

白皮書

傳承創新的深厚底蘊， 迎向資安的未來

攜手 Broadcom，
打造值得信賴的資安韌性基礎

傳承創新的深厚底蘊，迎向資安的未來

攜手 Broadcom，打造值得信賴的資安韌性基礎

目錄

執行摘要

轉型中的資安態勢

抵禦進階攻擊的韌性

安全遷移至雲端

符合政府法規要求

大規模現代化威脅防禦

結論

執行摘要

當今企業正面臨一項矛盾局面：IT現代化與生成式AI雖然為企業開啟新的成長機會，卻同時也擴大攻擊面。這樣的擴張，讓組織暴露於勒索軟體(Ransomware)、內部威脅、雲端組態設定錯誤，以及複雜的國家級駭客攻擊之下。資安團隊承受著極大壓力，必須在日益混合化的IT環境中，保護資料、應用程式與使用者；而這些資安團隊必須在因應日益提高的合規要求與資源有限的雙重挑戰下，完成上述所有工作。

在此環境下，單點式產品與分散式廠商策略已顯不足。客戶所需要的軟體，必須符合以下要求：

- 具備數十年經驗證的資安軟體專業能力
- 涵蓋身分、資料、端點與雲端的統一資安產品組合
- 以深度情資為後盾的可信賴基礎

此資安產品組合，建立於Broadcom所併購之資安軟體龍頭企業——Carbon Black、CA Technologies與Symantec——的深厚歷史基礎之上。Broadcom提供獨具特色的產品組合，其廣度足以為企業與政府機關提供所需的策略性解決方案。

本文件將重點闡述當今影響組織的關鍵資安挑戰，並針對這些挑戰對應說明適切的Broadcom®解決方案。本文件同時也將檢視既有資安解決方案，與Broadcom最新併購之VMware之間的綜效。我們的目標，是協助客戶建置一套端對端、安全的私有雲基礎，無縫整合基礎架構與資安防護。

轉型中的資安態勢

長久以來，科技始終是企業策略與成長的基石，然而第四次工業革命(數位經濟)的興起，已從根本上重塑了整體格局。這場革命具備全球化、以客戶為核心、持續演進、以科技為驅動力，並以資料為核心等特性。

資料雖然驅動著創新與營收成長，但其價值也使其成為網路威脅鎖定的首要目標。為支援數位轉型而進行的IT環境現代化，已擴大了攻擊面，進而增加資安缺口並放大風險。客戶目前主要面臨以下痛點：

- **攻擊手法日益精密：**網路犯罪分子不斷精進其攻擊手法，運用勒索軟體(Ransomware)、零時差(zero-day)攻擊利用，以及遭入侵帳戶，藉此繞過傳統資安防禦機制。
- **雲端導入：**組織為維持競爭力，已將應用程式與工作負載遷移至雲端基礎架構；然而，這些遷移過程也暴露出容易遭到利用的資安缺口。
- **合規要求：**隨著資料外洩事件日益增加，組織面臨與日俱增的壓力，須確保資料保護與治理措施能符合新興的資料隱私與資安法規要求，在高度受監管的產業中尤其如此。
- **人才短缺：**速度、靈活性與經驗，正是驅動現代應用程式開發的關鍵要素，然而組織同時也必須在日益嚴重的人才短缺之下，兼顧維持穩定性、品質與資安的需求。

這些痛點更因廠商分散而加劇。本文件將重點闡述Broadcom所提供、可因應上述挑戰的關鍵資安技術。

抵禦進階攻擊的韌性

勒索軟體防禦

勒索軟體(Ransomware)依然是最重大的網路威脅之一。根據《2025年Verizon資料外洩調查報告》指出，勒索軟體的發生率大幅成長，較前一年度報告增加37%。在2025年所檢視的所有資料外洩事件中，有44%涉及勒索軟體，較前一年度的32%明顯上升。

勒索軟體屬於惡意軟體(Malware)的一種，可透過多種方式散布，常見的攻擊向量包括網路釣魚(Phishing)電子郵件、惡意下載內容，以及不安全的網站。

勒索軟體防護面臨以下主要挑戰：

- **偵測：**以特徵碼為基礎的工具，難以偵測新型威脅與攻擊手法。
- **防護做法：**以機器學習與信譽評等為基礎的工具，對於新興的就地取材式攻擊(Living off the Land)手法效果有限。
- **介入處置：**端點偵測與回應(EDR)工具，仍需投入人力進行事件分級處理。

