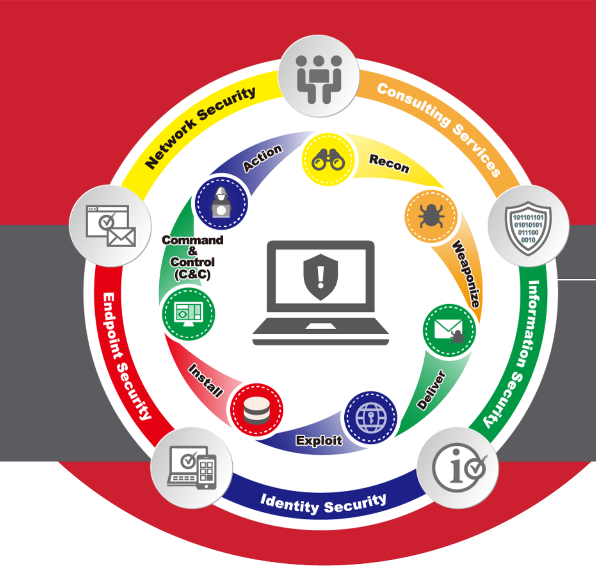


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

透過動態誘騙網站模板竊取微軟憑證的釣魚攻擊

2026 年 4 月 6 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

賽門鐵克的 Cloud Secure Web Gateway (Cloud SWG) 與 Edge Secure Web Gateway (Edge SWG) 偵測到一場針對 Microsoft 365 用戶的持續性網路釣魚攻擊活動。該攻擊活動利用動態生成的誘騙網站模板及自訂 CAPTCHA 驗證作為規避機制，其最終目的是竊取使用者憑證。

觀察到的技術手法--包括在每次頁面載入時提供會變化的多樣態誘騙內容、模仿企業服務子網域、濫用各種頂級網域 (TLD) ，以及利用 Cloudflare Workers 基礎架構--均與 Tycoon2FA 釣魚即服務 (PhaaS) 平台 (微軟追蹤代號為 Storm-1747) 的作案模式一致。該平台曾於 2026 年 3 月 4 日成為歐洲刑警組織主導的協調性打擊行動目標，行動期間查封了超過 330 個網域。然而，該活動在數日內便恢復至遭打擊前的水準，賽門鐵克持續觀察到流向新建立的釣魚基礎設施的流量，這些流量仍呈現上述行為特徵。

背景：誘騙規避技術的演變

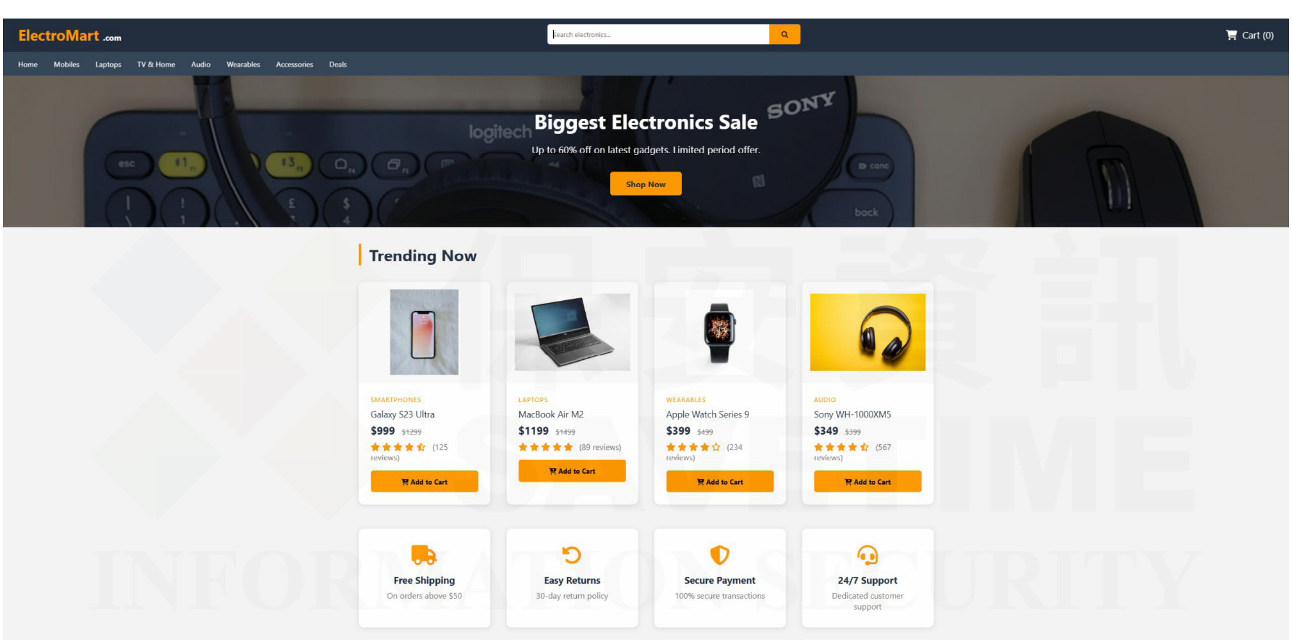
在先前的一篇《防護重點》中，賽門鐵克曾記錄此規避手法的一項具體案例：某釣魚基礎設施冒充 Microsoft Outlook，向研究人員和自動化掃描工具提供以汽車收藏為主題的誘騙網站 (參見：Broadcom 安全中心--防護亮點：賽門鐵克的網頁生態即時分類系統--WebPulse 持續偵測到唯妙唯肖的釣魚、詐騙網站) 。

