

Symantec® Content Analysis

導入最先進雲端沙箱防禦系統，
強大的投資效益立竿見影



目錄

代理伺服器與多層式威脅分析，加上雲端企業級沙箱防護

進階威脅防護：代理伺服器架構為何勝過次世代防火牆

代理伺服器架構＝更完善的防護

運用 ProxySG、Content Analysis 與沙箱技術，獲得更完善的防護

強大的實際成效

為何循序漸進的雲端導入策略最為理想

您是否善用了雲端與地端資安的雙重優勢？

為何信賴賽門鐵克解決方案，助您邁向雲端？

地端、雲端，或介於兩者之間——選擇權在您手中

結論

代理伺服器與多層式威脅分析，加上雲端企業級沙箱防護

隨著進階威脅日益增加，整合式資安防護方式已成為關鍵。若您正考慮遷移至雲端，在篩選最能保護企業資訊的資安方案時，這項課題可能會變得更加重要。

審慎評估各項方案是明智之舉。我們都聽過資料外洩事件所造成的實質金錢損失，但外洩事件發生時，同樣會衝擊企業品牌形象。Ponemon 機構的研究發現，資料外洩事件公布當天，企業平均股價會下跌 5%，客戶流失率達 7%，且有 27% 的消費者曾終止與發生外洩事件之企業的往來關係。

有鑑於這些數據，無論您考慮將部分或全部基礎架構遷移至雲端，保護資料安全都是重中之重。在本文中，我們將深入探討，無論您邁向雲端的腳步快慢，該如何為您的資訊提供最佳保護。內容涵蓋代理伺服器架構與次世代防火牆（NGFW）的比較、為何在遷移至雲端時仍須保留企業級威脅防護，以及可考慮的部署選項。

進階威脅防護：代理伺服器架構為何勝過次世代防火牆

次世代防火牆在企業資安環境中確實有其定位。舉例來說，次世代防火牆能有效根據 IP 位址或地理位置，阻擋透過特定通訊協定進行的非預期網路通訊，也能控管並鎖定企業內部對外連接網際網路的多重通訊管道。若您願意承受效能大幅下降的代價，甚至可將這些功能延伸至簡易的串流式惡意程式掃描。然而，若論及網頁流量的資安防護，以及保護企業免受進階攻擊、零時差威脅與精密惡意軟體侵害，沒有任何技術比得上代理伺服器架構。

以下範例說明代理伺服器架構在抵禦惡意程式方面，為何比次世代防火牆更為有效：

要達到有效的威脅防護，
流量必須對資安工具可
視，以利分析與檢測；但
與此同時，企業組織仍須
遵守法定的隱私保護政策

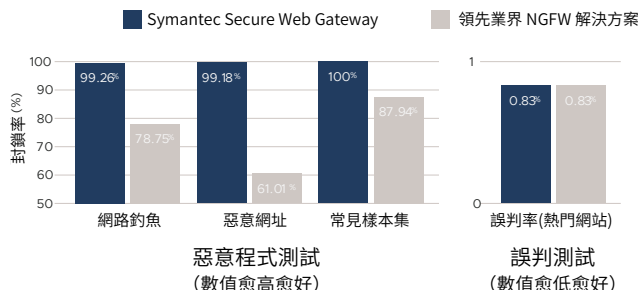
- **完整檔案重組，揪出真實身分：**次世代防火牆採串流式架構，因此容易受到規避型惡意程式所矇騙。相較之下，代理伺服器會先重組完整的工作階段及其內容，才會傳送給使用者。這種做法會先重組通訊內容與檔案，判定是否具有危害性，才會送往最終目的地。
- **檔案在判定結果出爐前暫不放行：**代理伺服器可暫扣檔案，直到所有封包全數蒐集、組合完畢，並運用多種檢測與分析方法，比對所有可用的威脅情資進行檢視。唯有判定安全無虞後，檔案才會送往預定目的地。
- **安全且可擴充的加密流量處理能力：**對許多企業而言，加密資料可能占網路流量的60%至70%以上。這類資料也日益成為攻擊者藏匿惡意活動的媒介。要達到有效的威脅防護，流量必須對資安工具可視，以利分析與檢測，但與此同時，企業組織仍須遵守法定的隱私保護政策。
此外，一份近期學術論文比較了多款加密流量檢測工具（包括次世代防火牆及其他串流式工具）攔截加密流量的成效。報告發現，幾乎所有工具都會降低資安防護水準，甚至有多款工具引入了嚴重的安全弱點。在受測產品中，僅有 Symantec® ProxySG 獲得 A 等評等，其餘產品則全數僅獲得 C 或 F 等評等。
- **代理伺服器封鎖成效更佳：**論及完整工作階段終止、解密與檢測能力，代理伺服器架構完勝。一份比較 Symantec Secure Web Gateway 與領先業界 NGFW 解決方案的 Tolly 報告清楚顯示，代理伺服器架構在網頁資安防護方面的效果遠勝於次世代防火牆。在網路釣魚、惡意網址，以及常見已知惡意程式等多項惡意程式測試項目中，Symantec Secure Web Gateway 的防護成效遠遠勝過領先業界的 NGFW 產品。

