白皮書

人工智慧 (AI)、自動化以及網路安全

令人憂心忡忡也帶來機會無窮：博通・賽門鐵克的觀點

白皮書

人工智慧 (AI)、自動化以及網路安全

瞬間席捲全球的 ChatGPT 令全世界大吃一驚。它會引發生存威脅，還是下一次偉大科學革命的先兆？博通公司提出了自己的觀點。

目錄

簡介

人工智慧(AI)的概念早已存在於我們大家集體想像之中。幾乎在所有的傳說、民間故事和流行文化中，它都被認為是把雙刃劍。

因此，人工智慧是一個既令人驚奇又令人不安的話題也就不足為奇了。這一點現在尤為重要，因為 ChatGPT、Bard 和其他生成式人工智慧技術的出現突然改變人工智慧應用普及化的預期時程表。

人工智慧到底是一種生存威脅還是一場科學革命？它是好是壞？這個問題合理嗎？

在本文中，我們將在探討人工智慧，特別是生成式人工智慧的過程中，消除迷思，探討機會。我們將重點關注在人工智慧與當今企業組織關聯度最高的層面，特別是其對網路攻擊、隱私、智慧財產權和版權問題造成的影響。

博通觀點

Broadcom 持續導入人工智慧已有很長一段時間。它是我們保護用戶和企業IT的重點和產品解決方案不可或缺的一部分。在本白皮書中，我們將探討以下立場：

1. 生成式人工智慧為企業組織提供有價值的新工具。
2. 如果人們能夠控制生成式人工智慧的使用和發展，它就不會構成生存威脅。
3. 生成式人工智慧的廣泛應用很可能預告著第五次工業革命的開始。
4. 博通網路安全解決方案確保人工智慧始終是一種有益的力量。

讓我們從定義什麼是人工智慧開始，探討其對網路安全和企業的影響。

人工智慧術語表

人工智慧
斯坦福大學名譽教授約翰・麥卡錫於1955年定義的術語：『製造智慧型機器的科學和工程技術』。

狹義的人工智慧
只做一件事的智慧系統，例如：臉部辨識。

生成式人工智慧
一種根據訓練集(圖像、影片、音檔、文字等)中的模式生成資料的人工智慧；最著名的生成式人工智慧是 ChatGPT。

大型語言模型（large language model，LLM）
一種使用大數據集來理解、總結、生成和預測新內容的人工智慧。

神經網路 (Neural Network:NN)
一種人工智慧技術，可訓練電腦以類似人腦的方式處理資料。

調適型 (Adaptive) 人工智慧
一種具有應變能力的新興人工智慧，可根據資料或資料環境的變化進行自我調整和改進。

什麼是人工智慧？

想像一下向過去的人解釋人工智慧。你會怎麼做呢？一種方法是告訴他們，想像世界上最聰明的人都聚集在一個房間裡。這群人非常聰明，他們掌握人類有史以來產出的所有知識；任何問題都可以向這群人提問。讓人類歷史上所有最聰明的人聽命於你，這就是人工智慧的一種描述方式。

另一種方法是考慮我們如何看待披薩這樣簡單的東西。不同的人會對披薩有不同的構想。有些人會說，它只應該有特定的形狀。其他人可能會說，它只應該有特定的配料。但總括來說，人們可能會一致認為，披薩一般是圓形的，通常會有乳酪和醬汁。這種判斷來自於人們長期以來對披薩的集體經驗。人們對披薩的描述方式與人工智慧的工作方式相同，都是透過長期的經驗學習得出。

人工智慧透過深度學習系統驅動的神經網路運行，就像大腦一樣。這些系統就像人類學習的過程，但與人類學習不同的是，機器學習(ML)或人工智慧中的使用者社群資料能力意味著回應問題解答的速度要快得多。對個人來說可能需要30年的時間，對人工智慧來說可能只需一眨眼的瞬間。

人工智慧與自動化

人工智慧最具變革性的使用案例之一是它如何與自動化相結合。自動化中受人工智慧影響最大的兩個面向是自動決策和內容生成。

自動決策

人工智慧的目的在協助簡化人類工作或執行人類需要學習才能完成的工作。這些任務可能是讓生活更輕鬆的工作，如重複性工作，也可能包括人工智慧可能比大多數人做得更好的具有創造力的事情，如撰寫法律案件摘要或解釋複雜的技術。

