

Symantec[®] Content Analysis

多層式威脅檢測、偵測與沙箱分析， 揪出未知威脅



目錄

在當今不斷演變的威脅態
勢下，兼顧防護與賦能

業界既有的資安因應之道

更優異的進階威脅防護架構

威脅隔離

彈性化部署與整合選項

結論

在當今不斷演變的威脅態勢下，兼顧防護與賦能

毫無疑問，企業組織所面臨的資安攻擊將持續增加並不斷演變。真正的問題在於：企業組織該如何因應惡意程式與其他風險，同時又不會對員工造成不必要的限制？

企業組織該如何跳脫恐懼與焦慮的心態——這種心態往往導致過度的禁止、預防、封鎖與排除——讓資安技術既能保護員工，又能賦予員工更大的工作能力？

答案就在於多層式防禦——結合進階資安技術與精密的維運實務，全面涵蓋各類威脅途徑。本白皮書將探討在當今瞬息萬變的網頁環境中，多層式防禦為何日益重要，並說明落實有效多層式防禦策略時的關鍵考量。

克服在所有進入點確保網頁安全的障礙

網頁至今仍是惡意程式散布的主要來源，但由於網頁環境瞬息萬變且規模龐大，企業組織要確保網頁安全並非易事。心懷強烈動機的惡意程式作者，只需要一個極其微小的資安漏洞，就能藉此謀取財務或競爭優勢，或達成政治、意識形態目的。

攻擊者可運用五花八門的手法，並任意組合運用以利用弱點。企業組織資料的行動化程度提高，加上自帶裝置 (BYOD) 政策的推行，正為網路犯罪者創造大量可乘之機。

BYOD 所帶來的生產力優勢，也因其引進了必須加以防護、但企業組織卻難以掌控的新平台 (例如：iOS 與 Android) 而大打折扣。此外，雲端與社群媒體應用程式，也讓企業組織極難掌握所有潛在的攻擊途徑。

根據 Symantec[®] 網際網路安全威脅報告 (Internet Security Threat Report)，2018年：

- 每分析 10 個網址，就有 1 個被判定為惡意網址
- 勒索軟體偵測總數達 545,231 件；企業端偵測件數成長 12%
- 針對端點的網頁攻擊成長 56%

為何需要進階多層式防禦

由於電腦與網路可能經由多種攻擊途徑遭到感染，單點偵測的時代已成過去式。新興、動態的網頁威脅與進階持續性威脅 (APT) 日益增加，需要一套能將涵蓋範圍最大化的多層式資安架構，才能確保企業獲得業界頂尖的資安防護。

企業組織必須部署多種資安機制的組合，才能將攻擊防範涵蓋範圍最大化。這不僅代表要在環境的多個層級中運用多種資安技術，也代表要落實良好的維運實務，例如：及時套用更新與修補程式，並要求供應商針對弱點快速提供修復方案。

從防惡意程式／防毒(AV)的角度來看，多層式防禦應涵蓋桌面、伺服器與網路層級的防護。PCI(支付卡產業標準)等產業標準，對特定產業別應建置何種防毒防護，訂有嚴格規範。終端客戶往往希望獲得保證，確信企業已採取一切必要措施以防範資安事件發生。因此，無論從資安角度或商業角度來看，多層式防禦做法都相當合理，有助於降低企業組織與品牌所面臨的風險。

業界既有的資安因應之道

端點防護：不可或缺的第一步

端點防護解決方案可因應源自受感染桌面裝置的威脅，並能協助抵禦源自網路內部的攻擊，例如：當使用者插入受感染的USB隨身碟，並將惡意程式上傳至其電腦時。部分企業組織也可能同時採用多家廠商的端點防護解決方案，以將攻擊涵蓋範圍最大化。

端點防護固然重要，但若僅依賴端點防護，恐將帶來一種錯誤的安全感。使用者可能竄改或停用代理程式設定，也可能未定期更新軟體以防範最新威脅。此外，隨著BYOD的興起，許多用於存取企業組織資源的行動裝置完全暴露於風險之中——適用於iOS與Android裝置的防毒解決方案本就不多，願意在裝置上安裝這類資安應用程式的使用者更是少之又少。因此，企業組織必須採用多層式防惡意程式防禦，以涵蓋各種可能的感染途徑，藉此最佳化防護範圍。

