STOP THE PARASITES ON YOUR NETWORK

高風險、不需要、甚至是惡意的應用程式像寄生蟲般隱藏在許多組織的網路上，這是因為大多數新一代防火牆無法勝任它們的工作。 它們無法識別特定的應用程式，最多只能識別 HTTP、HTTPS/SLL、UDP 或 TCP 等通訊協定。對於試圖了解網路上出現的安全性、合規性和生產力風險的網路管理員而言，這是沒有用的。

究竟這些寄生應用程式是什麼？為什麼新一代防火牆發現不到它們？您該如何識別出網路上的每一個應用程式？

寄生蟲程式問題有多嚴重？

「平均來說，企業網路上有 **45%** 的網路流量是無法識別的。」

換言之，一般組織無法識別或分類其網路上將近一半的應用程式。對於小型或中型組織而言，這可能意味著有數十或數百個未知應用程式在網路上執行。
這些應用程式並不需要有犯意就能對網路造成問題。許多應用程式會對寶貴的網路頻寬造成額外的壓力，但不會造成傷害，而其他應用程式則可以透過使用未經核准的連線來開啟安全漏洞。

對於四分之一的組織來說，這種情況更糟糕：他們有 70% 的網路流量都是未經識別的。

下圖是一般防火牆在應用程式訊息方面的儀表板。很可能您已經在目前或之前的防火牆中看到類似的介面。

主要應用程式

應用程式名稱	應用程式百分比
一般 UDP	25.45%
一般 HTTP 管理	24.26%
一般 DNS	17.8%
一般 TCP	14.39%
服務 RCP 服務 (IANA)	8.86%
Bit Torrent 通訊協定 - UDP 活動 1 (Reqs SIB 5)-63	1.6%

一般防火牆儀表板顯示無法識別的類別。

在此範例中，大約 90% 的網路流量只能識別為廣泛類別，這對於想要更多詳細資料以優先處理關鍵應用程式，以及限制不需要的應用程式的管理員來說毫無用處。

您的防火牆為什麼無法識別這些應用程式？

絕大多數現代防火牆使用特徵碼來偵測應用程式(類似傳統的防毒產品)，這存有明顯缺點；如果應用程式與已知特徵碼不相符，則防火牆無法告訴您它是什麼。有些應用程式使用狡黠的手法不斷改變流量模式以及它們連往組織外部的連線方式，以逃避偵測。其他應用程式使用加密以躲避偵測，或偽裝成一般web瀏覽器以便自由通過防火牆。最後，有些應用程式則是最近改版、經過自訂或太過模糊而無法識別。

無論原因為何，這些隱藏的應用程式都會對您的網路效能、合法應用程式造成威脅，而且在某些情況下還會對更廣大的企業網路帶來安全或合規性風險。

系統管理員為何擔憂

「**84%** 的 IT 管理員同意，缺乏應用程式可見度是很嚴重的安全性顧慮。」

毫無疑問，絕大多數 IT 管理員都擔心這些隱藏的應用程式出現在組織的網路上。

- 它們可能意味著安全顧慮，無論是直接威脅或惡意應用程式，或讓未經核准的影子 IT 將資料置於風險中或造成其他安全風險
- 它們可能會利用頻寬和主機資源而對網路效能造成負面影響
- 如果使用者將這些應用程式用於非法、不適當或未經核准的活動，則可能意味著合規性、生產力或責任問題
- 它們有可能是重要的關鍵性應用程式，讓您無法使用 QoS (服務品質) 和流量塑形來正確設定優先順序以確保最佳效能