考慮其在工廠產線上的價值。想像一下，必須決定將某個特定零件安裝在哪裡。或者考慮一輛要出廠的新車。檢查員需要判斷汽車的組裝是否正確。是否少了一個螺栓？人工智慧可以更好、更快地做出這類決定，而且無需人工來做出這類決定。這就是自動化決策。

優化決策

人工智慧的最佳和最廣泛的自動化應用案例之一是優化決策。以建築設計為例，人工智慧在優化決策方面的能力已經遠遠超過人類工程師。例如：人工智慧可以確定哪裡需要曲線，或者推薦一種從未有人考慮過的奇特形狀。生成式人工智慧的出現很可能預告著第五次工業革命的開始：一個技術可以代表人類做出更好、更智慧、更快速決策的新時代開始了。

當賽門鐵克團隊談到在我們的解決方案中應用人工智慧時，我們幾乎總是在談論使用它來優化決策的制定。

目前，AI正被駭客用來增加惡意軟體和社交媒體攻擊的數量和頻率。

不過，這也給網路安全專業人員帶來了好處：他們可以利用CHATGPT和AI更好地使用這些相同工具來防禦攻擊者。

內容生成

無論是總結現有資訊、撰寫文章，還是創作圖案、影片、音樂，內容生成都是人工智慧的第二大自動化的使用案例。

人工智慧與程式碼生成

人工智慧可以幫助生成文本，同樣也可以幫助生成程式碼。這可能是危險的，因為它可能被用於好的目的，也可能被用於壞的目的。如果人工智慧可以編寫程式碼，這就意味著在編寫程式碼(包括惡意的、非常複雜的程式碼)的能力方面，障礙已經減少。

人工智慧已經被用於生成釣魚網站。在全球範圍內，賽門鐵克威脅研究人員已經看到人工智慧被用於將網路釣魚或其他社交媒體攻擊翻譯成多國語言，進而大大擴展了目標領域。ChatGPT 非常適合用於翻譯，成效也非常好，尤其是將英語翻譯成其他語言。該程式往往能正確處理所有問題：單詞、語法、句法，甚至口語表達。

夜幕尚未來臨

人工智慧可以幫助威脅者編寫垃圾郵件、欺騙性釣魚電子郵件、社交媒體貼文和惡意軟體的能力，正在增加這些網路攻擊的數量和頻率。幸運的是，人工智慧的複雜程度還不足以讓這些攻擊與現有的攻擊大相徑庭。人工智慧可以使現有程式碼樣本或惡意程式碼樣本有更多變化，但不能使這些程式碼樣本有更複雜的版本。要讓生成式人工智慧程式想出更複雜的攻擊方式，必須有人已經想到，並在網際網路上發佈相關背景資訊。

需要注意的是，人工智慧不可能有自己的意識去創造出更複雜的攻擊策略。至少現在還不行。雖然使用現有策略的攻擊會越來越普遍，但它們不會變得更加複雜。一旦人們真正知道如何提取正確的資訊、更快地將其濃縮並使其更加複雜，這種情況很有可能會在以後出現。

提升網路攻擊防護

人工智慧的好處正被網路攻擊者用來增加惡意軟體和社交媒體攻擊的數量和頻率，反過來，它也可以讓網路安全專業人員使用ChatGPT或其他人工智慧工具，以便提供更好的防禦應對使用這些工具的攻擊者。企業可以在組織內部更廣泛地利用這些工具的功能。這樣，企業既能提高安全運營中心(SOC)團隊的專業技能，又能加快他們應對潛在威脅的速度。

人工智慧與自動化相輔相成：有好有壞。人工智慧實現攻擊鏈和防禦攻擊鏈的自動化。它也是自我調整人工智慧的一個關鍵部份，自我調整人工智慧是一種可根據不斷變化的條件自動調整的人工智慧。自動化使自我調整人工智慧成為可能。