閘道端進階威脅防護：不可或缺的必要措施

網際網路閘道是所有網際網路流量的進入點，來自PC、筆記型電腦、平板電腦、智慧型手機及物聯網裝置等各類端點的流量，都必須通過此處。透過加入以網路為基礎的威脅防護，企業組織可強化桌面裝置的資安防護，並降低攻擊風險，同時建立一個使用者無法停用或竄改的單一控管點。盡可能在靠近資安邊界、遠離桌面裝置之處攔截惡意程式，可進一步降低受感染資料觸及終端使用者的風險。

網路防毒：網路防禦的關鍵要素

為企業組織加入以網路為基礎的防毒防護，可強化桌面裝置的資安防護，並協助降低攻擊風險。雖然加入網路防毒有所助益，但僅憑此步驟並不足以提供辨識當今威脅所需的防護能力。若僅依賴單一網路防毒引擎，意味著僅擁有來自單一廠商的單一偵測方法。這種設計的侷限，在於該廠商對可能攻擊的認知範疇、其檢測方法、其更新排程，以及其威脅情蒐蒐集能力——而這些情資可能僅來自一小群客戶，未必涵蓋辨識最新威脅所需的最新更新資訊。網路防毒雖是關鍵要素，但仍須搭配其他偵測方法，才能提供更有效的威脅防護。

更優異的進階威脅防護架構

架構設計

單一產品或服務無法提供萬無一失的資安防護。更優異的資安架構，需要多層防護相互搭配運作，才能發揮整體大於個別加總的成效。賽門鐵克整合完整的產品、服務與技術範疇，在網頁閘道端提供進階威脅防護。此架構始於網頁代理伺服器，先全面掌控所有網頁流量，接著導入賽門鐵克所提供的多層防護。這個銜接多層威脅檢測的流量終止點，正是提供優異進階威脅防護的關鍵所在。

1：代理伺服器——不可或缺流量終止點

網頁代理伺服器是流量終止點的一種形式，可為網頁流量提供隔離檢疫服務。它會檢查使用者與HTTP／HTTPS網站之間100%的流量，並針對所有網址進行分類，藉此辨識並封鎖惡意網站或網頁，同時依政策讓正常網址維持可存取狀態。由於代理伺服器提供了流量終止點，因此也能善用此優勢，將可疑檔案傳遞給Content Analysis等其他資安工具進行進一步檢測。

非代理伺服器架構的網路資安部署方式，以及次世代防火牆(NGFW，包括TAP或SPAN埠部署方式)等其他技術，均無法有效終止流量。採用TAP或SPAN埠裝置時，閘道器僅位於網路的側邊位置，只能觀察經過的流量，而無法加以攔截並終止。