面對勒索軟體攻擊，並不存在單一的解決方案；唯有結合多項資安技術與做法，才能有效預防並緩解此一威脅。以下提供六項建議，可納入貴組織的資安策略之中，協助防範勒索軟體與其他電子郵件型攻擊：

- 導入完善的電子郵件資安防護，檢測並封鎖可疑電子郵件與連結，防止其進入使用者的收件匣。
- 安裝具備即時防護能力、信譽良好的防毒軟體，攔截漏過電子郵件資安防護的惡意郵件。
- 確保端點持續更新並套用修補程式。許多攻擊者會利用已知弱點入侵筆記型電腦與伺服器。
- 定期將檔案備份至雲端或外接硬碟，確保一旦資料遭到入侵，也能迅速復原。
- 針對具有提升權限或特權的使用者、帳戶與系統，訂定並落實政策控管措施。
- 將所有敏感資料加密，防止駭客存取並竊取；同時導入遠端抹除機制，一旦資料落入駭客手中，即可將其徹底銷毀。

如需進一步資訊，歡迎參閱我們的電子書《Code Red Alert: Don't Become the Next Digital Hostage》，其中詳細說明如何落實上述最佳實務做法。

零時差攻擊防禦

Carbon Black®軟體與Symantec®軟體採用多層次防禦架構，結合預防機制、AI／機器學習(ML)驅動的行為分析，以及端點偵測與回應(EDR)能力，在零時差攻擊(zero-day attack)造成損害之前，即加以辨識並修復，藉此因應零時差攻擊威脅。

零時差攻擊往往難以偵測，且要求組織必須迅速應變；採用具備多層次防禦能力的端點資安解決方案，可拖延攻擊者的行動速度，讓資安團隊在損害發生之前，有更充裕的機會加以辨識並回應。

- **預防**：部署多層次的預防性技術，包括入侵防禦系統(IPS)與AMSI(Antimalware Scan Interface，防惡意軟體掃描介面)防護，並搭配傳統特徵碼與雲端信譽特徵碼防護，可將許多威脅阻絕於端點之外。
- **行為分析**：持續監控正常行為模式，確保當使用者或裝置出現異常行為時，Symantec CloudSOC CASB 分析人員能即時收到警示並展開調查。搭配 AI／機器學習(ML)驅動的模式辨識技術，即使是細微的異常行為，也能被辨識並加以調查。
- **EDR**：持續監控並分析端點資料的能力，確保當事件需要進一步調查時，分析人員能取得所需的完整脈絡資訊。
- **應用程式控管**：防範零時差威脅的另一項關鍵防禦措施，是由 Carbon Black 率先開創的應用程式控管技術。應用程式控管在預設情況下，僅允許可信任的軟體於環境中執行，主動封鎖零時差攻擊可能利用的多種滲透途徑。

遭入侵帳戶防禦

帳戶遭竊，向來是資安領域的重大隱憂。隨著全球組織的工作模式轉向「隨處、隨裝置」的辦公型態，傳統資安防護的界線也隨之被拉伸擴展，如今企業網路內外皆須具備防護能力。帳戶遭入侵已不再僅是內部問題，客戶帳戶同樣面臨相同的風險。

當今的資安挑戰，促成了零信任架構(zero-trust architecture)的興起。此資安架構要求，無論使用者與裝置位於何處，都必須先經過驗證，才能獲准存取資源。現代化的身分與存取管理(IAM)解決方案，是確保僅有經授權人員能存取正確系統的關鍵所在。

有效的政策控管，取決於對使用者身分是否具備足夠的信任度；若無法確信使用者的真實身分，便無法授予存取權限。隨著零信任(ZeroTrust)原則日益普及，這樣的信任更顯得至關重要。零信任原則要求，必須持續重新評估每一次存取請求的脈絡背景與使用者身分，藉此降低風險並維持資安防護。

Broadcom的IAM產品組合，數十年來始終位居市場領導地位，涵蓋自CA Technologies與Symantec併購而來的產品線，過去始終著重於強固的資安防護。如今，我們的IAM策略則以提供靈活性、營運效率，以及簡化使用者互動體驗為核心。Broadcom的策略，支援組織在演進與轉型過程中持續前行。

