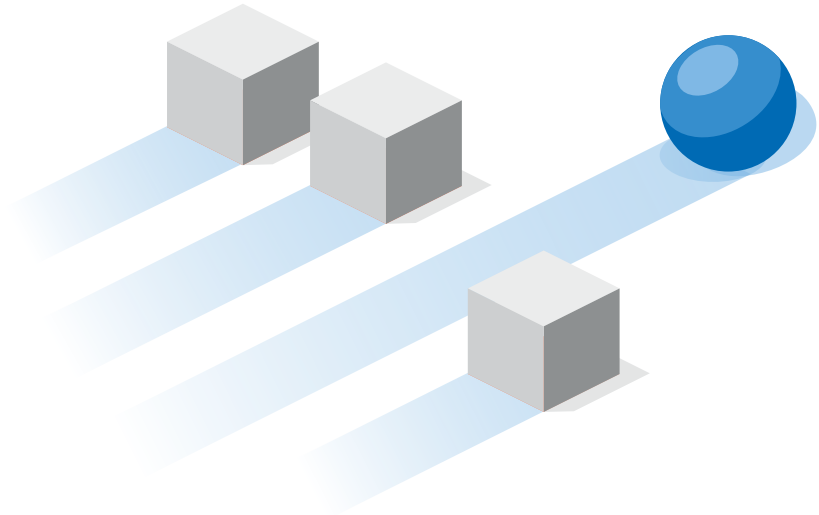
SOPHOS



新一代防火牆的致命弱點

針對 12 個國家 3,100 名 IT 管理員的全球調查結果。

網路安全是每個組織網路防禦的根本，而網路防禦則是建基於其他保護服務 (例如端點、伺服器、行動和加密) 的各層次。它是值得信賴的主力，在維持組織營運方面發揮著關鍵作用。

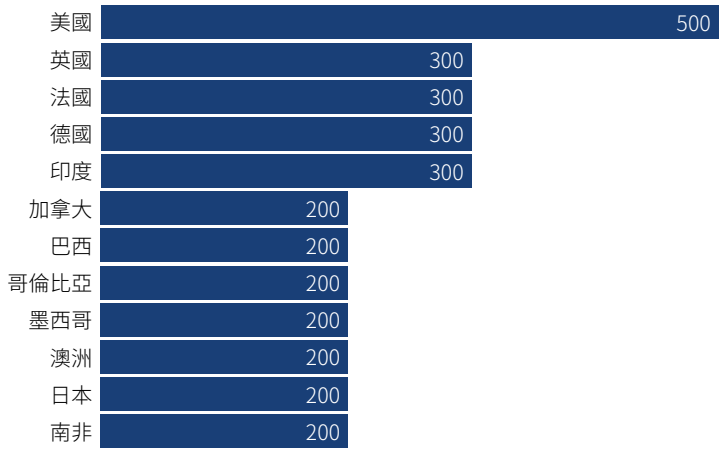
為了深入了解網路安全的現況，Sophos 委託業界領先的市調公司 Vanson Bourne 針對橫跨 6 大洲 12 個國家的 3,100 名 IT 管理員進行了獨立調查。

結果揭露了全球 IT 團隊在網路威脅和新一代防火牆方面的日常經驗。這項調查讓我們了解現今網路安全的實際情況，以及 IT 團隊所面臨的挑戰。它也揭露出新一代防火牆的致命弱點：奮力在效能、隱私和保護之間取得平衡。

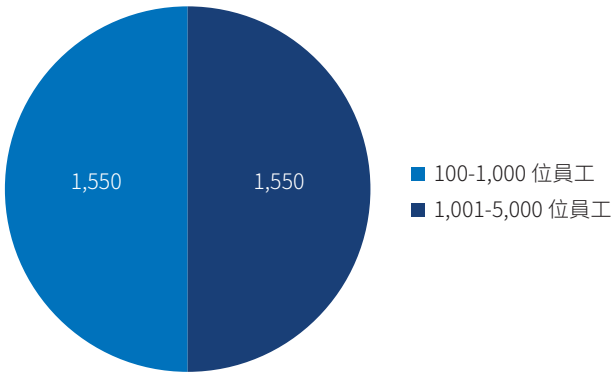
調查

總部位於英國的研究機構 Vanson Bourne 在 2018 年 12 月至 2019 年 1 月期間採訪了 3,100 名 IT 決策者。為了讓每個國家/地區的組織規模具有代表性，受訪者平均分配在 1001,000 個使用者和 1,001-5,000 個使用者的組織。