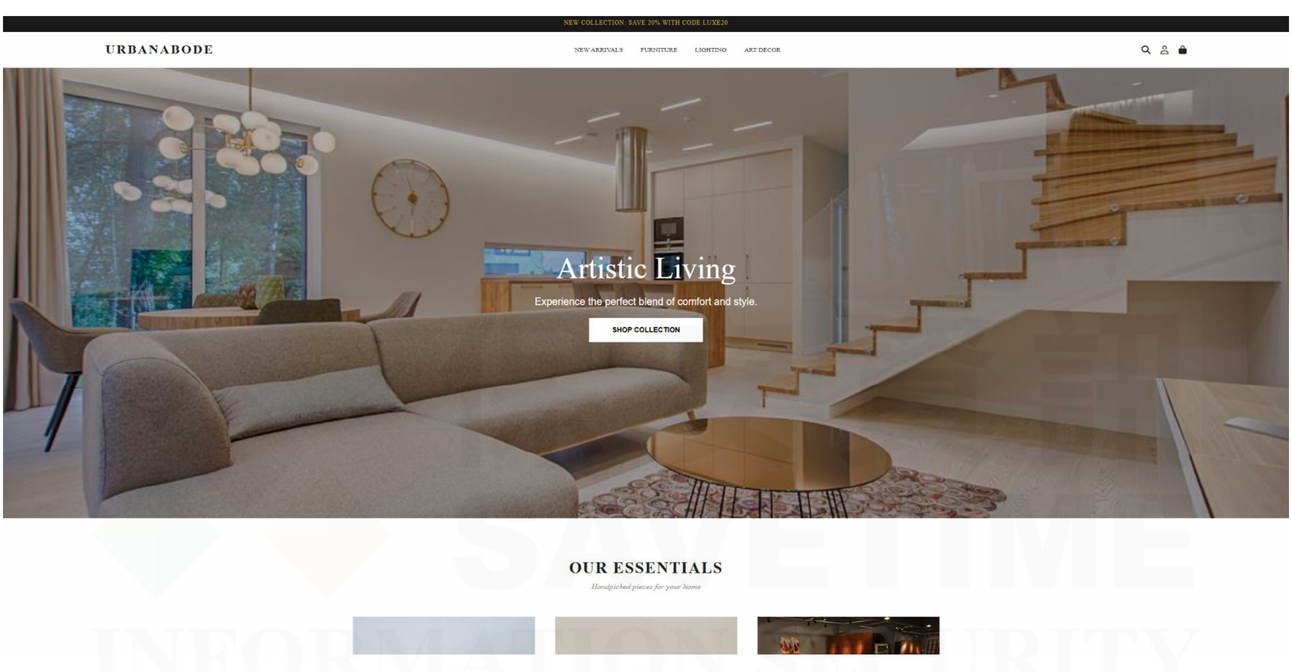
自該報告發布以來，這項規避策略已大幅演進。該攻擊活動已從單一、靜態的誘騙主題，轉變為涵蓋多個垂直產業領域、動態生成且隨機輪替的模板。早期攻擊活動會向非目標訪客持續顯示相同的汽車收藏網站，而當前的架構則會在每次頁面載入時生成完全不同的網站模板，使得基於特徵碼比對的誘騙層偵測變得更加困難。