人工智慧與網路搜尋有何不同？

人工智慧與網路搜尋有兩大不同：

- 人工智慧與網路搜尋的第一個不同點在於決策。想像一下計畫一次跨國渡假。目標是使用最省油的路線完成旅行。搜尋引擎會提供地圖，為旅行者提供指引。它們可能會提供景點列表，甚至還能提供沿途加油站的油價列表。然而，人工智慧會獲取同樣的資訊並做出獨立的決定。它將決定哪條路線最快，哪裡有最便宜的加油站，並為旅行者規劃出最佳路線。
- 人工智慧與網路搜尋不同的第二個方面是，它總是提供單一或摘要總結的答案。例如：假設一位研究人員想瞭解亨利八世。使用谷歌(Google)，截至 2023 年 5 月，研究人員將得到 105,000,000 條結果。研究人員可以自行決定關注哪些結果。而人工智慧的作用恰恰相反：它能為研究人員提供問題的直接答案。網路搜尋提供的是資料。而閱讀和分析這些資料則取決於進行搜尋的人。人工智慧對資料進行總結，而總結可能是完全錯誤，也可能遺漏對分析師或研究人員非常重要的資訊。

網路安全面向： 現在該是學習的時候了

當壞事發生在好人身上時

人工智慧可以透過多種方式直接或間接地影響網路安全。ChatGPT暴露企業資料的例子已有數例，而這可能只是冰山一角。生成式人工智慧程式正在被瘋狂採用。最近的一項調查顯示，近 60% 的受訪企業已經購買或計畫在 2023 年底前購買生成式人工智慧工具。

錯誤資訊：機器中的幽靈漏洞(Ghost Bug)

如今，人工智慧對企業造成的最大威脅之一就是企業依賴人工智慧獲取真實資訊。依賴人工智慧的問題在於無法驗證其準確性。當有人使用搜尋引擎時，它會傳回帶有資訊來源屬性的答案。資訊來源屬性允許使用者驗證資料的真假。而人工智慧則沒有來源屬性，因為它將來自成千上萬個不同地方的資訊關聯起來。企業目前無法信任人工智慧提供的資料。缺乏驗證就像是機器系統中的一個幽靈漏洞(Ghost Bug)。

信任問題

人工智慧本質上的問題，在於人工智慧可能會由於其模型及其訓練或微調方式而向使用者提供錯誤資訊。有鑒於人工智慧在企業中的應用和普及速度，這是人工智慧目前對企業構成的最大威脅。如果不加以考慮，5年後的情況可能就不是這樣。這些不正確的資訊可能會給今天的企業帶來生存危機。

展望未來，我們不難想像，到那時企業將承租一個ChatGPT系統，或其他由自己的資料集訓練出來的人工智慧，供自己使用。問題和答案將與他們的業務和資料集相關。人工智慧肯定會朝著這個方向發展。但如今，每個人都有一個共同的資料集；這正成為全球企業面臨的一個大問題。

撲朔迷離的三個術語：生成式人工智慧、神經網路以及大型語言模型

在考慮ChatGPT的潛在優勢時，我們真正應該考慮的是大型語言模型(large language models：LLM)，而不是只針對ChatGPT。現在有很多使用機器學習的案例，但事實證明LLM 可能更準確。

在賽門鐵克，我們使用機器學習(ML)分析來關聯組織內機器上發生的各種看似無關緊要的事件。我們利用這一點來識別嚴重等級的漏洞，例如：攻擊者橫向移動的情況：單台機器上的每個行為都不足以引起關注，但是個別行為的彙整關聯是整體運作最重要基礎，這些行為被認定為漏洞活動。這些類型的使用案例可能會受益於LLM。要理解其中的原因，可以將每個攻擊事件看作單一個字：單一個字毫無意義，但將它們組合在一起，LLM就能『理解』這些單字在整起情境中的上下文中的含義。

LLM還可以協助知識性問答系統，作為知識和建議來源，提高安全運營中心(SOC) 的效率。分析師幾乎可以提出任何知識性問題，如修復指導或LLM對特定感染指標(IOC)的瞭解。目前，ChatGPT已經掌握一些這方面的知識，但我們在測試中發現，這些知識還不夠充分，還需要更多的訓練資料。

不難想像，如果有正確的訓練資料，LLM可以提供全面的戰略建議，而不僅僅是在戰術情況下，例如：『有鑒於以下資產或限制，請提供我應該採用的網路安全設計架構』。LLM仍處於起步階段，尤其是在產業應用方面，但企業應期待未來幾年會有更多的應用。

