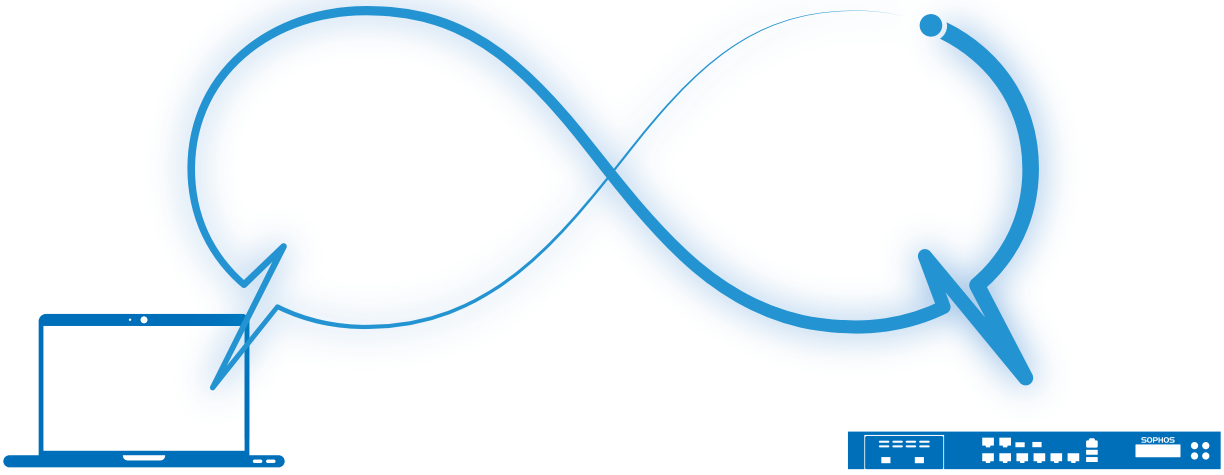
SOPHOS

Security made simple.



可同步的安全性：資訊安全的革命

第一章：在危險區中求生—今日的網路風險環境

「一路衝向危險地帶。我會帶你直驅危險地帶」

– Kenny Loggins，〈Danger Zone〉

受攻擊面、攻擊複雜性和精密程度都增加了

無論規模為何，今日企業都必須生活與學習在網路風險不斷增加的環境中存活。風險增加的原因很多，包括受攻擊面增加，以及攻擊的複雜性和精密程度都提升了。

首先，由於員工必須使用大量的行動裝置和雲端服務，以及各種規模的組織紛紛導入虛擬和雲端基礎結構，因此「受攻擊面」大幅擴大。考慮以下事實：

- 英國使用者平均擁有 3.1 個聯網裝置 (來源：statista.com)
- 員工數 250-999 人的公司使用 16 個經過許可的雲端 app；員工數 1,000-4,000 人的公司是 14 個，而最大型的企業只使用 11 個。(來源：Okta Business@work，2015)
- 產業預估 2015 年基礎結構即服務 (Infrastructure as a Service) 的營收將超過 160 億美元 (來源：Gartner，http://www.gartner.com/newsroom/id/3055225)
- 到 2015 年底，會有 49 億個「物件」連上網際網路。到 2020 年，這個數字還會成長到 250 億。(來源：http://www.gartner.com/newsroom/id/2905717，2014)

由於受攻擊面增加，可以預見會有更多攻擊出現並成功導致資料外洩事件發生。

其次，攻擊的複雜性和精密程度都持續上升。即使最沒有技術背景的攻擊者也能取得灰色市場和黑市的精密商用工具套件。

這些「工具套件」經過妥善測試，甚至擁有商業支援，並不容易被偵測或打敗。例如 UnRecom Remote Access Tool Kit (或稱 RAT)，2014 年 5 月首次由 Threatgeek.com 報導，已經經過數次改版，包括 AlienSpy 和最近的 JSOCKET，均被認為和包括資料外洩到政治謀殺等活動都有牽連 (來源：Threatgeek.com)。