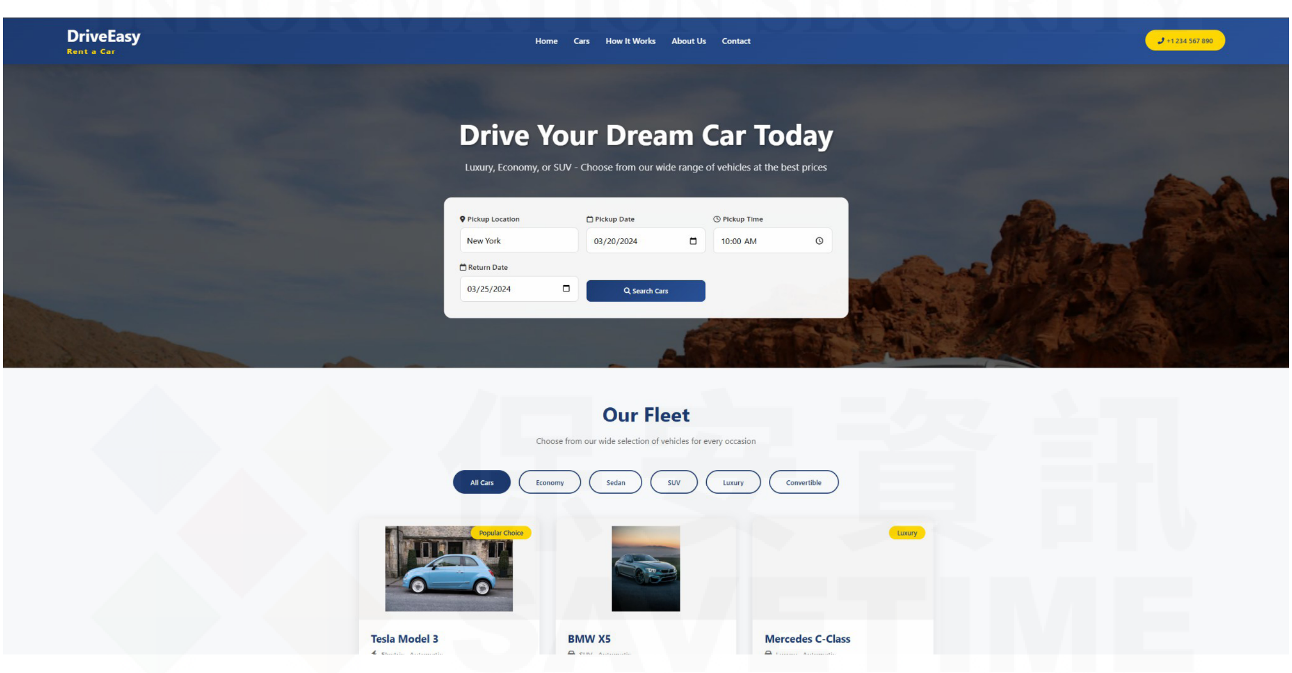
這種演變與 PhaaS 生態系統中觀察到的更廣泛趨勢相符，在該生態系統中，營運商正日益利用自動化與範本系統，以大規模產出具有說服力的誘騙內容。這些誘騙頁面並非釣魚內容本身--它們是一層防禦機制，旨在向資安研究人員、自動化掃描工具及其他非目標訪客展示看似無害的內容。