生成式人工智慧的網路安全風險

在考慮使用人工智慧的網路安全風險時，有三個主要考慮因素：攻擊者、隱私以及智慧財產權和版權。

網路攻擊者

對於網路犯罪分子來說，ChatGPT、GitHub Copilot 和其他生成式人工智慧解決方案不會帶來太多額外收益。在某些領域，生成式人工智慧工具可以幫助發起攻擊，例如：構建更好或動態的釣魚郵件、撰寫惡意程式碼。ChatGPT與其他生成式人工智慧工具一樣，是一種資訊內容開發工具，而不是一個具有自我意識的實體。可以要求它『告訴我所有感染機器的常見方法』。但不能要求它『以一種以前從未想過的方式感染這些機器』。

惡意軟體程式碼或釣魚郵件本文中的內容只占成功發動攻擊所需全部投入的1%占比。雖然人工智慧有助於倍數增加攻擊次數，也有常見實作在攻擊鏈的某些階段，但它並不能從頭到尾在攻擊鏈的每個階段完全自動化地滿足網路攻擊者的需求。

意外攻擊是另一個需要考慮的問題。從生成式人工智慧工具獲得的惡意程式碼未經驗證就直接投入攻擊，可能會無意中引入新的攻擊面或造成業務中斷。

隱私、資料外洩和風險

說到隱私，主要考慮的是員工使用ChatGPT的方式。他們不僅可能上傳敏感檔案或提出會洩露公司敏感資訊的詢問，而且他們所提供的資訊和詢問還可能被整合回ChatGPT應用程式中。

使用人工智慧的員工必須謹防無意中洩露公司敏感資訊。向人工智慧生成程式提供敏感資訊與將資訊提供給第三方的效果是一樣的。輸入人工智慧程式(例如：ChatGPT)的資訊將成為其知識庫的一部分。ChatGPT的任何用戶都可以搜尋運用該共同資料集。這意味著任何上傳或詢問的資料都可以在特定的應用程式之護欄保護範圍內，一再提供給可能提出類似問題的第三方。

透過學習衡量人工智慧系統以防止其出現偏差和無意中混入關鍵企業資料至關重要。人工智慧系統提供的資訊必須經過驗證。錯誤資訊和偏見在網際網路上隨處可見。就人工智慧而言，在使用人工智慧接收到的任何資料之前，都必須對這些因素進行測試和修正錯誤。如果企業使用ChatGPT進行程式碼編寫，這一點就更加重要。重要的是要理解，人工智慧系統的偏誤和結果是可以衡量的，因此它們在一定程度上是可以預測。

智慧財產權和版權問題

生成式人工智慧最棘手的問題之一是其對智慧財產權(IP)的影響，尤其是對使用ChatGPT的程式碼或創意工作的影響。這些問題並不像有些人認為的那樣簡單。如果企業開發人員使用ChatGPT建立程式碼，這些程式碼是屬於企業的智慧財產權，還是屬於網際網路的智慧財產權？如果ChatGPT建立的程式碼有兩個來源呢？是50/50歸屬還是廢除另一個開發者的 IP？

使用 ChatGPT 或類似 GitHub Copilot 的人工智慧解決方案來構建文件或程式碼的企業需要瞭解，這些文件或程式碼的來源可能有版權疑慮。他們可能會將程式碼結合到自己製作的應用程式中，而這些程式碼並未獲得適當的授權許可。他們可能需要重新發佈已受版權保護的網頁程式碼或文件。

偏誤、智慧財產權和資料洩露

在人工智慧和我們的世界中，偏誤都是導致決策出現偏差或錯誤的現象。企業需要人工智慧的說明來識別資訊來源、建立防護欄，並提供額外的上下文來驗證人工智慧資訊的準確性。* 在決策過程中，決策者常會受到框架效應的影響，而導致決策出現偏差或錯誤的現象。

目前，企業對人工智慧的兩大擔憂涉及智慧財產權：

- 我的資料是否洩漏？
- 我該如何控制我的系統從資料中學習的內容？

原創性問題

人工智慧執行創作性任務的能力引發人工智慧相關問題中最具爭議的一個：

人工智慧所創作的作品在某種意義上是否具有原創性，還是永遠只是一個很好的副本或贋品？

答案很複雜。雖然聽起來有些違反直覺，但在確定什麼是原創、什麼不是原創時，其界線相當模糊。大多數人工智慧都需要經過訓練才能學習，就像人隨著時間接受訓練與學習一樣。最終，人工智慧軟體也會像人一樣，根據以往的經驗做出決定。那麼，這兩者有區別嗎？