我們已運用雲原生(cloud-native)、微服務架構(microservice-based)，以及對DevOps友善的容器驅動能力，將整體技術堆疊完成現代化升級，得以迅速因應不斷變化的驗證與授權需求。此產品組合，如今已涵蓋針對使用者、裝置與軟體的進階驗證機制，並採用FIDO2、Passkeys、WebAuthN、OIDC與OAuth等標準。這些解決方案橫跨從行動裝置到大型主機的各類平台，提供整合式風險評估以支援零信任(Zero Trust)架構，並針對企業與外部應用程式，納入即時到職開通(just-in-time onboarding)與自帶身分驗證(bring-your-own-identity)機制。

客戶正積極透過Broadcom轉型其IAM解決方案，以達成以下目標：

- 在符合法規要求的同時，強化資安防護與客戶信心
- 作為政府資安倡議的一環，提升品牌聲譽
- 透過雲原生(cloud-native)驗證機制，實現現代化消費者應用程式

特權身分與憑證遭入侵，是導致資料外洩得逞的主要原因之一，促使監理機關要求針對特權存取採取更嚴格的控管措施。Symantec特權存取管理(PAM)軟體透過安全管理機敏系統管理憑證的存取，並在授予特權存取權限之前，要求進行雙因子驗證以核實使用者身分，藉此緩解此一風險。此解決方案落實以政策為基礎的控管機制，限制每位使用者可存取的憑證範圍，確保最小權限原則的落實，並約束超級使用者(superuser)活動。此外，Symantec PAM軟體會持續監控並記錄所有特權操作，將各項操作與個別使用者相互連結，藉此強化課責機制，並透過詳盡的稽核軌跡與報告，支援法規遵循要求。

安全遷移至雲端

運用雲原生資安防護與SaaS防護

組織必須在雲端環境中保護資料與使用者的安全。Symantec CloudSOC® CASB軟體，是業界領先的雲端存取安全代理(CASB)解決方案，專為提供SaaS應用程式的深度可視性與控管能力而設計，確保敏感資料無論存放於何處，皆能受到妥善保護。此軟體可直接整合Microsoft 365、Google Workspace、Workforce、Slack與Salesforce等主流SaaS平台；Symantec CloudSOC CASB軟體並提供精細的政策執行、使用者行為分析以及即時威脅防護能力。透過此項整合，組織得以偵測影子IT(shadowIT)、防止資料外傳(滲出／竊取)，並在日益成長的雲端服務組合中維持合規，同時不影響使用者的工作效率。

在網路邊緣，Symantec Secure Web Gateway(安全網路閘道，SWG)軟體，於保障使用者存取網際網路與雲端應用程式的安全上，扮演著關鍵角色。Symantec SWG軟體可部署於雲端或內部部署環境，即時檢測網頁流量，對網站進行分類與歸類，封鎖惡意內容，落實可接受使用政策，並防範進階威脅。當與Symantec CloudSOC CASB軟體搭配使用時，Symantec SWG軟體可將防護範圍延伸至受管理與未受管理的裝置，為分散式員工提供安全的存取能力。透過整個平台共享的統一政策管理與威脅情資，組織得以確保無論使用者從何處連線，都能維持一致的政策執行與可視性。

透過Symantec CloudSOC CASB軟體與Symantec SWG的相互搭配，Broadcom提供端對端的雲端資安解決方案，保護SaaS與IaaS環境。此解決方案，以數十年來始終定義Symantec軟體核心價值的信任為根基，賦能企業安全地推動創新。

保護 VMware Cloud Foundation®

VMware Cloud Foundation®(VCF)是企業推動應用程式現代化、加速導入混合雲，並持續掌控關鍵任務工作負載的可信賴平台。Broadcom併購VMware，為客戶開啟了嶄新機會，得以部署一套安全的端對端私有雲基礎，於整個環境中整合強固的基礎架構與進階資安防護。

