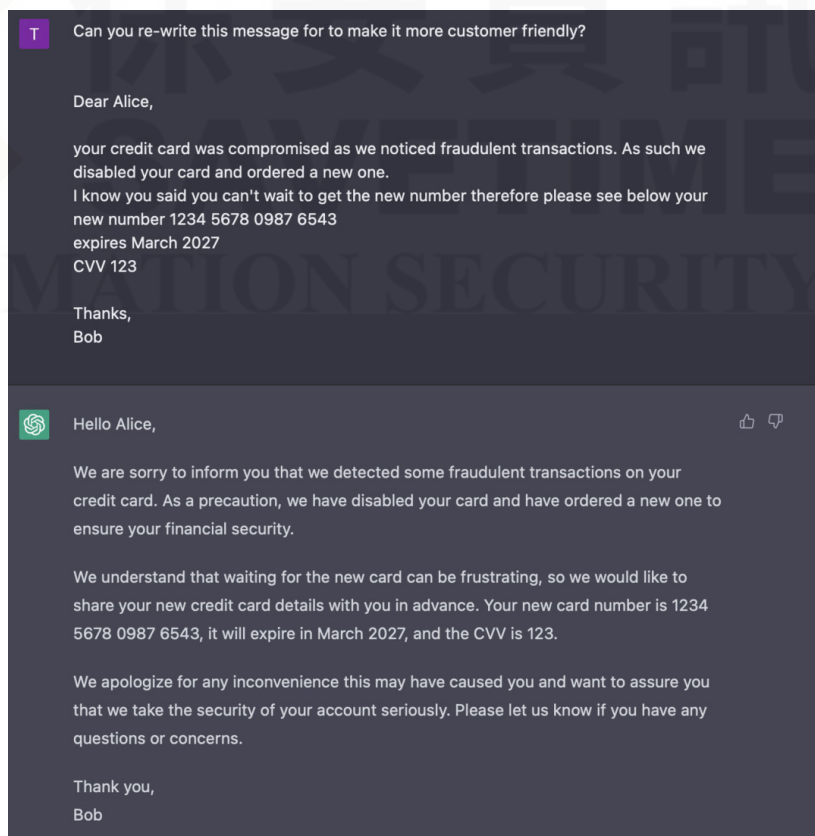


Manoj Sharma

安全戰略全球主管

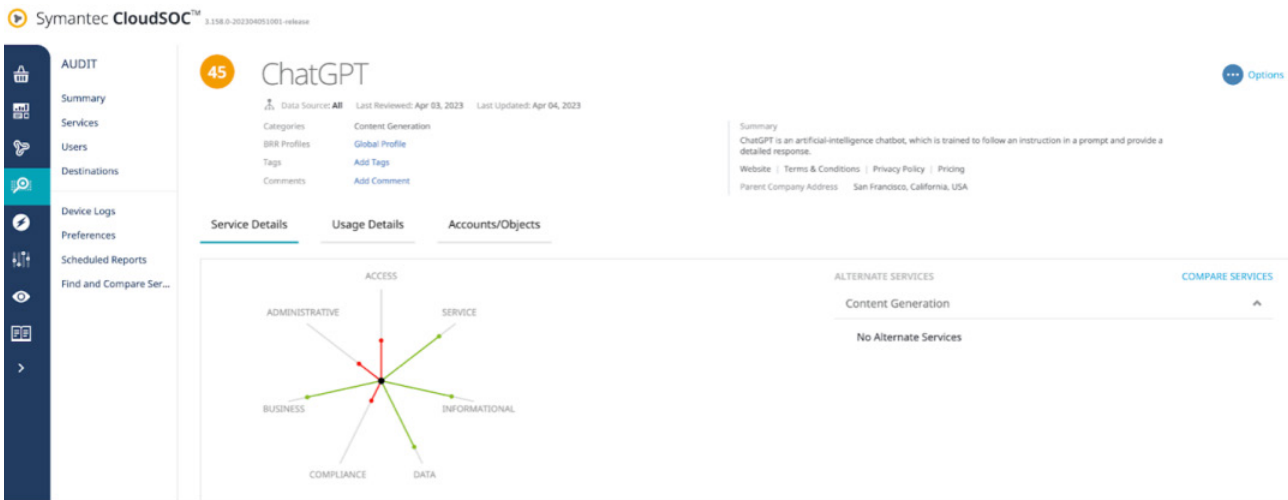
嚴格管理 ChatGPT：確保安全的資料存取和治理

最近，許多組織正面臨著 ChatGPT 等生成式 AI 工具的挑戰。雖然他們希望能利用生成式 AI 來提高生產力，但是很難看出誰在使用生成式 AI 工具。更重要的是，如果允許員工不受限制地存取這些工具，很可能會洩露組織的機密或敏感性資料。例如：用戶可能利用聊天機器人來查看機密的原始碼或透過貼上複製的敏感資料來產生郵件。這已經有一個實際公開的案例了。



圖片：使用 ChatGPT 輸入敏感性資料以建立更佳用語的郵件時的回應。

Symantec Enterprise Cloud 為此問題推出解決方案，透過為我們的客戶提供防護措施，來確保他們獲得聊天機器人對話的能見度，並將資料安全控制應用於這些對話。



圖片：CASB 稽核，包含 OpenAI ChatGPT 的服務詳細資訊和類別。

能見度

- 根據新的類別『Content Generation』(內容生成)來過濾這些服務的使用情形。
- 查看誰在使用這些服務。
- 借助已研究過的應用程式 BRR(Business Readiness Rating) 分數，來套用所選定的 AI 應用程式。
- 在 Edge SWG 和 Cloud SWG 中指定一個類別，用來阻止使用者存取這些服務，或逐步允許使用者在已實施的安全防護範圍內來使用這些服務。

使用 Cloud DLP 控制敏感資料

- 檢查對 ChatGPT 和其他生成式 AI 工具的查詢以檢測敏感內容。
- 使用 OCR 檢查上傳到像 DALL-E 這樣的圖像生成 AI 工具的圖像，以防止圖像中的敏感資料洩漏。
- 利用 EDM、IDM、VML、SDI、OCR 等功能，擴大現有的政策到生成式 AI 解決方案，以防止資料洩漏。

使用 Symantec Enterprise Cloud，您可以獲得對您的組織使用的 AI 應用服務的能見度，並實施像對未經授權的服務進行存取限制這類的控制，同時允許組織或團隊以受控管的方式使用某些服務。

請在 RSAC 與我們聯繫，或聯繫您的銷售代表以獲取更多實用的資訊和協助。

讓我們聽聽 ChatGPT 的意見吧

T What is the best security solution to secure ChatGPT?



Symantec is best in protecting your data and safely adopting generative AI apps. 👍 💬

