

白皮書

以資安為本

Broadcom®
金融服務產業藍圖



以資安為本

Broadcom® 金融服務產業藍圖

目錄

執行摘要

金融服務業態勢

金融服務暨保險業(FSI)組織所面臨之關鍵挑戰

抵禦進階網路威脅的韌性

保護雲端環境

為安全資料交換提供API防護

符合法規要求

結論

執行摘要

隨著金融機構擁抱數位轉型，也正面臨網路威脅與法規複雜度日益升高的新時代。Broadcom®全方位資安套件，讓這些組織具備因應挑戰的能力——保護API、身分、端點與資料——同時實現合規與營運持續性。

金融服務業態勢

科技始終是驅動金融服務暨保險業(FSI)成長與創新核心力量。身為數位轉型的先驅，FSI組織已重塑其商業模式與服務交付方式，帶動數位經濟持續演進。然而，IT環境的現代化，雖然是創新與營收成長不可或缺的要素，卻同時也擴大了攻擊面，並提高資安與合規風險。

金融服務暨保險業(FSI)組織所面臨之關鍵挑戰

- **進階網路威脅**：金融機構日益成為高度複雜攻擊的鎖定目標，包括AI驅動的惡意軟體、深度偽造(Deepfake)詐欺，以及高度針對性的社交工程與網路釣魚(Phishing)手法。勒索軟體(Ransomware)——經常採用雙重勒索(Double Extortion)手法——如今更已威脅到支付系統、核心銀行業務與資金操作。
- **雲端弱點**：轉向雲端與數位服務的過程擴大了攻擊面，讓組織暴露於不安全的雲端存取，以及包括驗證機制失效、權杖外洩與輸入驗證缺陷等API弱點風險之下。在確保混合多雲環境安全的同時，仍須符合資料所在地要求與雲端服務供應商風險管理標準，此仍是持續存在的挑戰。
- **安全資料交換**：金融機構日益仰賴API，驅動數位銀行、支付與開放銀行(open banking)倡議中的資料交換作業，但這種以API為核心的架構，也帶來重大資安風險。一旦遭到入侵，暴露在外的API可能成為攻擊者的入侵切入點，導致財務損失、法規裁罰與商譽損害。
- **合規複雜度與法規變動**：各法域快速演進的法規要求，涵蓋嚴格的資料保護、資料外洩通報、韌性測試，以及第三方廠商監督機制。即使是最先進的資安計畫，也必須落實隔離、加密與多重驗證(MFA)機制，並在稽核與董事會審查過程中維持透明度。

Broadcom關鍵資安技術 ，專為直接因應金融服務 暨保險業(FSI)組織所面 臨之挑戰而設計

本白皮書將深入探討，Broadcom關鍵資安技術如何專為直接因應這些挑戰而設計。

抵禦進階網路威脅的韌性

當今的網路攻擊者運用AI、網域偽造(domain spoofing)與混淆技術，藏匿惡意連結，使得魚叉式釣魚攻擊(Spear Phishing)、勒索軟體(Ransomware)與商業郵件詐騙(BEC)等威脅，變得既普遍又難以偵測。金融機構面臨以下數項關鍵挑戰：

- 高度精密的社交工程手法
- 規避式惡意軟體與零時差(zero-day)攻擊利用
- 遭入侵帳戶的使用日益增加
- 刻意設計以繞過傳統資安解決方案的複雜攻擊鏈(Kill Chain)

電子郵件型攻擊防禦

Symantec® Email Security.cloud(ESS)是一套先進平台，可強化原生電子郵件防禦能力並降低誤判(false positive)。ESS運用即時連結分析、雲端沙盒分析、點擊時保護(click-time protection)、隔離機制，以及全球威脅情資，針對電子郵件型威脅提供全方位防護。

勒索軟體防禦

Symantec特權存取管理(PAM)軟體，於伺服器核心層級落實精細的主機層級控管措施——即使面對root層級攻擊亦然。此做法可消弭多種勒索軟體攻擊向量，並實現快速的事件應變。

遭入侵帳戶防禦

Broadcom身分與存取管理(IAM)，針對使用者、裝置與軟體提供進階驗證機制，確保憑證獲得強力保護。其雲原生(cloud-native)、對DevOps友善的架構，能迅速因應不斷變化的需求，為多元企業需求提供現代化身分網路。

相關案例包括：

- 一家財星100大(Fortune 100)金融機構，在符合合規要求的同時，強化資安防護與客戶信心
- 一家歐洲財富管理機構，透過雲原生(cloud-native)驗證機制，實現現代化消費者應用程式

保護雲端環境

隨著組織轉向混合雲與私有雲環境，保護這些生態系——以及連結其間的API——已成為至關重要之事。Broadcom併購VMware，得以在私有雲中實現全面的端對端資安防護：

- **端點防護**：Symantec Endpoint Protection與VMware vShield Endpoint整合，為虛擬機器提供免代理程式(agentless)的防毒與惡意軟體防禦，將資源額外負擔降至最低，並自動化執行修復作業。
- **工作負載防護**：Carbon Black® Workload與VMware vSphere®整合，針對勒索軟體與無檔案式(Fileless)威脅，提供進階的預防、偵測與回應能力，並由持續性資安衛生監控與行為分析提供支援。
- **API與身分安全**：Layer7™ API Gateway透過強固的驗證與政策控管機制，保護VMware Cloud Foundation® (VCF) 的API安全。Symantec Identity Security Platform與Symantec PAM，則針對雲端應用程式與管理主控台，提供可擴充的驗證與特權存取保護。