為保護VCF平台，組織可運用Broadcom整合式資安解決方案，強化威脅預防、存取控管、安全API管理，並確保符合當今複雜雲端環境的合規要求。

在差異化資安產品組合所提供的能力方面，競爭對手難以望其項背：

- **端點防護**：Symantec Endpoint Protection可與VMware® vShield Endpoint整合，為虛擬機器提供免代理程式(agentless)的防毒與惡意程式防護。透過使用vShield manager，組織無需每部虛擬機器中都部署資源密集的代理程式，即可實現全面的端點資安防護。此解決方案可即時偵測威脅並自動修復，大幅降低VCF工作負載所面臨的風險。
- **工作負載防護**：Carbon Black Workload與VMware vSphere® 軟體緊密整合，針對勒索軟體與無檔案式(Fileless)攻擊等威脅，提供進階的預防、偵測與回應能力。此軟體運用行為分析與威脅情資，持續執行風險評鑑與資安衛生監控，其原生整合架構可實現快速、高效且低額外負擔的工作負載防護。Layer7™ API Gateway軟體則進一步透過強固的驗證、授權、政策控管與完整分析能力，保護VCF的API安全，防範關鍵應用程式核心架構遭受資料外洩與網路威脅侵害。
- **身分防護**：雲原生(cloud-native)架構的Symantec VIP Authentication Hub軟體，針對 VCF 私有雲中執行的應用程式，提供可擴充的第一與第二階段驗證，以及政策協作能力。Symantec PAM軟體透過在加密儲存區中管理管理員憑證，保護VMware vCenter® 的存取安全，符合零信任(Zero Trust)要求，並保護資源免於未經授權的存取。Broadcom API閘道，則透過提供雲端自動化與協作作業所需的精細存取控管與稽核能力，強化VCF對API安全的管理。
- **資料防護**：Symantec資料外洩防護(DLP)平台、Symantec CloudSOC CASB軟體以及零信任網路存取(Zero Trust Network Access)政策，可直接延伸至VMware私有雲與混合雲部署環境。這些解決方案落實資料分類、監控使用者與裝置行為、防止未經授權的分享，並確保虛擬機器、容器或雲原生應用程式所使用之靜態、傳輸中及使用中敏感資料，皆能符合法規遵循要求。與vDefend等VMware原生資安服務的整合，可實現跨分散式環境的資料保護規則協同執行。

透過Broadcom，資安防護是私有雲與生俱來的內建能力，而非事後追加的附加功能。Broadcom資安軟體提供更強固的防護、簡化的維運作業，以及支撐安全數位轉型的韌性基礎。此整合平台，可在快速演進的科技格局中，為企業帶來無可比擬的信任、營運效率與資安韌性。

符合政府法規要求

落實以資料為核心的資安防護

隨著法規要求日益複雜，加上資料在混合環境中的分布愈趨分散，組織需要經過驗證的解決方案，才能大規模保護敏感資訊並確保合規。業界領先的Symantec DLP平台與整個資安技術堆疊緊密整合，無論敏感資料存放於端點、雲端服務或網路之中，此平台皆能提供統一的可視性與控管能力。

透過深度內容檢測與情境感知偵測能力，Symantec DLP平台協助組織辨識並保護受監管資料，包括個人識別資訊(PII)、受保護健康資訊(PHI)，以及財務紀錄。Symantec DLP平台符合GDPR、HIPAA與PCIDSS等法規要求。業界已對此有目共睹：2025年，Broadcom獲Google Cloud評選為年度資料資安夥伴，並獲IDC評選為DLP領導廠商(Leader)，以及獲Radicati Group評選為DLP頂尖廠商(Top Player)。

雲端應用程式合規的核心，正是Symantec CloudSOC CASB軟體。我們的CASB解決方案，將Symantec DLP平台的可視性與控管能力，延伸至Microsoft 365、Google Workspace、Salesforce等SaaS平台。Symantec CloudSOC CASB軟體讓組織能夠監控使用者活動並稽核資料使用情形，於雲端環境中落實即時政策，並嚴格遵守全球及各產業特定法規。憑藉進階分析能力與AI驅動的異常偵測，Symantec CloudSOC CASB軟體能辨識具風險的雲端應用程式，以及使用者於這些應用程式中的行為，並協助分類敏感資料、套用適當的控管措施以防止資料外洩，確保使用情形同時符合內部政策與外部法規要求。

強大的資料分類能力，貫穿於Symantec DLP平台及更廣泛的Symantec產品組合之中。此資料分類能力，讓組織能依內容敏感度、使用情境與合規要求，為資料加註標籤並加以治理。這些分類設定，於雲端與內部部署環境中皆能一致執行，確保無論資料存放於何處或透過何種方式存取，敏感資料皆能受到妥善保護。無論資料處於儲存、分享或下載狀態，組織皆可確保法規遵循能持續獲得維持。

橫跨整個Symantec產品組合(DLP、CloudSOC CASB、Secure Web Gateway、Endpoint)的整合式政策執行機制，讓組織得以在每一個控管節點，自動化落實資料保護與合規要求。從防止SaaS應用程式中未經授權的資料分享，到封鎖來自未受管理裝置的高風險存取嘗試，Symantec軟體將合規要求深植於企業的營運架構之中。在法規快速演進、執法力道同時日益加強的環境下，Symantec產品組合賦能組織隨時做好稽核準備、降低合規風險，並維護客戶、監理機關與利害關係人的信任。