圖 1：Content Analysis 提供多層式威脅檢測方式

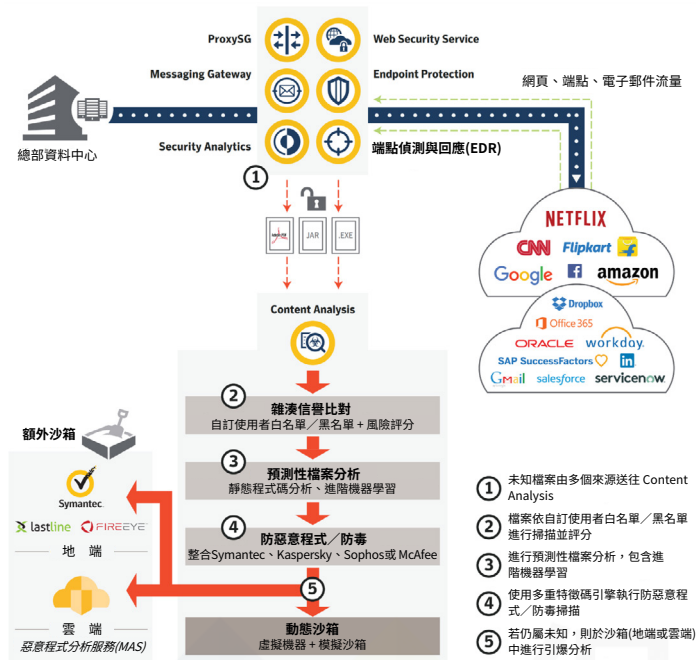
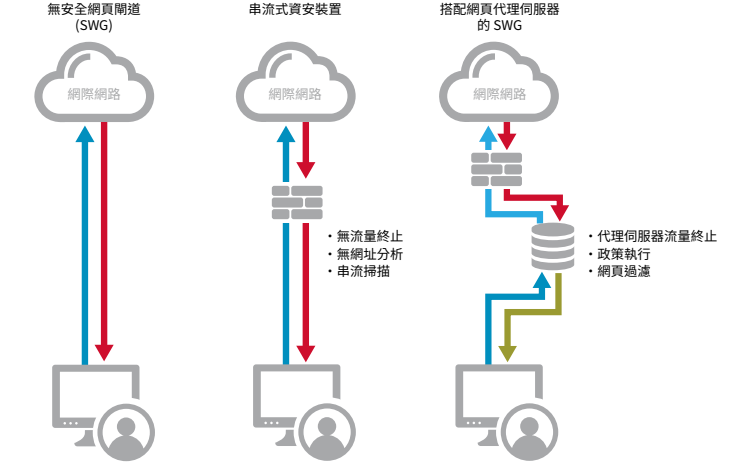


圖 2：代理伺服器解決方案提供流量終止點，以利政策執行、網頁過濾與更深入的檢測



態。

系統會將這些雜湊值比對一個每日更新、總計超過50億筆記錄的資料庫。透過運用自訂核可清單與拒絕清單，以及來自多家廠商(包括賽門鐵克自有的全球情資網路)的檔案信譽資料，Content Analysis可執行即時應用程式與檔案識別，這些檔案將獲得1至10分的信任分數。

Content Analysis會將已知「可接受」的檔案放行給使用者，並封鎖被判定為「已知惡意」的檔案。這道過濾程序可進一步減少傳遞至下游防惡意程式檢測與沙箱分析階段的檔案數量。

為避免對已識別信譽狀態的檔案進行不必要的掃描與分析，您可在Content Analysis中新增一份SHA1雜湊值清單。在檔案處理過程中，Content Analysis會先檢查這些清單，才會向雲端檔案信譽服務進行查詢。手動設定的核可／拒絕清單，可快速做出「允許」或「拒絕」的判定，無需進一步分析。只要雜湊值存在於任一清單中，該檔案即會直接獲准放行或遭到拒絕，無需進一步處理。

3：預測性檔案分析／機器學習

在預測性檔案分析階段，Content Analysis會執行靜態程式碼分析與進階機器學習，判定檔案程式碼中是否有任何內容被標記為惡意。系統會剖析並擷取檔案程式碼，與超過500萬筆已知惡意資料或已知惡意程式碼的資料點進行比對。

透過結合對威脅與檔案的深度瞭解，以及最先進的機器學習技術，Symantec進階機器學習(AML)能理解檔案的特徵，並產生機率分數，藉此判定檔案是安全或惡意。這項機率分數將決定Content Analysis接下來該如何處理該檔案：

NGFW採用串流式偵測方法，在流量於線路上傳輸的過程中進行檢查。這類部署方式存在一項特定缺陷：惡意程式或其他威脅可能趁隙通過閘道，因為NGFW未能及時偵測到威脅，或未能及時送出TCP重設封包以中斷流量傳輸。此外，由於串流式掃描的特性，惡意程式可能利用一段時間內分批傳送的分割封包進行遞送，因而始終未被偵測到。代理伺服器就其本質而言，會等待整個物件完整組裝並掃描完畢後，才允許其被遞送。

在駭客手法瞬息萬變的快節奏網頁環境中，同時部署Symantec ProxySG與NGFW的縱深防禦策略，是提供最佳防護的必要做法。ProxySG經過精心設計，足以抵禦規避技術，因此是NGFW的絕佳互補方案。其領先業界的網頁代理伺服器技術，能辨識並封鎖惡意網頁內容，其開放式架構更可與業界頂尖產品整合，進一步強化資安態勢。