觀察到的誘騙模板

以下截圖是透過重新載入同一網址：hxxps://chaivucu[.]ru/zLUR1r!YqUf 所擷取的。每次重新載入都會產生完全不同的網站模板：

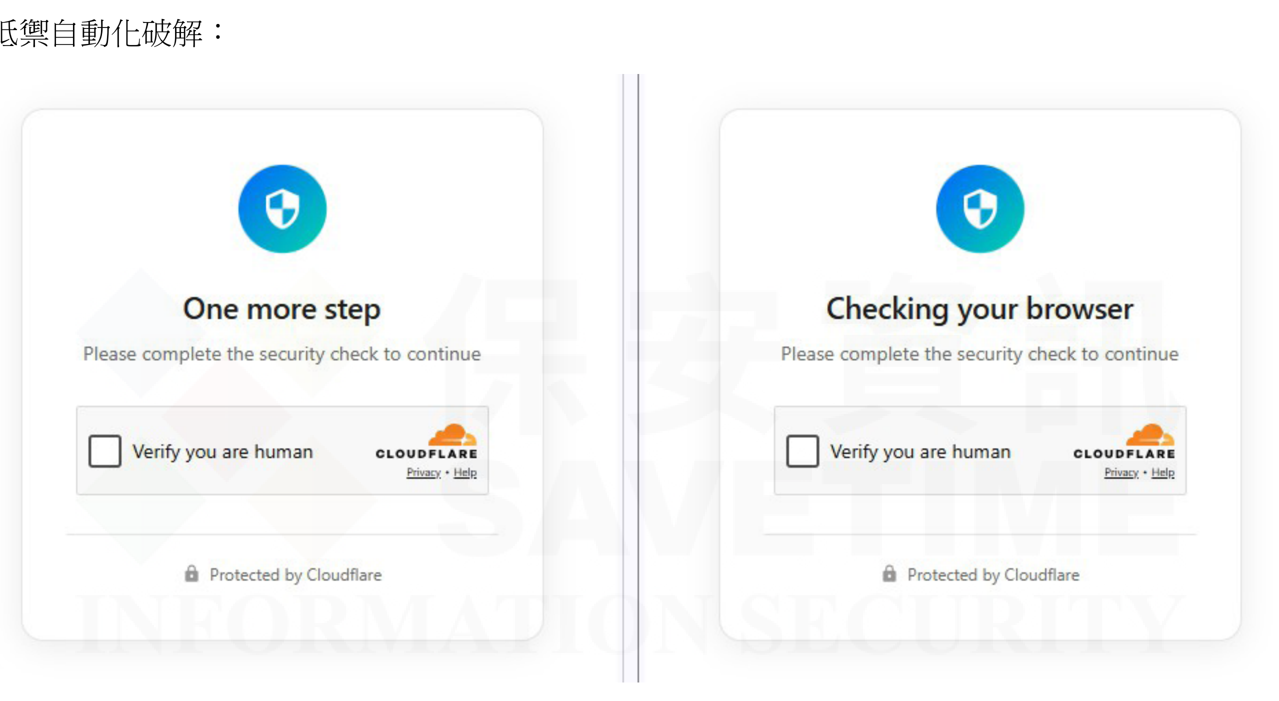



NEW COLLECTION: SAVE 20% WITH CODE LUXE20
URBANABODE
NEW ARRIVALS
FURNITURE
LIGHTING
ART DECOR
Artistic Living
Experience the perfect blend of comfort and style.
SHOP COLLECTION
OUR ESSENTIALS
Handpicked pieces for your home



自訂 CAPTCHA 驗證

此活動的基礎架構亦部署了自訂 CAPTCHA 驗證，取代了先前對 Cloudflare Turnstile 等第三方服務的依賴--這些服務曾為攻擊者提供了可預測的指紋識別訊號。目前的實作採用透過 HTML5 canvas 渲染的 CAPTCHA，其中包含隨機字元、背景雜訊及輕微的視覺扭曲，使其能有效抵禦自動化破解：