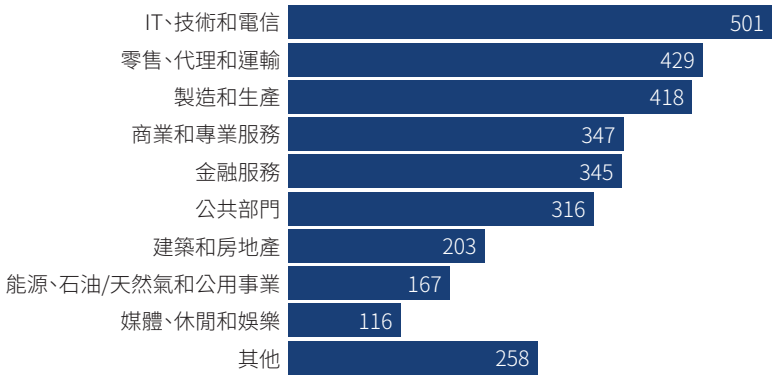
每個國家/地區的受訪者人數



按組織規模劃分受訪者



按行業劃分的受訪者



預期在您的網路上找到威脅

該調查的第一點揭示出，組織應該預期會遭到網路威脅的攻擊。去年有超過 2/3 (68%) 的受訪者淪為網路攻擊的受害者。

成為威脅受害者的這種傾向，並不是缺乏保護的結果：91% 受影響的組織在遭到攻擊時正在執行最新的端點安全保護。然而，良好的意圖和良好的做法顯然不足：組織的防禦中仍然存在漏洞，讓威脅得以入侵。

該調查還突顯出網路犯罪分子傳播其攻擊的廣泛策略和技術。知道威脅如何進入其組織的 IT 團隊的資料指出：

- 33% 透過電子郵件進入
- 30% 透過惡意或遭入侵的網站進入
- 23% 透過他們所使用的軟體進入
- 14% 透過 USB 隨身蝶/外部裝置進入

不過在 20% 的案例中，IT 團隊不知道威脅進入點何在。這種缺乏可見度的現象突顯出 IT 團隊在保護其組織方面所面臨的重大挑戰：如果不知道威脅是如何進入，就很難阻止未來的攻擊。

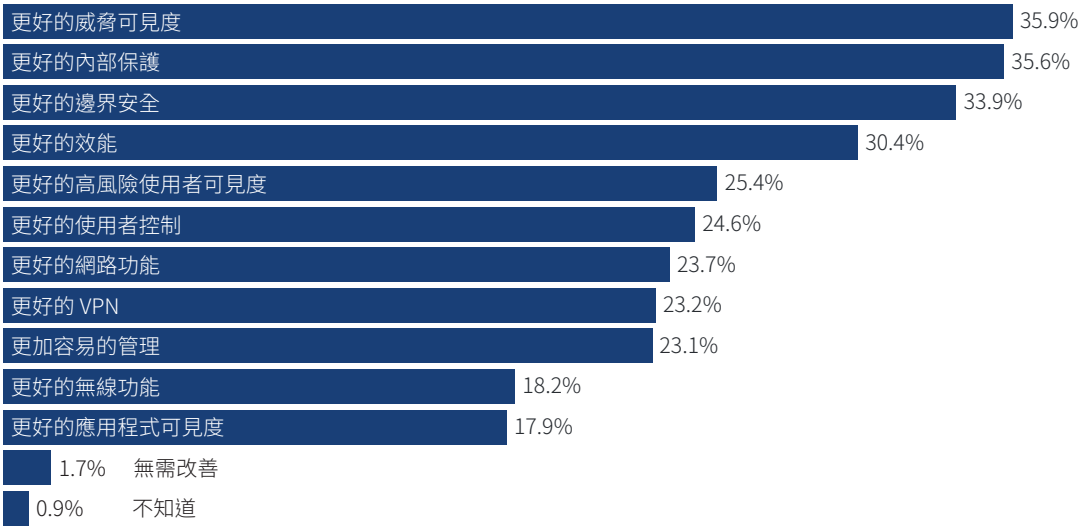
威脅在網路中停留的時間越長，對組織的風險就越大。調查指出，組織平均花 13 小時來偵測其網路中的威脅。顯然，此時駭客就有機會進行各式各樣的破壞。

同時，有 17% 的 IT 管理員在發現威脅之前，不知道那些威脅在其環境存在了多久時間，這進一步證明 IT 團隊在網路安全上所面臨的可見度問題。

防火牆改善願望清單

更好的威脅可見度，是調查受訪者希望其防火牆改善的整個清單的第一名，有 36% 將這一點納入他們前三名希望的改善功能中。可見度勝過更好的保護而登上第一名這一點，說明了缺乏資訊對 IT 團隊是多麼嚴重的問題。