不幸的是，越來越多被證實的資料外洩報告中，中小型企業似乎特別容易成為受害者。根據 Verizon 2015 年資料外洩調查報告：

- 在 2014 年，79,790 件安全事件中，經確認有 2,122 件資料外洩
- 與 2013 年相比，安全事件增加 26%，而資料外洩部分暴增 55%

威脅態勢

- 中階市場企業儘管只佔 1.4% 的安全事件，但經確認的機密資料外洩事件超過 53%
- 較小的企業安全事件和資料外洩發生在多種產業，大多集中在金融服務、住房、零售和健康照護領域

受攻擊面和攻擊複雜性增加導致外洩事件也隨之增加，迫使我們應該提高警覺並思考應該採取不同的作法。

精簡的團隊、窘迫的資源、緊縮的勞動力市場

當攻擊和外洩事件增加，最自然的反應就是「投入更多人力」來解決問題。但是小型和中型企業只有精簡的 IT 安全團隊，擴充或重新部署資源並不是這些小型組織的實際選擇，即使那是一個有效的策略。如圖所示，中小型企業的專屬 IT 安全人力非常精簡：

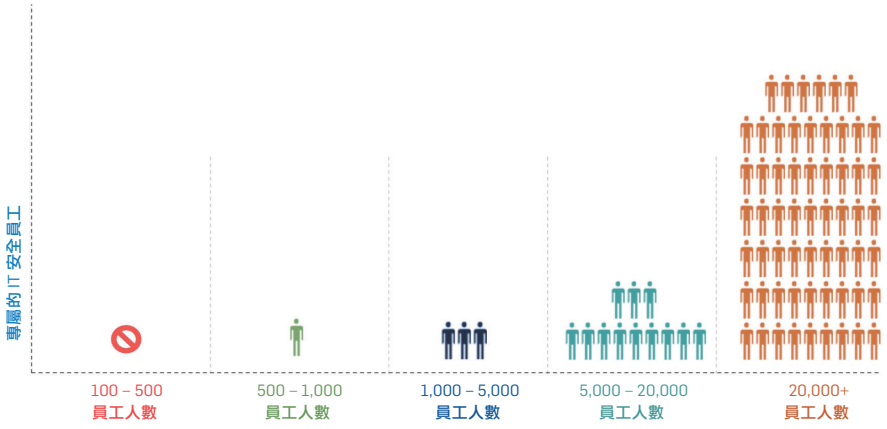


圖 1：中型市場 IT 安全團隊很精簡且資源有限 (來源：美國國土安全部，2014 年)

即使管理階層希望擴大自己的安全團隊，但也面臨著十分緊迫且非常競爭的就業市場。根據 BurningGlass 2015 網路安全工作報告，與網路安全相關的工作數自 2010 到 2014 年成長了 91%，比整體 IT 工作增加的速度快了 325%，而且「在美國，雇主釋出 49,493 個要求 CISSP 的工作機會，但全球只有 65,362 個獲得 CISSP 的專業人士。」