One more step

Please complete the security check to continue

☐ Verify you are human

Protected by Cloudflare

Checking your browser

Please complete the security check to continue

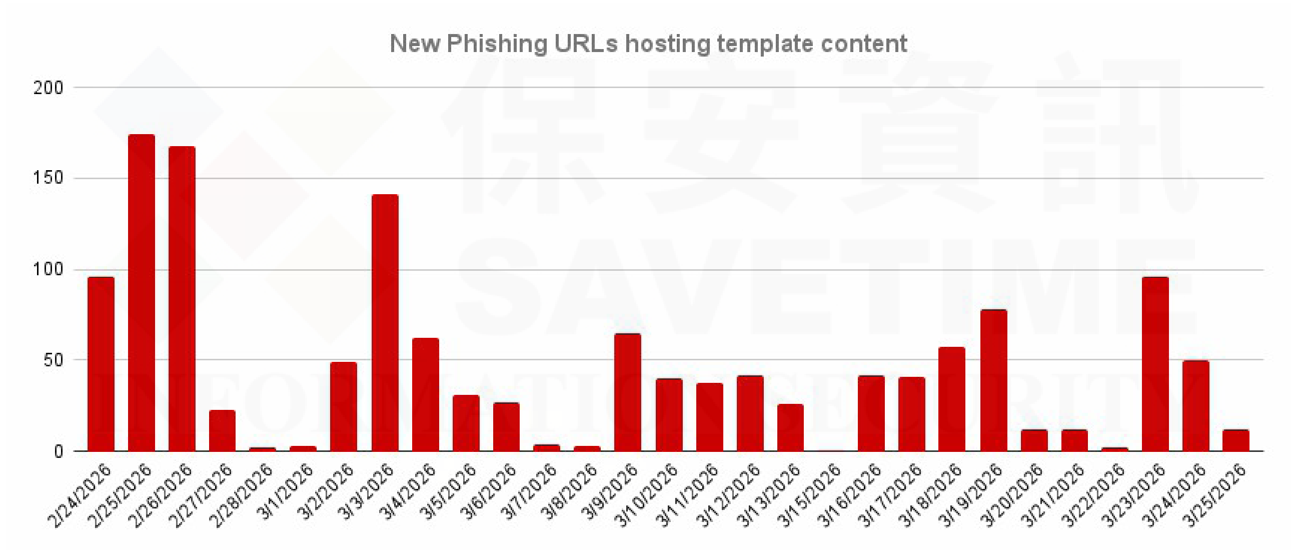
☐ Verify you are human

Protected by Cloudflare

驗證碼 (CAPTCHA) 具有雙重目的：一方面可過濾自動化掃描程式 (確保只有真實的人類流量會進入憑證竊取頁面) ，另一方面則能讓受害者產生一種正當性錯覺，使其將這項安全檢查視為登入流程的正常環節。

流量分析

賽門鐵克 WebPulse 遙測數據顯示，託管此動態誘騙內容的釣魚網站持續收到流量：



該活動的運作者濫用了多種頂級網域 (TLD) ，且其分布情況隨時間推移已發生顯著變化。這很可能反映了多種因素的綜合作用：包括在各註冊商間輪流大批量註冊網域、司法機構的下架行動迫使遷移至新的頂級網域供應商，以及為了規避基於模式比對的封鎖而刻意進行的多樣化佈局。

- 過去 30 天 (2026 年 2 月至 3 月) ： 按請求量計算，遭濫用最嚴重的頂級域名 (TLD) 依序為：.com(890 次請求)、.org(134 次)、.bio (32 次)、.ink(30 次)、.dev(29 次)、.sbs(22 次)、.ltd(22 次)、.world(19 次)、.one(18 次)以及 .ru(17 次)。.com 的壓倒性主導地位，顯示出趨勢正轉向主流且看似值得信賴的網域名稱。
- 2026 年 1 月：相較之下，1月的頂級域名分布呈現顯著差異：.id(548次申請)、.pl(257次)、.co(143次)、.digital(113次)、.in(105次)、.business(102次)、.com(96次)、.institute(90次)、.contractors(81次) 以及 .dev(79)。印尼的 .id 與波蘭的 .pl 網域佔據主導地位，同時也有小眾 gTLD 出現。