Tolly 報告發現，Symantec Secure Web Gateway 具備以下優勢：

- 在各類受測威脅中均展現優異的偵測率
- 由業界規模最大的即時情資饋送所支援的優異惡意程式資料庫
- 對規避技術具備卓越的偵測能力
- 提供更多防惡意程式引擎與沙箱技術選項

圖1：Tolly 報告發現，相較於領先業界的次世代防火牆解決方案，Symantec Secure Web Gateway 在各類受測威脅中均展現優異的偵測能力。

Symantec Secure Web Gateway 對比領先業界 NGFW 解決方案
網頁資安防護成效



Symantec Secure Web Gateway附註：「封鎖」類別已盡可能採相似設定進行配。Symantec 允許更精細的封鎖層級設定。

資料來源：Tolly，2017年3月

賽門鐵克解決方案以代理伺服器架構的優勢為基礎，透過多層式防護方式，將 ProxySG、Symantec Messaging Gateway 與 Symantec Endpoint Protection 所擷取的內容，送往 Symantec Content Analysis 進行分析，藉此提供進階威脅防護，高效揪出網頁或郵件流量中的惡意活動。

代理伺服器架構＝更完善的防護

採用賽門鐵克解決方案的代理伺服器架構	次世代防火牆
優異的惡意程式掃描與防護能力： ・流量終止處理 ・多廠商開放生態系	無法終止流量並進行檢測： ・單一廠商架構 ・容易遭到繞過
輕鬆加入串接式資料外洩防護 (DLP)	無法終止流量並加入串接式資料外洩防護 (需仰賴代理伺服器)
SSL 解密功能，支援業界領先的加密演算法	加密演算法支援有限，且效能將下降 60% 以上
市場領先的雲端存取安全代理 (CASB) 控管能力	僅提供 API 防護，不具備串接式 CASB 能力
免硬體雲端服務，可支援漫遊使用者或整個辦公室	漫遊使用者的防護需透過VPN回程連接至客戶自建／自有防火牆
市場領先的端點整合能力： ・入侵指標 (IoC) 驗證、黑名單管理與修復	修復能力有限，且不具備端點管理功能

運用 ProxySG、Content Analysis 與沙箱技術，獲得更完善的防護

賽門鐵克解決方案以代理伺服器架構的優勢為基礎，透過多層式防護方式，將 ProxySG、Symantec Messaging Gateway 與 Symantec Endpoint Protection 所擷取的內容，送往 Symantec Content Analysis 進行分析，藉此提供進階威脅防護，高效揪出網頁或郵件流量中的惡意活動。系統會先運用檔案信譽服務、雙重防惡意程式引擎與進階機器學習進行處理，僅有真正無法辨識的未知檔案，才會送往沙箱進行完整引爆分析。