總之，這些風險增加、數量暴增、複雜度和攻擊得手機會增加的情形，都使精簡和資源緊迫的團隊無力招架，而讓組織處於無法承受的風險程度之中。

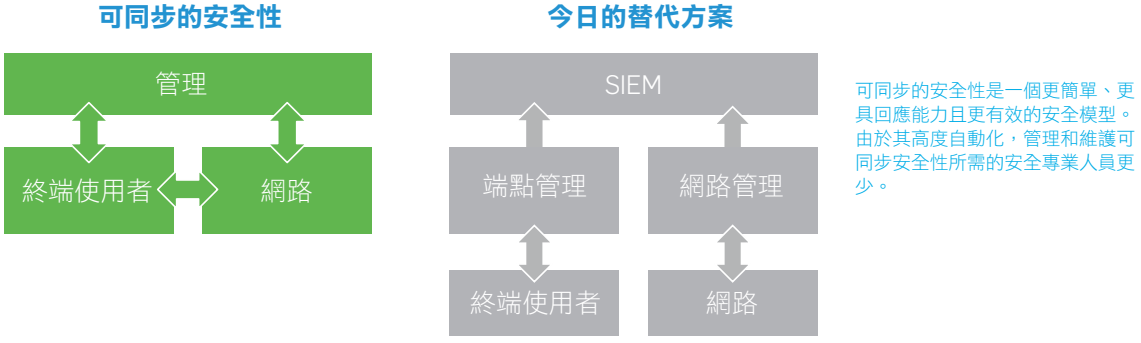
第二章：等等，我們過去的投資去哪了？

「就算聚集了國王所有的馬和國王所有的臣子，蛋殼先生也不能再恢復原來的樣子。」—鵝媽媽

太多層且整合不良。複雜又短視。和相近的前後個體互不往來。決策各行其是。前述這些說法都可以套用在我們當今的安全投資上。從過去的防毒、IPS、網頁、郵件和網路閘道，到今日的套件、UTM、沙箱和端點偵測與回應解決方案，我們其實仍然停留在一個產品各自為政且非常複雜的環境中。當攻擊者在我們的整個 IT 生態系統發動協同攻擊，無力阻擋當然不足為奇。攻擊一開始可能出現在端點，然後擴散到網路，最後則是竊取我們出站網際網路連線的資訊。

針對這個現實，IT 安全專業人員和廠商試圖透過部署關聯引擎、巨量資料倉儲、安全性資訊和事件管理系統 (SIEM)，如 STIX 和 OpenIOC 等新興資訊共用架構，以及分析師的評比，「串連」起來自各資料來源的端點。但是，即使是最先進的工具，試圖了解各種單點產品的資料，以便快速偵測和修補風險與阻擋資料外洩，已經被證明很難讓「蛋殼先生」恢復原狀。事件和日誌的關聯性仍須仰賴於建立和維護複雜的關聯規則、無止盡的欄位對應和篩選定義，以及許多高技術性、難以配置的分析師時間和人力。SIEM 方面則需要可觀的資本投入和持續營運費用。而資訊共用雖然是未來安全性的關鍵，但仍未成熟到普及，可以簡單導入的程度。

結果或資源缺乏的情形不言而喻。正如我們所看到的，資料外洩和風險持續增加，絲毫沒有減弱的跡象，使得員工面臨巨大的壓力。根據最近 Ponemon Institure 報告指出，74% 的外洩事件都是超過半年才被發現。最糟的是，和資源豐沛的大型企業相比，中型企業更難減緩這個風險。顯然，答案不是另一個未整合的單點產品、更多主控台、更多員工或不聰明的 SIEM。總之這些作法都無法獲得成功。我們必須找到一個更好、更有效的作法。



可同步的安全性是一個更簡單、更具回應能力且更有效的安全模型。由於其高度自動化，管理和維護可同步安全性所需的安全專業人員更少。

第三章—可同步的安全性，一個全新的作法

新的革命理念

「你說你想來場革命。嗯，你知道我們都想改變這個世界。」
—The Beatles，〈Revolution〉

幾十年來，安全產業已經將網路安全和端點安全視為完全不同的個體。這就像把一個安全警衛放在大樓外，另一個放在大樓內，然後不允許他們交談一樣。可同步的安全性是革命性但非常簡單的作法—我們給每個警衛一支雙向無線電。往後當任何一人看到問題時，另一個可以馬上知道。

如果我們以不同心態，用一個全新作法重來，讓 IT 團隊可以成功阻擋今日網路的風險，會是什麼情形？結果之一是可以提供更好的保護，並在網路和端點安全解決方案間啟用自動化且即時的通訊；以及可以在整個被威脅面進行同步；最後一個則是高度自動化，因此無須增加員工或工作量就能達成目的。為了達成這項目的，我們需要一個具備以下能力的系統：

以生態系統為中心—我們必須經由完全感知附近物件和事件的能力，防止、尋找和阻擋整個 IT 生態系統上的漏洞。

全方位—這個解決方案必須是全方位的，而且能涵蓋所有的 IT「系統」、多平台和裝置，以便防禦針對整體而非單點而來的攻擊。

高效率—這個解決方案在改善保護能力的同時，還必須能減少團隊的工作量。它不能增加額外的技術和工作負載。

有效—這個解決方案必須能有效防禦、偵測、調查和修補今日整個被攻擊面上的威脅。

簡單—易於購買、易於了解、易於部署和使用。

這個清單看似是一個艱鉅的任務，確實如此。今日的 IT 安全產品則反其道而行；它們以威脅為中心，複雜、不夠全面性，而且需要密集的資源。總之，它們的協調性比不上所防禦的攻擊。顯然，需要創新才能獲得成功。我們將這項結論總結在圖 2 中。