資料生命週期全程加密

對當今大多數組織而言，部署加密解決方案的首要理由，在於緩解潛在資料外洩事件所帶來的衝擊，並保護客戶隱私。符合「持續診斷與緩解」(Continuous Diagnostics and Mitigation)、支付卡產業資料安全標準(PCI DSS)、健康保險可攜與責任法案(HIPAA)，以及歐盟一般資料保護規則(GDPR)等法規標準，皆要求採用具可稽核性的加密機制，以保護客戶資料。一旦發生資料外洩事件，此舉可能有助於取得安全港(Safe Harbor)保護，免除高成本的揭露義務，並減輕商譽受損的程度。

Symantec PGP® 加密產品組合，透過三大核心解決方案提供強固的資料保護能力：

- **PGP Encryption Suite**：提供全磁碟與卸除式媒體加密、自動化內部電子郵件加密／解密與郵件驗證，以及檔案與資料夾的端對端加密功能，為遠端與行動使用者提供全方位保護。
- **PGP Gateway Email Encryption**：自動化電子郵件加密機制，確保敏感資訊（財務資料、健康紀錄或智慧財產）能安全傳輸，無需終端使用者介入操作，亦無需安裝用戶端軟體。
- **PGP Command Line Encryption**：保護伺服器上大量儲存資訊免於未經授權的存取，並可輕鬆整合大多數資料傳輸與處理系統，確保日常營運資料交換的安全性。

上述解決方案結合運作，可保護靜態、使用中及傳輸中的敏感資訊，同時提供集中式管理、自動化政策執行，以及無縫的合規報告功能。與 Symantec DLP 平台及 Symantec Email Security 軟體的整合，可進一步強化對抗網路威脅的防護能力。

大規模現代化威脅防禦

全球情資網路

Symantec Global Intelligence Network(賽門鐵克全球情資網路，GIN)，是Broadcom資安優勢的核心所在。此網路歷經數十年建置而成，是全球規模最大的民間威脅情資網路之一，每天持續分析來自全球企業、政府機關與消費者的數十億筆事件。此無可比擬的可視性，為客戶提供因應新興攻擊的早期預警系統，並可深入掌握對手的戰術、技術與程序(TTPs)。

Symantec GIN的獨到之處，在於其能夠統整涵蓋端點、網路、雲端與電子郵件資安層級的遙測資料。Symantec GIN將來自Symantec與CarbonBlack端點、Symantec網路與網頁閘道、雲端資安服務，以及全球電子郵件防護的訊號相互關聯，將原本看似孤立的事件串聯起來。這種脈絡豐富的情資，讓系統得以更早偵測到複雜的多重攻擊向量攻擊。

Symantec GIN所做的不僅止於蒐集資料，更將其轉化為可據以行動的洞察。系統運用AI與進階分析技術，將原始遙測資料萃取為威脅指標、信譽評分與偵測模型，並持續更新、推送至Symantec與Carbon Black的各項解決方案之中。這代表每一位客戶，都能受惠於此網路的集體情資，往往能在威脅實際影響其環境之前，即予以攔截封鎖。

憑藉如此廣闊的視野，Symantec與Carbon Black解決方案能在威脅模式浮現後數秒之內，即辨識出新型攻擊行動。無論是新興威脅或普遍存在的威脅，此能力皆能帶來極大優勢。

歸根究柢，Symantec GIN是驅動預防能力與韌性的核心引擎。透過打通不同資安領域之間的可視性，Symantec與CarbonBlack解決方案得以提供更準確的偵測結果、降低誤判(false positive)，並協助組織加快回應速度。這正是核心差異化優勢，確保Symantec與Carbon Black解決方案，始終是全球組織信賴之選的防護方案。