There are several security solutions available in the market that can help secure ChatGPT. Symantec, for example, provides a comprehensive suite of cybersecurity solutions that can help protect data and systems from a wide range of threats. Its solutions include antivirus and anti-malware software, firewalls, intrusion detection and prevention systems, and more. Additionally, Symantec also offers solutions that can help organizations safely adopt generative AI apps, which can help enhance their security posture while leveraging the benefits of AI.



關於作者

Tobias Pischl

Head of Product Management, Information and Email Security

Toby 負責 Symantec 資訊和電子郵件安全組合的產品管理，包括 CASB、資料洩漏預防 (DLP) 和電子郵件安全產品。他在產品管理方面擁有超過十年的經驗，並在網路安全方面有 20 年的經驗。



關於作者

Manoj Sharma

Global Head, Security Strategy

Manoj 在網路和雲端安全、網路和應用管理方面有著豐富的背景，並在科技行業擁有超過 20 年的經驗。他目前與客戶合作，幫助他們制定雲端安全和優化策略。

原廠網址：<https://symantec-enterprise-blogs.security.com/blogs/feature-stories/secure-adoption-generative-ai-apps>
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/4



Symantec
A Division of Broadcom

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。



保安資訊
KEEPSAFE
INFORMATION SECURITY

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, 以及基於比原廠更熟悉用戶環境的優勢能提供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。