今日的多層式安全解決方案	想要的解決方案
以威脅為中心，相近的物件和事件均獨立運作	以生態系統為中心，運作時可完全感知相近的物件和事件
專用的單點產品	協同運作的產品
需要增加人手才能提高有效性	經由自動化和創新達成有效性；不需要增加人手
複雜	簡單

圖 2：今日的解決方案需要大幅改變

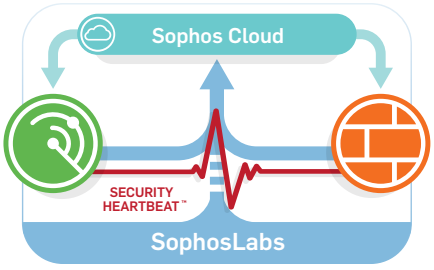
為了在今日環境中提供這種簡潔性和效益，需要一項巨大的技術創新，我們稱之為 Sophos Security Heartbeat。

Sophos Security Heartbeat

「如同鼓上的跳動」
—Cole Porter，〈Night and Day〉

可同步的安全性讓次世代端點和網路安全解決方案可以持續共用有意義的資訊，在整個組織的擴展 IT 生態系統中找出可疑和確認為惡意的行為。透過稱為 Sophos Security Heartbeat 的直接安全連線，端點和網路保護能結合為一個整合式系統，讓組織可以近乎即時的速度防禦、偵測、調查和修補威脅，而不需新增任何人力。

例如，當 Sophos 次世代防火牆偵測到一個進階型威脅或外洩機密資料的行為後，它會自動使用 Sophos 安全性產品。安全心跳會在網路和端點上採取一系列動作來減緩風險，並且立即防止資料外洩。同樣，如果受保護的端點被發現遭駭，可同步的安全性會自動且近乎即時地隔離該端點，避免其外洩機密資訊或傳送資料到指揮與控制伺服器。這類的發現與安全事件回應過去要花上數週或數月，有了可同步的安全性，現在只要數秒鐘內就能完成。



Sophos 可同步的安全性使用 Security Heartbeat、Sophos Labs 和 Sophos Cloud，可為端點和網路提供簡單且非常有效的安全保護。

總結

「一個彼此連結的真理，連結起看不見、幾乎無法察覺且難以形容的事物。如果你採取行動如你想，錯失的連結是同步性。」

—The Police，〈Synchronicity〉

為了在今日環境中提供這種簡潔性和效益，需要一項巨大的技術創新，我們稱之為 Sophos Security Heartbeat。

可同步的安全性；資訊安全的革命

複雜且以威脅為中心、依賴員工數量的短視作法，並無法滿足資源有限的 IT 安全團隊的需求。為了扭轉安全事件和違規行為日益增加的趨勢，我們必須採取和過往不同的作法。為此，我們必須實作一個新解決方案，其簡單有效、可自動且能協同作業。簡而言之，就是透過如 Sophos Security Heartbeat 這種技術創新進行的同步性。好消息是 Sophos 已經開始提供這項功能，並可以讓您容易地進行評估。如需更多 Sophos 可同步的安全性能如何協助您戰勝今日高風險環境的資訊，請造訪 sophos.com/heartbeat。

可同步的安全性

更多資訊請造訪 **sophos.com/heartbeat**

英國和全球銷售
電話：+44 (0)8447 671131
Email：sales@sophos.com

北美銷售
免付費電話：1-866-866-2802
Email：nasales@sophos.com

澳大利亞和紐西蘭
電話：+61 2 9409 9100
Email：sales@sophos.com.au

亞洲銷售
電話：+65 62244168
Email：salesasia@sophos.com

牛津，英國 | 波士頓，美國

SOPHOS

2015-10-13 WP-NA (GH)