除了缺乏網路可見度而造成的安全性問題之外，IT 管理員還指出更進一步的顧慮：

「**52%** 擔心未知網路流量導致生產力損失。」

在企業網路上存取社交媒體應用程式或玩遊戲的使用者，除了降低他們自己的生產力外，還會對頻寬造成額外壓力。

「**42%** 擔憂由於內容可能非法或不當，而導致法律責任和合規性問題。」

使用串流或下載受版權保護和非法內容的使用者，可能對組織產生更廣泛的影響。

必須注意的常見網路寄生蟲

「**五分之二**的 IT 管理員擔心他們無法評估頻寬消耗情況。」

我們現在已了解這些隱藏的應用程式如何將您的網路置於風險之中，接著看一下較常見的應用程式類型和每一種的具體範例。

即時通訊 (IM) 和會議應用程式

例如 Skype、TeamViewer

IM 和會議應用程式的迴避行為惡名昭彰，因為它們要確保能夠不受約束地穿透大多數防火牆。 當然，現在每個組織的日常業務運作都相當依賴某種形式的 IM 和會議應用程式套件，因此能夠識別並設定這些應用程式的 VoIP 和畫面共用優先順序，是非常重要的。 同時，未經批准的 IM 不僅會有生產力損失的風險，而且還可能意味著影子 IT 安全性或合規性風險，因為使用者能夠在很少或完全沒有監督的情況下，與組織外的人聯繫並將檔案傳輸出去。

點對點用戶端

例如 BitTorrent、uTorrent

點對點 (P2P) 用戶端最常用於共享非法或有版權保護的內容，並且經過精心設計以掩飾其流量和活動。此外，這些應用程式可以輕易消耗相當大量的頻寬。此類看不見的應用程式代表了龐大的合規性和責任風險、生產力和資源挑戰，以及如果入侵下載透過這些工具進入您網路而造成的重大安全性風險。

Proxy 和通道用戶端

例如 Psiphon、Ultrasurf、Hotspot Shield

加密雲端 Proxy 伺服器的設計是為了掩蓋使用者身分、位置和活動。許多人利用這些服務繞過地理位置限制，例如，雖然用戶實際位置在歐洲，但仍可觀看僅限美國的 Netflix 節目。惡意使用者也常利用它們繞過防火牆；防火牆通常無視加密流量，這使他們能夠自由存取不適當或非法內容。

遊戲平台

例如 Steam、Origin

遊戲平台讓使用者能夠存取成千上萬的遊戲，這些遊戲對生產力造成顯著風險，而且串流型遊戲或多人連線遊戲也會對頻寬造成壓力。

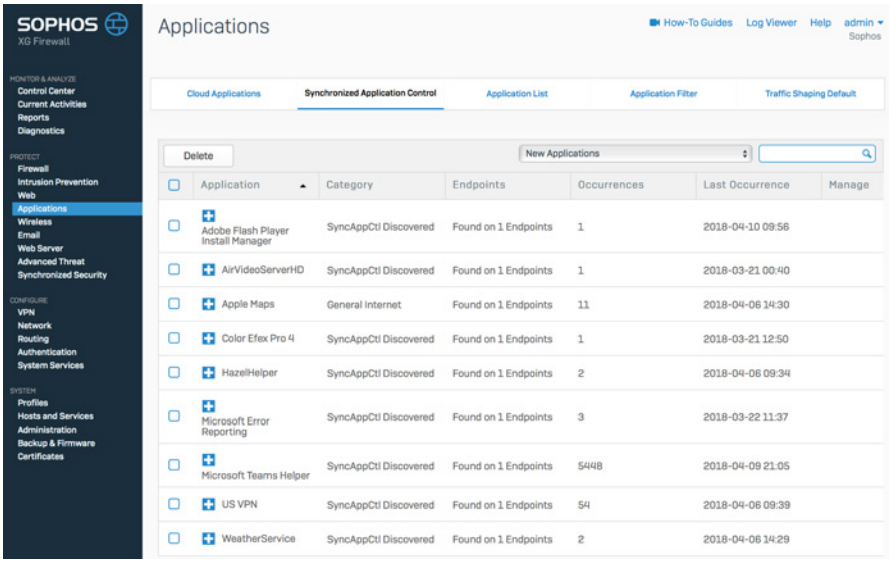
這幾個只是無法識別的應用程式對組織網路有意或無意造成負面影響的少數範例。

解決可見度問題

「**67%** 的 Sophos 客戶已發現超過 100 個不需要的應用程式。」[1]