API是現代金融基礎架構
的核心骨幹

- **資料防護**：Symantec DLP、CASB與零信任網路存取(ZTNA)，落實資料加密與分類，監控使用者與裝置行為，並針對傳輸中、靜態及使用中的敏感資料，提供協同一致、以政策為導向的控管機制。

資安防護是私有雲與生俱來的內建能力，提供強固的防護、精簡的維運作業，以及支撐持續數位轉型的韌性基礎。

為安全資料交換提供 API 防護

API是現代金融基礎架構的核心骨幹，支援從行動銀行、支付處理，到開放銀行(open banking)平台與第三方金融科技整合等各項應用。隨著金融機構致力於提供無縫的數位體驗，並符合PSD2與全球開放銀行倡議等法規要求，API已成為連結傳統系統與創新服務不可或缺的橋樑。然而，這種以API為核心的做法，也帶來重大資安風險，因為這些介面經常掌管極為敏感的金融資料。一旦API遭到入侵，可能導致重大財務損失、法規裁罰，以及長遠的商譽損害。

為因應這些風險，金融級API(FAPI)框架，樹立了保護高風險金融交易與資料交換的標竿。FAPI Advanced資安設定檔，透過採用預先因應個別資安層級潛在突破情形的縱深防禦策略，進一步強化防護能力。

Broadcom Layer7 API Security解決方案，賦能組織依循上述標準保護其API安全。Layer7作為控制層，負責管理驗證與授權、防禦OWASP API資安十大漏洞、支援進階資安設定檔、落實政策，並根據身分屬性、裝置狀態與作業情境，實現精細授權。此解決方案同時提供速率限制與配額管理，防止API濫用與阻斷服務(DoS)攻擊。此外，Symantec PGP®命令列工具可與商用及客製化資料傳輸系統無縫整合，提供多樣化的加密選項，確保無論收件方具備何種能力，皆能安全傳輸資料。

符合法規要求

金融服務暨保險業(FSI)組織面臨日益複雜的威脅，包括不斷擴大的數位攻擊面、升高的第三方風險，以及日益嚴苛的合規義務。形塑此產業的主要法規，包括一般資料保護規則(GDPR)、紐約州金融服務署規範(NYDFS)、支付卡產業資料安全標準(PCI DSS)、支付服務指令第二版(PSD2)、加州消費者隱私法(CCPA)，以及數位營運韌性法(DORA)，另外還有其他涉及事件通報、隱私保護與營運韌性之相關法規要求。

Broadcom資安產品符合
產業合規要求

表1：影響金融服務業之關鍵法規要求

法規	地區／適用範圍	影響
GDPR	歐盟／全球	資料隱私、資料外洩通報、跨境資料控管
NYDFS	美國(紐約州，並作為其他州之範本)	資安計畫、風險評鑑
PCI DSS	全球	支付資料、加密、存取控管
PSD2	歐盟	透過安全API開放銀行系統、多重驗證(MFA)
CCPA	美國(加州)	隱私保護、資料外洩通報、消費者權利
DORA	歐盟	營運韌性、事件通報、韌性測試

Broadcom統一式做法， 簡化資安管理

以下說明Broadcom解決方案如何對應資安與合規要求：

表2：Broadcom 資安產品與合規要求對照表

產品	關鍵功能	GDPR	NYDFS	PCI DSS	PSD2	CCPA	DORA
Identity and Access Management	多重要素驗證、集中式角色型管理、可供稽核之控管措施	✓	✓	✓	✓	✓	✓
Layer7 API Security	防禦OWASP API資安十大漏洞	✓	✓	✓	✓	✓	✓
Symantec Control Compliance Suite	針對逾100項法規、要求與最佳實務框架，提供資安合規評鑑	✓	✓	✓	✓	✓	
Symantec Email Security	沙盒分析、網路釣魚/商業郵件詐騙(BEC)防護、DLP	✓	✓	✓	✓	✓	
Symantec IT Management Suite	端點生命週期與修補程式管理、裝置合規性、快速威脅回應		✓	✓			✓
Symantec PGP Encryption	AES-256/PGP靜態資料及傳輸中資料加密、政策導向控管、詳細記錄檔	✓	✓	✓	✓	✓	

透過整合上述解決方案，金融服務組織得以更有效地管理身分與存取、於各通路確保資料安全、防範端點威脅，並持續掌握不斷演變的法規要求。此全方位做法，協助機構同時緩解網路風險與合規風險，確保更高的韌性與營運信心。

結論

與Broadcom攜手合作，賦能金融服務組織自信因應當今複雜的資安與合規格局。Broadcom整合式產品組合，針對身分、端點、資料與API提供進階防護，同時精簡法規遵循與營運韌性作業。憑藉能因應複雜威脅、雲端弱點與不斷演變之法規要求的解決方案，機構得以保護關鍵資產，並維護客戶與利害關係人的信任。

Broadcom統一式做法，簡化資安管理、降低風險，並支援無縫的數位轉型。透過將強固的資安防護，深植於金融生態系的每一層級——包括私有雲與混合雲環境——Broadcom讓組織得以專注於創新與成長，並對自身防禦實力與合規態勢的可靠性充滿信心。

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安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。