整合式情資與自動化

複雜的IT環境，已使得情資與自動化成為任何資安技術堆疊不可或缺的必備元件。兩者皆已內建於Broadcom資安產品組合之中，提供以下能力：

- **AI 驅動分析：**運用AI與機器學習(ML)，Carbon Black與Symantec端點產品組合提供具備深度脈絡的整合式告警，讓資安團隊得以縮短平均偵測時間與平均回應時間。
- **串聯預防、偵測與回應：**將多項端點資安能力整合於單一平台之中，可讓預防、偵測與回應工作流程無縫銜接，並讓Symantec CloudSOC CASB團隊在需要進一步資訊時，能迅速從告警轉入調查作業。
- **SOAR整合：**將端點資安資料與回應動作，與資安協作、自動化與應變平台(SOAR)相互整合，可實現資料蒐集與情資強化等重複性人工流程的自動化。舉例來說，透過將Carbon Black Cloud Live Response與SOAR平台整合，分析人員可在調查過程中自動執行端點查詢，無需逐一手動查詢各個端點，即可取得所需的完整資訊。
- **威脅情資強化：**進一步運用來自Broadcom GIN的威脅情資加以強化，讓團隊得以將自身環境中所觀察到的情況，與來自更廣泛威脅態勢的即時洞察相互連結。憑藉事件預測等AI驅動能力，資安團隊無需採取任何人工操作，即可攔截依循已知攻擊鏈(Kill Chain)進行中的攻擊行動。

因應遭忽視的弱點風險

在當今遠端與混合作業環境下，IT團隊承受著日益沉重的壓力，須管理並保護不再受限於傳統辦公室網路的端點。所面臨的挑戰不勝枚舉：在無現場支援的情況下佈建新裝置、維持一致的組態設定、確保及時完成修補程式套用，以及掌握分散式員工的整體可視性。為因應這些需求，組織需要與精簡團隊同樣靈活且具擴充性的工具。

Symantec Endpoint Management產品組合，提供專為因應上述挑戰而設計的解決方案，協助IT團隊超前部署。此產品組合透過兩大核心解決方案，於遠端、混合與辦公室內環境中，提供強固的集中化控管能力：

- **Symantec GHOST® Solution Suite**：此解決方案協助部署筆記型電腦、桌上型電腦與伺服器，支援Windows、Windows Server，以及多種Linux發行版本。組織可透過中央管理主控台佈建新裝置，並藉由一致化的部署方式，確保裝置所佈建的映像檔皆具備最新的資安更新與組態設定，藉此降低弱點風險、強化資安防護。
- **Symantec IT Management Suite**：此解決方案透過為組織提供廣泛且近乎即時的IT維運全貌可視性，管理端點的整個生命週期。Symantec IT Management Suite憑藉強固的修補程式管理能力，偵測並修復已知弱點，藉此強化端點防護。此解決方案同時透過自動化筆記型電腦、桌上型電腦與伺服器(無論位於防火牆內或防火牆外)的部署、軟體安裝與庫存彙整流程，降低整體成本。最後，此解決方案透過終端使用者自助服務，將生產力與使用滿意度提升至最大化。

Symantec Endpoint Management產品組合，針對網路內與網路外裝置等多元環境，提供安全的管理能力，實現一致的組態設定、快速的威脅回應，以及最佳化的軟體派送作業。Symantec GHOST Solution Suite可實現與硬體無關的映像處理、裸機部署，以及遠端佈建能力；Symantec IT Management Suite則透過自動化修補程式派送、即時裝置可視性、資產庫存管理、免代理程式(agentless)管理，以及自助服務入口網站，與前者相輔相成。最終成果，是一套強固、統一的端點管理解決方案，協助精簡的IT團隊降低成本、提升靈活性，並維持生產力與安全的遠端工作團隊。

結論

在當今快速演進的科技格局中，資安挑戰較以往更為複雜。Broadcom擁有以Symantec、Carbon Black與CA Technologies軟體實力為基礎的獨特產品組合廣度，針對現代網路資安挑戰，提供全面且整合的因應之道。Broadcom的資安軟體，運用進階端點防護、零信任(Zero Trust)身分與存取管理、業界領先的資料外洩防護、API安全，以及雲原生(cloud-native)防禦能力，為企業提供無可比擬的防護能力。

我們對創新的堅持承諾，確保能持續走在新興威脅之前，透過AI驅動的分析與自動化能力，減輕貴組織資安團隊的負擔。透過Broadcom，您可以確信貴組織已具備所需工具，能安全因應數位經濟的種種複雜挑戰。

誠摯邀請您進一步了解我們的解決方案，探索Broadcom如何協助貴企業打造具備韌性且安全的基礎。歡迎立即與我們聯繫，深入了解更多資訊、預約產品展示，或與我們的專家團隊交流。

讓我們攜手打造安全的未來。

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併入全球網路晶片巨擘—博通(Broadcom)，美國股市代號AVGO，全世界網路流量有99.9%經過博通的網路晶片。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統整合擴充性，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諮詢對象。