Symantec ProxySG是業界領先的代理伺服器解決方案，連續12年獲Gartner評選為領導廠商(Leader)，是企業組織網路資安架構中的關鍵一環。ProxySG可保護網頁流量，提供網址信譽評等、SSL解密、分類與政策控管，以及即時封鎖等功能。經過第一階段處理後，凡未經代理伺服器立即封鎖的內容，均會傳遞至Content Analysis進行檢測與深入審查。

2：CA——雜湊信譽比對與檔案信譽服務

ProxySG分析並分類所有網頁流量後，會將未知檔案的雜湊值從代理伺服器傳送出去，進行分析以判定其已知信譽狀

威脅隔離

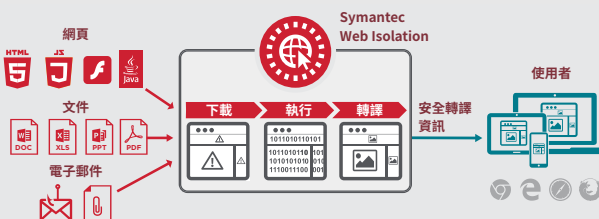
威脅隔離是進階威脅防護中的另一項創新做法。此防護層並不依賴「偵測後預防」的循環，而是在不影響使用者的前提下，隔離惡意的網頁與電子郵件內容。此做法採取「假設一切皆可放行」的原則，允許將所有分類為「未知」的網站請求，或所有來自關鍵員工的請求，一律轉往威脅隔離機制處理。如此一來，使用者仍可存取該網站，同時又能隔絕任何威脅。

圖3：Symantec Web Isolation 與 ProxySG、Web Security Service 整合，提供安全的瀏覽體驗



Symantec Web Isolation可輕鬆整合至進階威脅防護中，讓所有未知／高風險網站都能被隔離，同時也可用於隔離電子郵件中的連結與附件。

圖4：未分類的網站、連結與內容，會在可拋式隔離容器中安全轉譯給終端使用者，藉此保護使用者免受未知惡意程式侵害



- 機率評估為高度惡意的檔案，將直接遭到封鎖(判定為惡意)。
- 未被判定為惡意的檔案，則會轉往其餘資安防護層進行進一步分析。

AML提供額外的控制項，可定義AML執行檔案封鎖的門檻值與積極程度。在高偵測敏感度設定下，AML對於檔案是否可能構成威脅的判定會更為積極，但也可能因此誤封並非真正惡意的檔案。在較低敏感度設定下，AML封鎖的檔案數量會較少，但也可能因此有部分威脅未被偵測到。

機器學習並非仰賴特徵碼比對樣式，而是採用經過驗證、通過嚴格測試的統計方法。這使得AML能以特徵碼技術做不到的方式，學習並理解檔案特性。透過這種做法，全新且先前未知的威脅也能被有效阻擋。即使攻擊手法透過複製機制、散布機制，或酬載本身而有所變化，AML仍能有效發揮阻擋威脅的作用。

4：CA——防惡意程式／防毒

Content Analysis可部署來自Symantec、Kaspersky、Sophos或McAfee等廠商的雙引擎組合。系統會評估特徵碼以識別已知惡意檔案，並將其封鎖。賽門鐵克內部測試發現，相較於僅使用單一引擎，同時採用兩套引擎可將偵測能力提升12%。特徵碼資料庫每5分鐘更新一次，並支援最大5GB的檔案大小。

採用多套防毒引擎的效益，不僅在於能封鎖更多惡意程式與病毒，還有其他益處。運用多套引擎的優勢，在於不受限於單一更新排程，也不侷限於單一掃描技術。防毒引擎的選擇，可依理想防禦策略靈活搭配。若已採用某防惡意程式／防毒引擎掃描端點，於網路層級改採不同廠商的引擎，可望帶來額外的防護成效。