試問考慮讓人工智慧程式建立一幅當今世界上還不存在的圖片。比方說，讓一隻貓坐在籃球上面吃披薩。從某種意義上說，這就是一幅原創圖片。這幅畫的任何構成元素都是原創的嗎？如果是一位藝術家畫的，這幅畫會被認為是原創嗎？如果有人質疑人工智慧是否能創造出原創性的東西，那麼我們是不是也可以問一下人類是否也能做到這一點呢？

2020年，一個團隊建立一種演算法，產出680億首獨特的旋律。然後，他們將這些旋律發佈到公開領域。這樣做的目的是為了抵制音樂行業中越來越常見的藝術家對其他藝術家提起的版權訴訟，這些藝術家被指控竊取他們的旋律來創作熱門唱片。這一努力是有效的，還是對藝術自由的又一次侵犯？這個問題仍然沒有定論，因為該專案本身就可能違反版權法，因為人工智慧產生的一些旋律早就由其他藝術家所錄製。

圍繞在人工智慧和原創性的這一問題在未來幾年肯定會更加嚴重。

讓我們看看兩個固有使用案例，一個用於DLP，一個用於法規遵循(合規性)，看看生成式人工智慧在每個用案例中發揮的作用。

傳統DLP使用案例：網路釣魚

有了人工智慧，內部威脅就會變得嚴重。對企業瞭若指掌的內部人員可以使用ChatGPT製作出非常逼真的電子郵件。他們可以如法炮製他人的風格、錯別字等一切內容。此外，攻擊者還可以完全複製一模一樣的網站。

Symantec® DLP等企業等級的資料外洩防護 (DLP) 解決方案可以幫助阻止這類攻擊。現在的程式碼還不夠複雜，但五年後可能會是另一番景象。除其他優勢外，DLP還能利用人工智慧加快事件優先順序的排序，幫助高級分析師篩選最嚴重的威脅，並識別那些對企業不構成嚴重威脅的威脅。

ChatGPT、Bard和諸如此類的生成式人工智慧程式並不像某些人認為是那樣成熟的工具。當今真正的網路資安問題是人工智慧程式如何提高網路釣魚郵件和惡意網站的質量。社交工程攻擊依賴於使用者的粗心大意或匆忙點擊魚叉式網路釣魚郵件的連結。這不是人工智慧本身的問題，而是人性的問題。就安全性而言，防禦這類攻擊與部署針對臉書和其他社交媒體網路釣魚攻擊的防護機制其實沒有什麼不同。最大的威脅在於，與個人在社交媒體上發佈單個貼文不同，在 ChatGPT 上，壞人可以一次性發佈大量資料。

傳統法規遵循(合規性)使用案例

當生成式人工智慧根據的是錯誤資訊而做出決策時，很容易導致典型的法規遵循(合規性)案例。為避免出現法規遵循(合規性)問題，企業必須要特別注重在測試人工智慧解決方案時，需要改善資料衛生狀況並評估偏誤。企業將需要新的資源來管理人工智慧以處理偏誤和我們還不知道的情況。

對安全專業人員的益處

我們曾經提到過，當我們從攻擊數量增加的角度討論威脅形勢時，樣本數量的增加對安全專業人員來說也是一種正面發展。如果 SOC 能夠增加樣本數量，他們就有了更大的資料集來調整自己的人工智慧，進而能夠防範這些類型的攻擊。更強的運算能力與更大的資料集相結合，還能更快地應對攻擊。這有可能改變遊戲規則，因為平均回應時間(MTTR)有可能從幾周縮短到幾天，甚至幾毫秒。

當這些工具在可靠、已知良好和相關的資料集上接受訓練時，它們的真正威力才會顯現出來。賽門鐵克安全威脅與響應(STAR)團隊一直在使用這種技術和方法來生成可靠、準確的威脅情報。