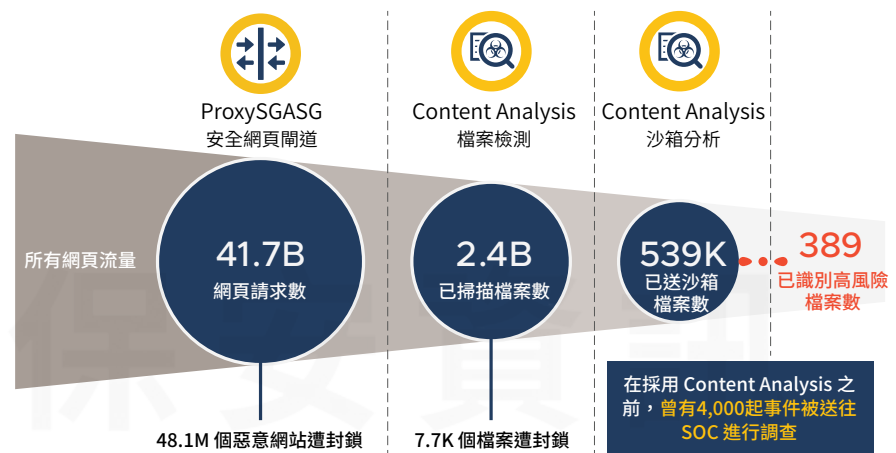
圖2說明某客戶如何透過這種做法獲得實際成效。在此範例中，這家財星20大企業客戶在30天內收到近420億筆網頁請求。賽門鐵克技術以多階段流程分析所有請求，最終篩選出僅389個需要進一步調查的高風險檔案。

強大的實際成效

財星20大企業

圖2：某客戶在30天內收到數十億筆網頁請求，但究竟哪些需要進一步調查？ProxySG、Content Analysis 與沙箱技術三者結合，將請求篩選至僅389個需要資安團隊調查的檔案。