5：沙箱分析

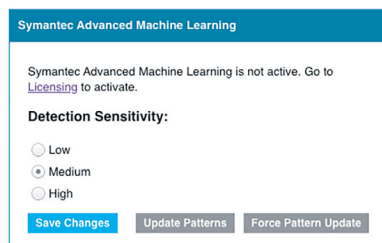
Content Analysis同時具備賽門鐵克精密的沙箱分析能力。企業組織可在同一台Content Analysis設備上授權使用此沙箱功能，或選擇採用賽門鐵克代管的沙箱服務。Content Analysis的沙箱功能具備多項進階特色，使其相較於競爭產品更具吸引力。這些特色有助於快速分析並排定進階惡意程式與零時差威脅的修復優先順序，並可持續強化資安防護：

- 獨特的雙重沙箱架構：結合模擬與虛擬化混合技術，達到最佳的規避手法偵測效果
- 標準映像設定檔複製：可自訂的分析環境，與正式作業系統高度相符
- 惡意程式規避偵測方法：Content Analysis 採用一套積極的反制措施，偵測並挫敗規避型惡意程式

- **虛擬使用者外掛程式**：模擬使用者行為，包括按鍵操作與接受安裝步驟，藉此誘騙惡意程式執行，進而觸發偵測
- **偵測樣式庫**：可偵測目標式攻擊與一次性使用的惡意程式，且不依賴特徵碼式偵測方法
- **沙箱規避偵測**：可偵測並繞過刻意設計用來拖延、等待沙箱分析結束的長短時間休眠機制，同時也能識別惡意程式試圖偵測自身是否正處於人工分析(虛擬機器)環境中的行為
- **靜態程式碼與 YARA 規則分析**：執行檔案指紋比對、偵測封裝工具(packer)、分析字串，並運用文字與二進位樣式識別及分類惡意程式樣本
- **詳細報告**：提供自訂報告，顯示整體風險分數、關鍵風險指標、詳細的惡意程式活動報告、惡意程式執行行為的螢幕截圖，並可下載惡意程式相關檔案，全方位簡化惡意程式識別與修復作業
- **檔案暫扣**：以 Symantec ProxySG 作為流量終止點，Content Analysis可在檔案接受檢測期間暫予扣留，唯有在完整分析並判定可安全放行後，才會遞送給使用者。相較於競爭對手在沙箱分析仍在進行時，便逕自放行未知檔案，這是賽門鐵克獨有的能力

對於效能需求較高的企業組織，沙箱功能可部署於另一台專門配置用於沙箱分析的Content Analysis設備上，可選用賽門鐵克，或FireEye、Lastline的技術。此外，也可選擇透過Malware Analysis Services，將未知檔案轉送至賽門鐵克雲端沙箱進行檢測。