雖然新一代防火牆需要依靠深度封包檢測、模式比對和特徵碼來嘗試識別出在網路中傳播的應用程式，但是端點的獨特位置使其可以絕對清楚地知道哪些可執行檔正在產生所有的網路交通。因此，解決方案應運而生，作法是將端點與防火牆連接起來，以共享這些有價值的資訊。幸運的是，Sophos 已經擁有可以簡單且有效實現這一目標的技術：同步安全 (Synchronized Security)。

Sophos Synchronized Security 是一種革命性的全新 IT 安全方法，可使安全產品能夠共享資訊並共同協作，提供即時深入資訊、無與倫比的保護和自動事件回應能力。

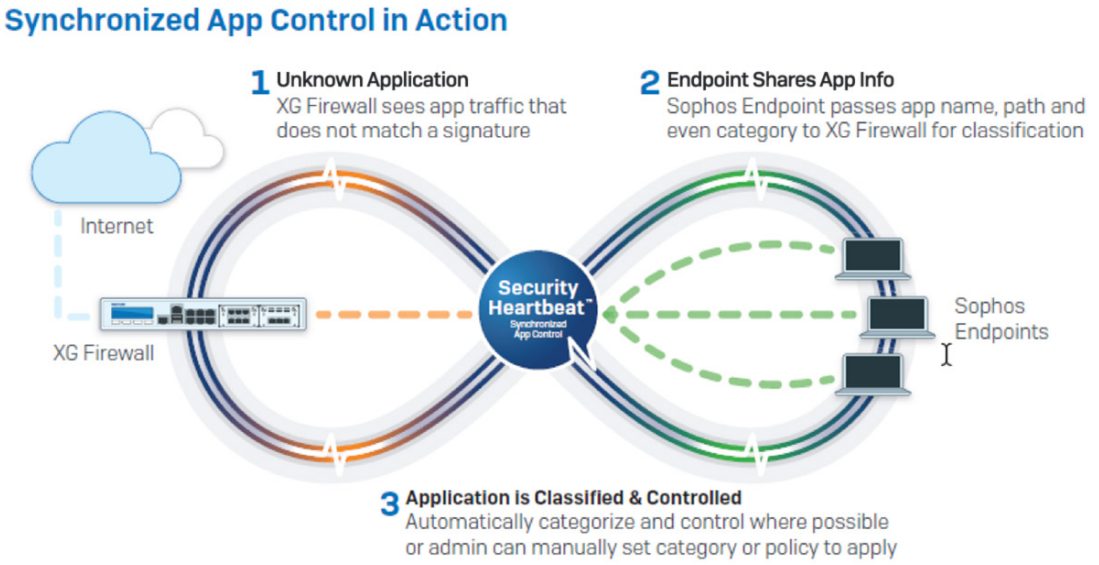


Sophos Synchronized App Control (同步應用程式控制) 會顯示所有網路應用程式

同步安全創新技術中的 Security Heartbeat™ 可將由 Sophos Central 管理的端點與 Sophos XG Firewall 相連，共享端點健康狀態，以便即時識別出面臨風險的系統。當端點或防火牆偵測到威脅時，就會即時發出流量燈號指示和警示，立即識別出相關的電腦、使用者和處理序。Security Heartbeat 最重要的優點之一，可能是防火牆可以在防火牆規則中包含端點健康狀態，以便實現自動回應，限制存取或者完全隔離被破壞的系統，直到清理完畢為止。藉此可將回應時間從幾小時縮短到幾秒鐘，並有助於降低感染擴散到網路其他部分的風險。