受訪者希望在其網路防火牆中看到的最大改善 (排名第一、第二和第三的組合)



在澳洲與加拿大，對威脅可見度的需求最強烈，有 41% 的受訪者將其納入前三名改善中，緊接在後的是美國，有 40% 的受訪者將票投給它。。日本受訪者是唯一與趨勢相反的，只有 21% 的人將更好的威脅可見度列在防火牆改善願望清單中。

有鑑於網路威脅的普遍存在，更好的邊界安全也名列受訪者願望清單前幾名並不為奇，有 34% 的人將這一點列在他們前三名想要的改善功能中。

不過，受訪者希望防火牆獲得改善的地方不只有安全性。有三成受訪者認為，更好的效能是他們需要防火牆獲得的最重要改善之一。

整體而言，以下狀況越來越清楚：問題不再是更好的效能或更好的保護。而是，現今 IT 團隊既需要效能也需要保護。

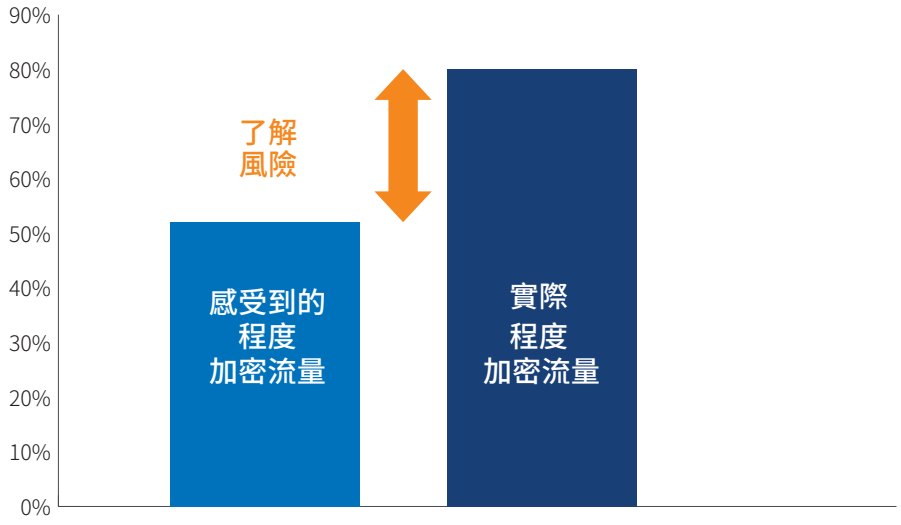
被低估的風險：加密流量

加密能讓網路流量保持隱私，但卻無法保持安全。實際上，加密流量是巨大的安全風險，因為它會讓防火牆對於網路中通過的內容視而不見，進而阻礙它們識別及阻擋惡意內容。那就像飛機乘客在通過安全檢查時，用全身毛毯裹住自己保持匿名一樣。

駭客正積極利用加密，使攻擊在偵測不到的情況下進入受害者。SophosLabs 的研究顯示出問題的嚴重性，該研究指出，在 2019 年的前八個月中，惡意軟體呼叫的 URL 中有 25% 使用加密。

加密網路流量的程度正急遽上升。Google 透明度報告的資料顯示，現在所有平台上超過 80% 的網頁工作階段已加密，這數字在兩年前僅為 60%。不過，調查受訪者心目中的印象似乎不一樣：平均而言，他們認為其網路流量中只有 52% 是加密的。在接受調查的所有國家中，回答都是一致的，全都介於日本 (46% 加密) 和德國 (57% 加密) 之間。