圖 5：在 Content Analysis 中設定 Symantec 進階機器學習的偵測敏感度

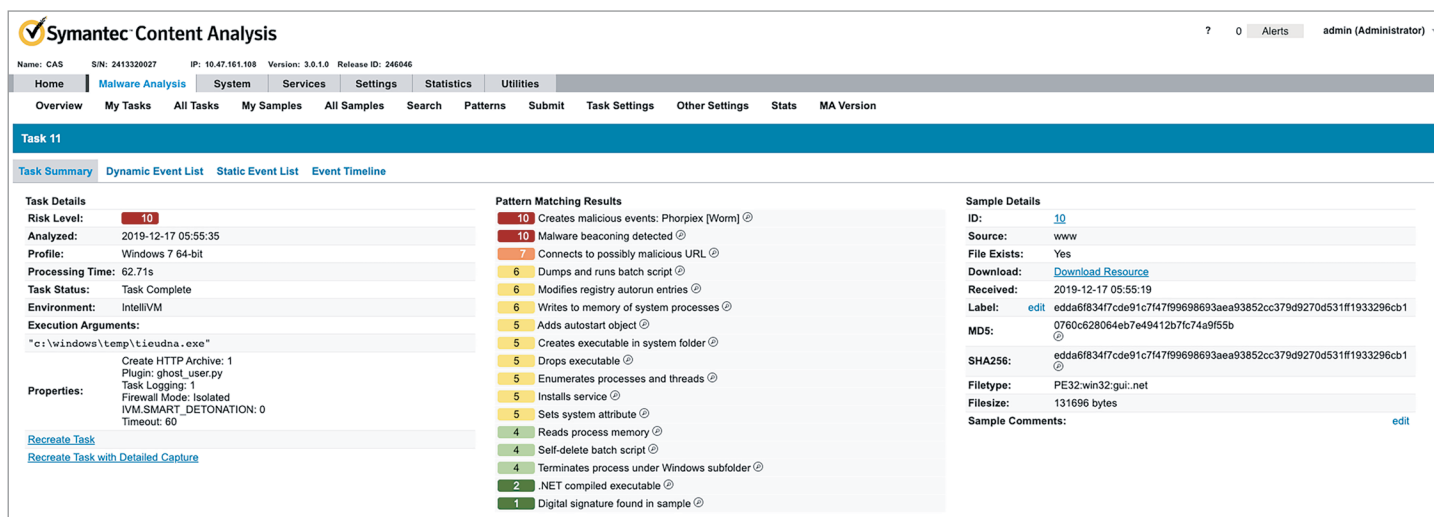


彈性化部署與整合選項

Symantec Content Analysis提供多種部署選項，以滿足不同企業組織的需求，可選擇實體設備或虛擬設備。虛擬設備選項可提供更高效能：在VMware® ESX 上最高可達 1.6 Gb/s。沙箱功能同時提供機箱內建與雲端兩種選項。對於已部署 Symantec Web Security Service(WSS) 的企業組織而言，Content Analysis 中所採用的同一套內容檢測引擎，在 WSS 中同樣可用。

將Content Analysis與其他資安工具整合，同樣能帶來極高的價值。運用ICAP協定，Content Analysis不僅能從代理伺服器接收未知檔案，也能從其他來源接收。這使得系統得以針對源自防火牆、郵件閘道、端點偵測與回應(EDR)解決方案，或環境中其他來源的未知內容，執行深度檢測。Content Analysis與Symantec Endpoint Security整合，提供從網路到端點的可視性、分析、封鎖與修復能力，以保護企業組織免受當今各種進階威脅侵害。若Content Analysis識別出惡意程式，即可將入侵指標(IOC)傳送至Symantec Endpoint Security Manager，或CounterTask等其他EDR解決方案，以驗證源自網路的威脅是否已侵入端點。系統隨即可為其他所有端點進行防護接種，並實現快速應變與修復。

圖 6：詳細沙箱分析報告，顯示具體的惡意程式活動



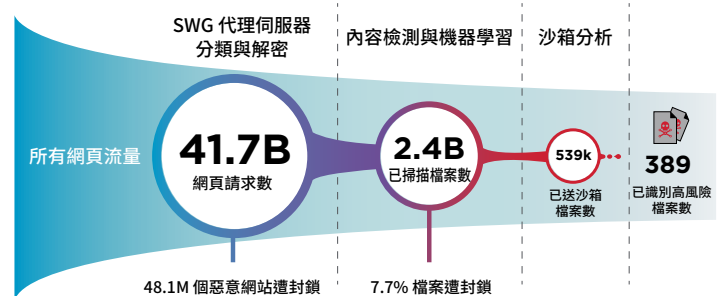
結論

與競爭對手不同，賽門鐵克採用多層式做法，形成一種漏斗效應：先運用快速掃描技術進行前端處理，唯有真正無法辨識的未知檔案，才會送交更精密、運算密集的流程進行更深入的檢測。此做法可望減少誤判、提升掃描效率，並讓應變資源專注於真正影響企業組織的實際威脅。

導入多層式資通安全平台，有助於減輕資安團隊的負擔，並降低「單點解決方案是否足夠」的疑慮與焦慮。隨著資安攻擊持續增加並不斷演變，唯有採取全方位的多層式資安防護做法，才能有效保護企業組織。

圖 7：Symantec 多層式漏斗效應

進階威脅防護 財星 20 大企業



如需更多資訊，請造訪我們的網站：<https://www.savetime.com.tw/>



關於賽門鐵克

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兼容性，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3年Symantec很少出現在由公開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績，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。(美籍華人王嘉康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年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。