分析師指出，資安專業人員若採取混合式做法，同時部署雲端資安與地端資安，將可獲得顯著優勢



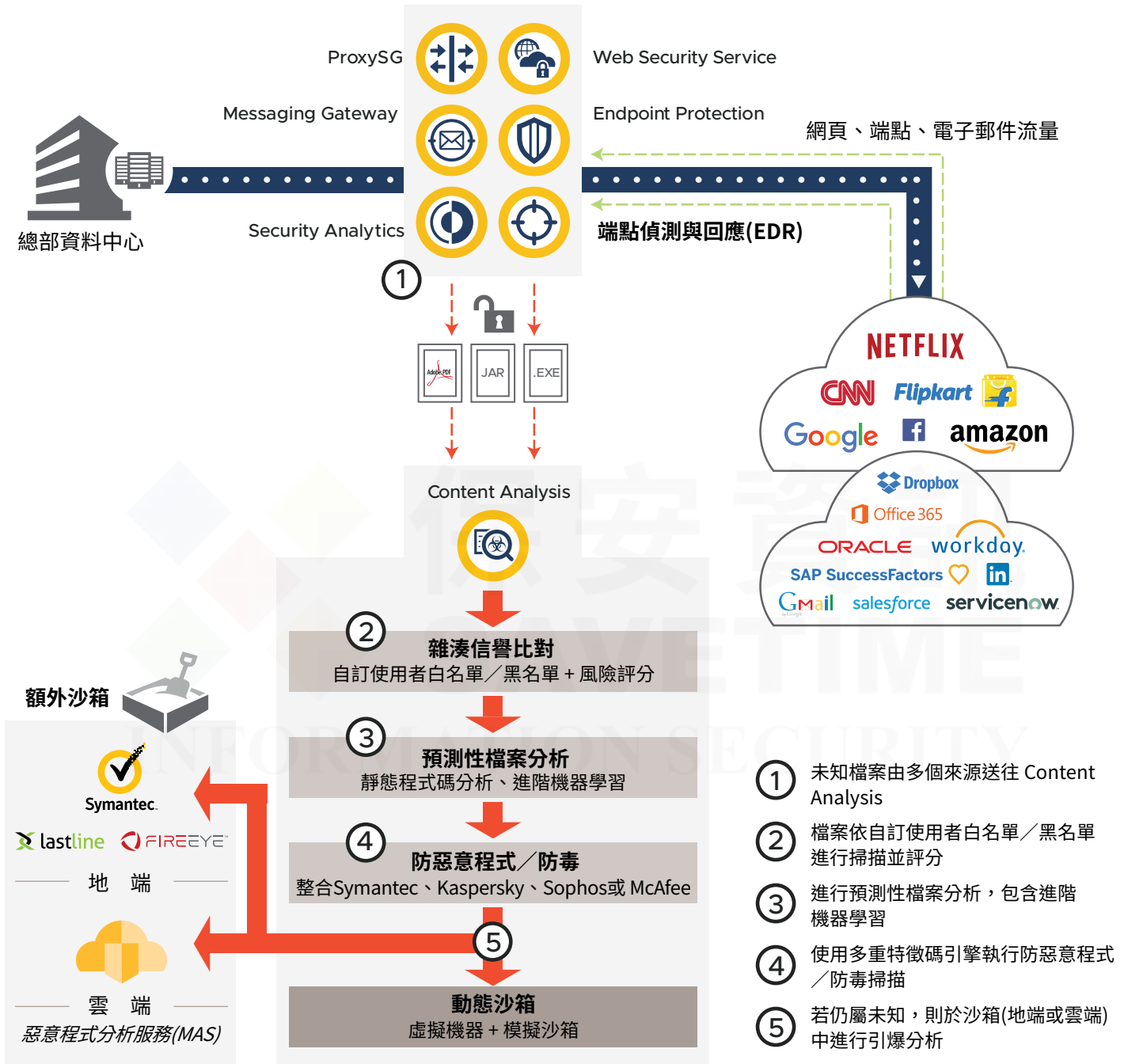
*財星20大企業客戶30天實際流量

為何循序漸進的雲端導入策略最為理想

您可能對遷移至雲端存有多重疑慮，包括被迫採取全有或全無的做法，或必須降低資安防護的期望。您可能也擔心生產力與效能能否維持，因為您不希望IT管理者與資安分析師，白白浪費過去在現有技能、流程、政策或整合方面辛苦累積的投資成果。

企業組織都看見遷移至雲端的價值，但在資安方面，許多企業尚未準備好全面投入。政策、效能、法規及其他要求，可能都需要您以更審慎的步調遷移至雲端。正因如此，我們認為依照您自己的步調、在準備就緒時採取行動至關重要，而循序漸進的做法正是最理想的策略。分析師指出，資安專業人員若採取混合式做法，同時部署雲端資安與地端資安，將可獲得顯著優勢。

圖3：ProxySG 詳細檢視網頁流量後，Content Analysis 會依據雜湊信譽與進階機器學習，分析該流量中的任何檔案，接著使用雙重防毒／防惡意程式引擎掃描惡意程式與病毒。若仍有無法辨識的未知檔案，則會送往動態沙箱進行進一步分析。



Broadcom是全球企業信賴的資安廠商，賽門鐵克解決方案更在多項資安領域居於領導地位，包括安全網頁閘道、資料外洩防護、雲端存取安全代理(CASB)、電子郵件安全、端點安全，以及加密流量管理

您是否善用了雲端與地端資安的雙重優勢？

無論您採取地端、混合式，或全雲端策略，Broadcom都能提供優異的解決方案，安全守護您的企業。您期待在地端環境中獲得企業級的進階威脅防護，而遷移至雲端時，也沒有理由降低您的資安防護標準。所幸，賽門鐵克解決方案能提供以下能力：

- 彈性化政策執行——可接受使用範圍與風險緩解
- 地端設備與雲端共用的共通政策
- 市場領先的網址分類／歸類能力
- 高效能／高輸送量
- 身分驗證
- SSL 解密
- 影子IT可視性與控管
- 網頁隔離技術，安全瀏覽未知網站
- 業界規模最大的民用威脅情資網路
- 多重惡意程式掃描引擎
- 雙重偵測（虛擬機器與模擬）沙箱技術
- 全方位報告與可視性