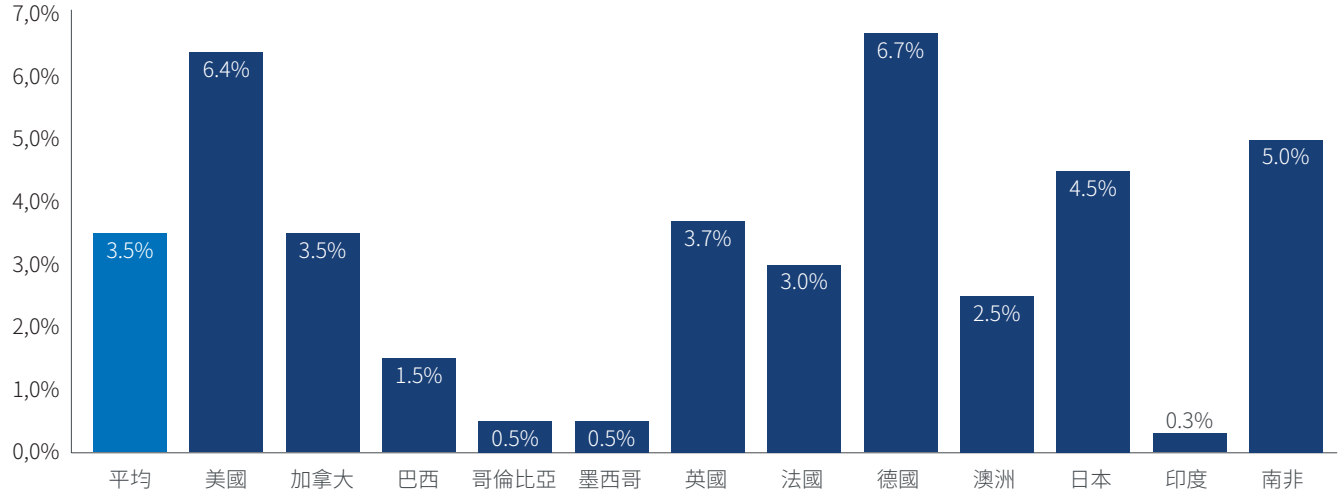
感受的印象與實際上的加密程度之間的差異，加上網路攻擊中廣泛使用加密的情況，表示加密流量的安全風險被低估了。這曝露出IT 團隊對於加密流量程度迅速提高一事毫不知情。此外，依據目前趨勢，加密流量的百分比將在不久的將來進一步提高。



網路安全的致命弱點

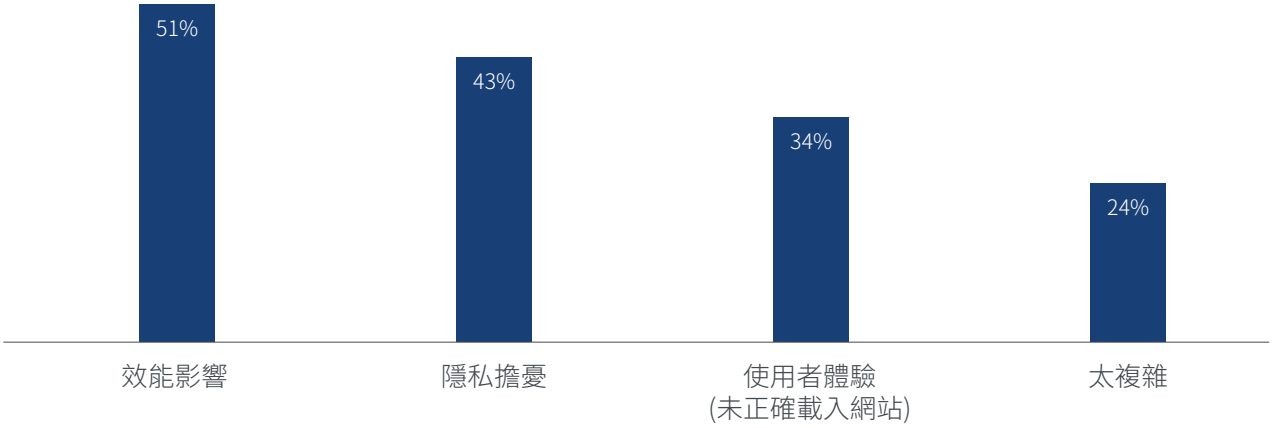
儘管有 82% 的調查受訪者同意 TLS 檢查是必要的，但只有 3.5% 的組織將其流量解密以進行適當的檢查。超過 6 % 的受訪者對其所有流量解密，其中德國和美國位居榜首，而印度、哥倫比亞和墨西哥的解密率最低。

將網路流量解密以進行適當檢查的組織百分比



調查顯示，組織未將網路流量解密的原因很多：擔心防火牆性能；缺少適當的政策控制；使用者體驗不佳；以及複雜性。

您組織不將網路流量解密以進行適當檢查的原因是什麼？(選取所有適用項目)