[1] 使用 XG Firewall 和 Sophos Endpoint 搭配啟用 Synchronized App Control 的 Sophos 客戶。

另一個同步安全創新是 Synchronized App Control (同步應用程式控制)。正如名稱所示，Synchronized App Control 可利用 Sophos 獨特的同步安全生態系統有效且簡潔地解決問題，在網路上識別未知、隱匿型或自訂應用程式的流量。Synchronized App Control 利用其與端點的資訊共享能力來確定網路上無法識別的應用程式流量的來源，可以去除掉今日覆蓋在網路上的層層面紗。



這是自從構思新一代防火牆以來，在網路應用程式可見度和控制方面的第一個重大突破。

當受 Sophos Central 管理的端點連接到有 XG Firewall 的網路時，它將會建立 Security Heartbeat™ 連線以共享健康和安全狀態以及遙測功能。此外，端點還將使用此一連線與防火牆共享所有網路應用程式的身分。

當應用程式是隱匿性、自訂、新建立或使用通用連線時，防火牆將無法使用傳統的特徵碼技術來確認應用程式的身分，此時端點提供的應用程式資訊將可用於識別、分類和控制這些應用程式。如果可行，由端點分享資訊得知的應用程式將被自動分類到適當的類別。接著可以自動對新識別和分類的應用程式套用已經在防火牆上實施的任何應用程式控制政策。

例如，一個具隱匿能力的 BitTorrent 用戶端將被自動分類到對等的應用程式類別。如果防火牆實施了一個阻擋點對點應用程式的應用程式控制政策，則會自動阻擋新的 BitTorrent 流量，而且無須任何網路管理員的介入。

另一個惡名昭彰的問題應用程式是 Psiphon，它會利用各式各樣連線方式，相當有效地躲避防火牆控制。使用 Synchronized App Control 可立即將它揭露出來，讓您得以輕鬆加以阻擋。

效益

「**90%** 的 Sophos 客戶表示，他們現在對網路流量擁有更大的控制權。」[2]

識別未知的應用程式

Synchronized App Cointrol 可發現網路上所有目前無法看到的應用程式，包括所有新的應用程式以及通常使用加密技術隱匿防火牆控制的通道、代理和 VPN 應用程式。這產生了一個巨大的盲點，以及各種合規性、效能和安全的風險。如果目前擁有可以阻擋或流量塑型這類應用程式的政策，被新識別出來並分類到某類別的應用程式將被自動套用相同的政策。此外，可以容易地識別出相關的使用者和主機，以便在可行時進行管理和調校。

排定自訂應用程式的優先性

Synchronized App Control 將可立即識別出目前防火牆無法看掉的自訂業務應用程式，例如財務、客戶關係管理、企業資源規劃、製造和其他對貴組織非常重要的網路應用程式。Synchronized App Control 首次提供應用程式流量塑型和 QoS 政策的機會，以確保這些關鍵性應用程式可以獲得適當的優先性和最佳效能。

控制隱匿型應用程式

Synchronized App Control 會自動發現所有不斷改變連線和通訊方式的隱匿型應用程式，以躲避偵測和控制。實際上，Synchronized App Control 一勞永逸地終結了這些手法。無論這些應用程式試圖如何隱匿，它們都無法逃避 Synchronized App Control 的掌握。

[2] 使用 XG Firewall 和 Sophos Endpoint 搭配啟用 Synchronized App Control 的 Sophos 客戶。

總結

新一代防火牆無法偵測隱藏在組織網路內的寄生應用程式，這將使這些組織面臨潛在的合規性違規和法律問題，而且使安全置於風險中並導致頻寬浪費。

Sophos打開了探照燈，讓這些應用程式無所遁形；您對網路上執行的應用程式將擁有100%的可見度，因此可以視需要設定應用程式優先順序、指派及阻擋應用程式。這是網路可見度和控制方面的一個重大突破，遠勝過其他還在迷霧中的新一代防火牆。

「沒有其他公司能在端點與網路安全性產品之間提供這種類型的通訊。」

Chris Christianson
IDC 安全性方案
副總裁