賽門鐵克人工智慧 (SymantecAI)：現在由 Google Vertex 人工智慧 (Google Vertex AI) 提供更豐富的功能

2023 年 9 月 21 日發布｜賽門鐵克與人工智慧

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

新的合作夥伴關係簡化並精簡了企業安全

生成式人工智慧 (Generative AI) 使社會對新的業務能力產生覺醒，這是 IT 行業以外的人很少能想像到。更重要的是，人工智慧 (AI) 技術的加速應用和使用案例正在激勵 IT 團隊推動下一步的發展。無論這些團隊是剛剛接觸人工智慧，還是像賽門鐵克團隊那樣早在十多年前就開始將人工智慧和機器學習 (ML) 融入到解決方案中，現在正是導入人工智慧技術進行創新和拉升價值的激勵人心的時刻。

雖然生成式人工智慧是令人興奮，但網路安全專業人員始終必須保持專注於消除威脅和保護資料的基本原則。當安全技術發生變化時，他們知道今天與供應商建立的合作關係將在未來長期影響他們的安全。他們需要確保別人不會產生出更好的誘捕技術，使得他們的決策看起來很糟糕。因此，他們迫切希望知道他們的安全合作夥伴能深入瞭解人工智慧技術，並且有計劃充分利用其潛力來創建安全解決方案。光有成功創新的悠久歷史還不夠，他們還想知道『下一步是什麼』？

博通轄下的企業安全部門--賽門鐵克為 SymantecAI 引入新功能--我們以人工智慧技術為動力的進階安全解決方案組合。利用我們與 Google Cloud 團隊的緊密合作關係，SymantecAI 利用 GoogleVertex AI 的強大功能，這是一個機器學習平臺，極大地擴展賽門鐵克人工智慧安全產品組合。通過與 Google 的合作，最好的人工智慧與最好的安全智慧和控制相結合。嶄新的新功能將大大提升我們客戶--企業網路安全專業人員的工作效益與效率。威脅獵手團隊將獲得攻擊預測能力和可採取行動的建議。網路團隊可以利用資料來優化零信任網路存取 (ZTNA) 解決方案的部署。安全管理員可以快速編寫更好的政策規則。每個人都將受益於更快地存取操作、研究和故障排除所需的特定內容。

新的安全使用案例

SymantecAI 是一套加持了人工智慧技術做為動力，先進的安全和生產力解決方案，透過簡化分析和矯正威脅、確保更好的資料保護和精簡安全操作來提高安全性。採用這些功能的客戶將在各種安全使用情境中獲得明顯而實際的效益：

- **安全回應團隊**將快速獲得針對選定內容的詳細威脅描述、指令檔分析和二進位檔案分析。
- **威脅獵手**團隊將更好地預測下一個攻擊鏈步驟，獲得快速事件摘要和適應性功能的前瞻性指導。

- **網路團隊**將看到其安全網頁閘道的內容策略語言 (CPL) 策略摘要，同時獲得撰寫或最佳化規則的協助，同時享受自然語言介面的報告。
- **電子郵件安全**將利用賽門鐵克人工智慧 (SymantecAI) 來提高效率，使用人工智慧進行調整，並利用它對提交的資訊進行更快、更強的分析。
- **網頁隔離**將啟用腳本分析，以瞭解下載的腳本是否是惡意的，並為客戶提供可操作的見解。
- 根據 VPN 日誌、Layer3 日誌、ldP／Active Directory 的組織結構提供模型化建議，**零信任網路存取 (ZTNA)** 將可獲得更快的部署效益。
- **端點客戶**將有一個人工智慧助手來總結、優先處理事件和事件。賽門鐵克 AI 還將幫助他們檢測有問題的政策規則。
- **DLP創新實驗室**將使用 AI／ML 進行資料分類，例如：原始程式碼、稅務、法律和金融文件，以便更好地進行開箱即用的資料分類。
- 賽門鐵克 AI 將增強**雲端存取安全性代理程式 (CASB)**，以檢測安全狀況問題並提出修復建議，同時自動生成 Gatelet。
- **賽門鐵克企業雲端平臺**可從產品控制台與技術知識互動式 AI 聊天機器人協作。引述的來源資料來源包括技術文件、使用手冊、知識庫等。

以上只是我們持續致力於解決方案嵌入人工智慧技術的精簡清單。

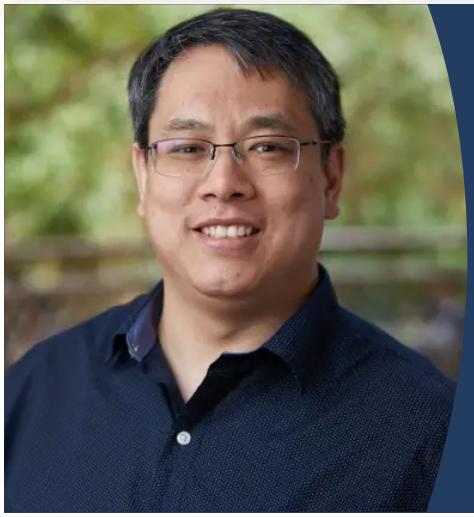
我們與 Google Cloud's Vertex AI 平臺的夥伴關係

賽門鐵克與Google Cloud 團隊建立長遠且成功的合作關係，雙方的工程師一起開展大量工作，在賽門鐵克用於存儲安全事件和事故的所有工作模式和格式上訓練網路安全專用大型語言模型 (稱為 SecPaLM 2)，而不會暴露實際事件或客戶資料。這使我們能夠在賽門鐵克產品中提供新的功能，自動、快速地分析和描述客戶安全事件的影響，並提出具體的修復步驟，所有這些都以簡單易懂的語言來溝通。

與 Google Cloud 的合作有助於賽門鐵克 AI 提供一套全新的生成式人工智慧工具，幫助威脅獵手團隊更迅速且正確地地分析客戶提交的可疑檔案。由於這些工具可以快速確定檔案是乾淨的還是惡意的，並詳盡說明該檔 (包括指令檔和二進位檔案) 的具體功能，因此團隊資源的效率將大大提高，對威脅的反應速度也將大大加快。這提高了我們每天為企業客戶提供的客制化威脅分析的速度和準確性。

賽門鐵克 AI 建立在悠久的創新歷史基礎之上，我們的開發團隊不僅對可能實現的目標有著深刻的理解，而且還具備以安全有效的方式將其付諸實施的遠見、技術和經驗，這一點值得我們的客戶放心。這就是著眼於未來的企業選擇賽門鐵克的原因。要瞭解更多資訊，請參閱賽門鐵克立場文件：人工智慧、自動化和網路安全。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/symantec-and-ai/symantecai-now-enriched-google-vertex-ai



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**。