為何信賴賽門鐵克解決方案，助您邁向雲端？

Broadcom 是全球企業信賴的資安廠商，賽門鐵克解決方案更在多項資安領域居於領導地位，包括安全網頁閘道、資料外洩防護、雲端存取安全代理（CASB）、電子郵件安全、端點安全，以及加密流量管理。

然而，多數資安廠商僅提供各自獨立的資安解決方案，但雲端環境需要的是全新的整合式資安模式。Symantec Cloud Security Platform 提供獨特的方式，可安全地推動雲端導入，同時整合雲端與傳統地端環境，實現無縫接軌的資安防護。

由龐大的賽門鐵克全球情資網路（Global Intelligence Network）所驅動的優異威脅情資，提供整合式網路防禦，實現無可比擬的可視性與防護能力。藉由運用雲端龐大的運算能力，我們得以分析超過37億行遙測資料，這是業界範圍最廣、深度最深的威脅情資資料集。

圖4：Symantec 全球情資網路(Global Intelligence Network)針對端點、電子郵件與網頁流量，提供無可比擬的可視性，可發掘並封鎖原本可能無法偵測到的進階目標式攻擊。

無論您選擇採取哪一種做法，這些業界領先的賽門鐵克服務均採雲端化設計，可支援您企業的資安需求



地端、雲端，或介於兩者之間——選擇權在您手中

無論您是想先小心試水溫，還是直接全力投入——選擇權都在您手中。無論選擇哪一種方式，賽門鐵克解決方案都能確保這片水域安全無虞。無論您選擇採取哪一種做法，這些業界領先的賽門鐵克服務均採雲端化設計，可支援您企業的資安需求：

- 代理伺服器／Web Security Services
- 資訊保護
- CASB（雲端存取安全代理）
- 網頁隔離
- 雲端工作負載防護（IaaS）
- 沙箱技術
- 端點防護
- 電子郵件
- 身分識別

Content Analysis 搭配 ProxySG、Symantec Messaging Gateway 或 Symantec Endpoint Protection 使用時，可封鎖已知威脅、來源與特徵碼，並集中分析未知內容

以下是我們依您環境需求所建議的解決方案組合：

- 若您整個組織選擇採用地端部署，建議採用 ProxySG 與 Content Analysis，並搭配專屬的 Content Analysis 設備配置沙箱功能。
- 若您的主要據點／使用者選擇採用混合式做法，建議採用 ProxySG、Content Analysis，並搭配雲端輔助沙箱技術。至於遠端據點／使用者，則建議採用 Web Security Services 與 Malware Analysis Service 進行沙箱防護。
- 若您希望將整個組織遷移至雲端，建議選擇 Web Security Service 與 Malware Analysis Service 進行沙箱防護。

擔心管理這些解決方案會影響 IT 團隊的生產力嗎？透過 Symantec 共通政策 (Universal Policy)，您可以在單一位置設定並管理政策，涵蓋您的資料中心、遠端與分支機構，以及行動使用者。共通政策提供惡意程式掃描、網址與風險評分、SSL 解密、身分驗證等各項政策控管功能，並可輕鬆進行集中管理。有了這項功能，遷移至雲端將變得無縫、順暢，且安全性一如既往。

遷移至雲端能為您的企業組織帶來豐厚的資安回報，但您仍須以負責任的方式進行遷移，並與整體 IT 雲端策略及業務需求相互配合。請放心，Broadcom 將在每一個階段全程陪伴您。

結論

有別於傳統封鎖工具，Content Analysis 提供企業級的單機平台，採多層次掃描與分析方式，能更有效地偵測並封鎖已知與未知威脅。此舉可最佳化資安維運 (SecOps) 與事件應變團隊的工作流程，讓他們得以專注處理真正影響其環境的實際威脅。所有內容都會經過這些步驟進行掃描、識別，並運用精密的過濾式威脅偵測與防護方式，封鎖鎖定企業組織的已揭露攻擊。

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，全世界網際網路流量有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進核心技術、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靈活性，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饋，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。