人工智慧大幅改變了事件優先排序的策略：它可以幫助安全分析師更有效、更一致地確定安全事件的優先順序。

事件優先順序

人工智慧大幅地改變了事件優先順序的應對策略。它可以幫助安全分析人員更有效率且能持續順暢運作決定事件順序，排定優先處理的風險項目。這對威脅防護和資料保護都大有裨益。當一個目標遭入侵時，問題往往不是安全分析師不知道發生了入侵，而是事件太多，根本無法對所有事件做出回應。

從DLP的角度來看也是如此：應該優先處理哪個DLP事件？分析師是要確認已經被阻止的4,000起可能的事件，還是確認已發生的敏感資料外洩事件的案例上？人工智慧可以幫助加快決策過程，幫助篩選並引導高級分析師首先處理這些案例。

博通與生成式人工智慧

自我調整和預測能力

博通的賽門鐵克企業安全部門擁有全球民營機構最大的威脅情資大數據，我們在這些資料上運行我們的AI／ML引擎。賽門鐵克至少在十年前就開始人工智慧的創新。這為我們提供了在自己的資料湖上運行ML和AI引擎的機會。這為我們提供一個如虎添翼的契機，讓我們能夠更好地利用我們擁有的資料和其他地方隨時發生的事件來辨識威脅。這使賽門鐵克解決方案能夠更快地識別威脅。

ChatGPT是一個例子，說明機器學習(ML：AI背後的基本模型)如何善用許多不同的資料點為分析人員預測攻擊事件，在根本上扭轉網路安全分析上的複雜度。我們可以採取任何行為，看看網路攻擊者如何利用它。然後我們可以說，即使沒有證據顯示這種特定的攻擊，是如何發生的，但可以在攻擊發生之前就阻止它。

賽門鐵克的優勢

我們採取獨特的方式，利用人工智慧和自動化將資料保護和威脅防護結合在一起。博通公司將這兩種資料方案與我們的賽門鐵克企業雲(SEC：Symantec Enterprise Cloud)安全解決方案相結合，在我們長期將人工智慧融入網路安全產品和解決方案的輝煌紀錄的基礎上更上層樓。

保護用戶和企業智慧財產權是我們關注的重點。對於生成式人工智慧系統帶來的威脅，已經擁有我們的DLP解決方案的企業會特別有信心。ChatGPT並不會製造出我們偵測不到的惡意軟體。在這個使用案例中，我們並非從零開始。十年前，我們就開始在定義檔中使用機器學習(ML)。這些經驗使我們在電腦病毒等惡意程式防護領域佔有一席之地。從那時起，我們就占得人工智慧創新的先機，至今仍致力於保持業界領頭羊的地位。最近，我們利用自我調整保護 AI 技術來保護企業環境，使其免受威脅形勢向更複雜、更有針對性的攻擊轉變的影響。

博通網路安全解決方案將確保人工智慧仍然是一股向善的力量。對於我們全球的客戶、合作夥伴和供應商，很清楚，當論及人工智慧和網路安全的未來時，博通將永遠是您的後盾。

結論：善的力量

生成式人工智慧系統為企業組織提供寶貴的新工具：

- 讓安全專業人員提供更好的安全軟體。
- 解決網路安全和其他利用資料分析結果制定方案等專業技能短缺的問題。
- 縮短檢測、事件回應和矯正的時間，進而縮短獲取可操作知識的時間。
- 縮短年輕網路人才發揮生產力的時間。

如果人們能控制人工智慧的使用和進化，那麼生成式人工智慧就不會對人類的生存構成威脅：

- 它本質上並不邪惡。不要害怕它。
- 它將改變我們的生活和工作方式，但我們必須小心謹慎。
- 我們相信--也看到了證據--許多公司正在為它的發展設置防護機制。

生成式人工智慧的出現很可能預告著第五次工業革命的開始：技術可以代表人類做出更好、更智慧、更快速的決策，這是一個新時代的開始。

博通・賽門鐵克的網路安全解決方案將確保人工智慧始終是一股向善的力量。對於我們的全球客戶、合作夥伴和供應商而言，請相信，在人工智慧和未來安全領域，Broadcom將始終是您的堅強後盾。

欲瞭解更多資訊，請瀏覽 symantec.com 或賽門鐵克解決方案專家：保安資訊有限公司的中文網站https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

關於賽門鐵克

賽門鐵克是資安業界的長青樹，品牌享譽至今超過四十年。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，近年來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

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。

BROADCOM®
connecting everything®