從一月份以 .id 和 .pl 為主的註冊量，轉變為三月份以 .com 為主的註冊量，顯示註冊商的大批量註冊流程已發生變化。一月份的頂級域名 (TLD) 註冊概況 (明顯偏向印尼的 .id、波蘭的 .pl，以及 .business、.institute 和 .contractors 等利基型通用頂級域名) 符合低成本、高量的註冊商濫用模式。近幾週轉向 .com 和 .org 的趨勢，可能顯示打擊行動取得成效，迫使相關註冊轉移至主流註冊商。

此次攻擊活動的一大特色，在於系統性地使用子網域來冒充合法的企業工具、DevOps 平台、人力資源工作流程及軟體服務。此技術是 Tycoon2FA 生態系統中已廣為記載的特徵，旨在提升外觀上的可信度，並繞過基於URL 過濾機制模式。已觀察到的範例包括：

- circleci.friogoufo[.]com -- 偽裝成 CircleCI (持續整合／持續交付／DevOps)
- 2fscrum.thiocraijio[.]com -- 偽裝成 Scrum 工具，並提及雙重驗證 (敏捷開發／驗證)
- backlog.yiolono[.]com -- 偽裝成 Backlog (專案管理)
- recruit.shiohucri[.]com -- 模擬招聘入口網站 (人力資源／人才招募)
- job.sijoloo[.]com -- 模擬求職入口網站 (人力資源／人才招募)
- activation.croocheagou[.]com -- 模擬帳戶啟用工作流程 (驗證)
- magento.titroujo[.]support -- 模擬 Magento (電子商務)
- worldcore.traibiru[.]world -- 模仿 Worldcore (金融科技)
- adminconfigurationxlsm.polytronicsgroups[.]com -- 模仿管理員設定／XLSM 工作流程 (企業 IT)
- securemailsharedmforms[.]com -- 模仿安全郵件／表單服務 (電子郵件安全)

用於託管的二級網域名稱呈現出獨特的音韻模式，暗示其可能由演算法生成：friogoufo、thiocraijio、shiohucri、yiolono、beasutea、mouchufru、titroujo、traibiru、croocheagou、chaivucu 以及 sijoloo。這些字串遵循一致的子音--母音--子音結構，並帶有重複出現的雙母音模式 (「ou」、「io」、「ai」、「ru」)，這暗示著存在共同的網域名稱生成演算法 (DGA) 或自動化註冊工具組。

所有被偵測到的網域和 IP 位址，都會在所有啟用 WebPulse 的產品中，被歸類至適當的安全類別 (網路釣魚、可疑、惡意軟體) 。當識別出新的基礎設施時，系統會即時更新分類。

參考資料

- 博通安全中心 -- 防護亮點：偵測以 Outlook 為主題的釣魚攻擊及偽裝成汽車收藏網站的誘騙網站
- 微軟安全部落格 --「深入解析 Tycoon2FA：領先的 AiTM 釣魚套件如何大規模運作」(2026 年 3 月 4 日)
- CrowdStrike --「Tycoon2FA 釣魚即服務平台在遭摧毀後仍持續運作」 (2026 年 3 月 20 日)
- Cloudflare 威脅情報 --「Tycoon 2FA 摧毀行動」 (2026 年 3 月)
- 歐洲刑警組織 --Tycoon2FA 基礎設施中斷公告 (2026 年 3 月 4 日)

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-microsoft-credential-phishing-via-dynamic-decoy-website-templates
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。

關於賽門鐵克 (Symantec)

Symantec
A Division of Broadcom

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 www.savetime.com.tw

保安資訊
KEEPSAFE
INFORMATION SECURITY

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、可以提供良好諮商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。
保安資訊連絡電話：**0800-381-500**。