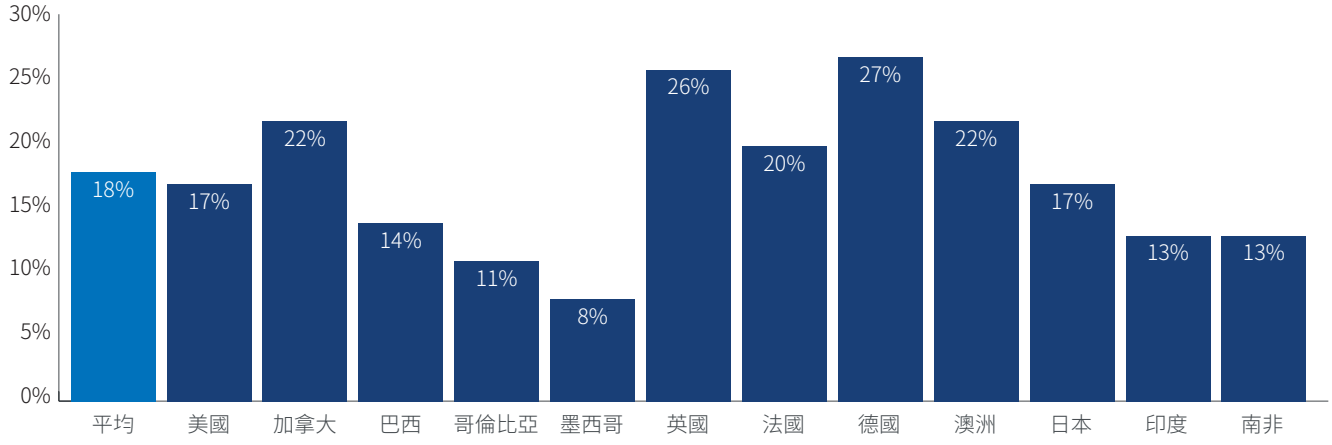


現實情況是，大多數組織都必須在效能、隱私和安全性之間謹慎地取得平衡。不過，他們缺少有效又高效率地進行此工作所需工具。因此，他們選擇讓加密流量通過，不加以檢查，而讓自己陷入隱藏網路威脅的風險當中。

無法在效能、隱私和保護之間取得平衡的此一缺點，是許多新一代防火牆和 UTM 解決方案的致命弱點，也是隱藏弱點。

同時，有極少數的調查受訪者沒有意識到解密網路流量的必要性。在德國和英國，有超過 1/4 的受訪者說沒有必要解密所有網路流量；反之，墨西哥只有 8% 的受訪者同意此一觀點。

認為沒必要解密所有網路流量的調查受訪者百分比



這表示，在加密網路流量相關風險的教育方面，安全產業仍有工作要做。

將加密流量的風險減到最小的防火牆功能

隨著我們即將來到 100% 網路流量加密的同時，Sophos 建議您在您的新一代防火牆中尋找下列五項功能：

1. **最新的 TLS 1.3 和加密套件支援。**儘管採用 TLS 1.3 仍處於初步階段，但是購買不具備 TLS 1.3 支援的防火牆是很不明智的。
2. **串流引擎解決方案**，能夠檢查所有連接埠/通訊協定的所有 TLS 流量，而且比傳統的 Web Proxy 型解決方案更快，使用的連線數也更少。
3. **強大的憑證驗證**，能夠處理無效、自我簽署、已撤銷或未受信任的憑證，避免可能的惡意攔截式 (MITM) 攻擊。
4. **強大又有彈性的政策工具**，可針對哪些應該加密及檢查，提供精細的控制，進而讓您在組織的隱私、保護和效能之間建立理想的平衡。
5. **高效能**，擁有足夠的連線處理、高效率的加密、硬體加速，以及高效率處理加密流量的整體能力。

Sophos XG Firewall 介紹：專為現代的加密網際網路而設計

XG Firewall 中的 Xstream 架構提供一種全新開發的解決方案，可消除網路流量盲點，同時不會影響效能。它提供：

- 高效能 – 具備高連線功能的輕量級串流引擎
- 無與倫比的可見度 – 可深入了解您的加密流量和任何錯誤
- 頂級安全性 – 採用強大的憑證驗證，支援 TLS 1.3 和目前所有加密套件
- 檢查所有流量 – 不論應用程式和連接埠，一律檢查
- 絕佳使用者體驗 – 提供多樣的互通性，可避免中斷網際網路
- 強大的政策工具 – 提供效能、隱私與保護之間的理想平衡

結論

目前的趨勢顯示，到 2020 年底時，超過 90% 的網路流量會加密。同時，駭客也會在網路攻擊中繼續利用加密。為了將加密網路流量的安全風險減到最小，組織應該將解密所有網路流量視為基本要件。這有助於提供 IT 團隊所需的更好的威脅可見度和網路保護。同時，防火牆效能依然是重要需求。選擇新一代防火牆時，請選擇能夠在效能、保護和隱私需求之間取得平衡的解決方案。