SOPHOS

Security made simple.

解決方案簡介：XG Firewall

防火牆正在走向一個與過去截然不同的發展。我們看到了威脅環境近期的轉變， 以及安全系統的數量和複雜性急劇增加。這些變化加上所產生的大量資料，造成 了一種危險的情況。我們必須採取一種全新的網路安全作法，一種可以使安全系 統協同工作的方法。這種作法不僅可以簡化工作流程，還能透過大量資料進行剖 析，以便將注意力集中在重要的事情上。為此我們需要安全整合的新方法、新的 管理系統，以及識別並回應風險和威脅的新方法。

目錄

現今的防火牆

早期的防火牆是在較低的網路堆疊層運作，可根據連接埠和通訊協定檢測提供基本路由以及封包篩選，以轉送或捨棄流量。這些防火牆有效地阻止了駭客常用的網路入侵嘗試。

由於威脅已經從直接攻擊網路轉變成感染網路內的系統(通常是透過入侵應用程式和伺服器中的弱點，或利用社交工程透過電子郵件或受感染的網站建立據點)，因此網路安全不得不隨之進化。長期下來，企業不得不為入侵防禦、網頁篩選、反垃圾郵件、遠端存取(VPN)，以及 Web 應用程式防火牆(WAF)增加額外的網路安全設備。UTM(統一威脅管理)設備從管理多種網路安全產品的重擔演變而來，因此 UTM 解決方案允許組織將一切整合到單一設備中。

防火牆技術也在不斷發展，同時將防禦層次提升到第 7 層以上，以識別並控制特定應用程式的流量。防火牆也發展成整合多種技術，以便更深入地檢測網路封包的內容並尋找威脅。這些防火牆還可以根據原始使用者或應用程式(而不只是流量類型)控制流量。這種從連接埠和通訊協定轉向應用程式和使用者的改變催生出一種新的網路保護類型：「新一代」防火牆。

新一代防火牆是包括傳統狀態式防火牆檢查，以及包含入侵防禦、應用程式感知和以使用者為基礎之政策的深度封包檢查的防火牆，而且能夠檢測加密的流量。

網路安全持續不斷地變化和發展，以應對一直在演變的威脅環境。諸如勒索軟體和殭屍網路惡意軟體之類的新型威脅比以往更進階、更具躲避能力，而且更有針對性。這些進階型持續威脅(APT)使用的技術可以讓每個執行個體都是全新的零時差威脅，這對使用特徵碼為偵測基礎的防禦系統而言是一項嚴峻的挑戰。

在任何時候，大多數的組織網路上都存在著一些已經遭駭的系統，這些系統可能是 API 或僵屍網路的受害者，而且自己幾乎毫無所悉。遺憾的是，這是一個普遍而廣泛的問題。

目前威脅與網路環境的性質是創造對網路安全方法進行根本性改變的需求。

第一：網路安全系統現在必須整合新的技術，以便在不使用傳統防毒特徵碼的情況下進行識別網路裝載中的惡意行為。以往大型企業才能夠負擔的起如沙箱之類的解決方案，直到最近對於中小型組織來說已經變得非常經濟實惠，而且現在是防禦新型惡意軟體的重要組成部分。

第二：曾經是受到隔離且獨立的安全系統(如防火牆和端點)現在必須整合在一起共同作業，才能在威脅可能造成重大損害之前，快速且有效率地偵測、識別並回應它們。

第三：由於特徵碼型引擎越來越無法識別最新的應用程式通訊協定、自訂應用程式，以及大量使用 HTTP/HTTPS 通訊協定的應用程式，因此需要新的動態應用程式控制技術，才能正確識別並管理未知的應用程式。

更糟的是，大多數的新型防火牆產品越來越複雜，通常必須使用數個個別但整合不良的解決方案，才能解決不同的威脅管道和合規性需求。因此，一般網路管理員的管理工作已經達到難以負擔的程度，而且這些系統產生的資訊和資料量也難以消化。

事實上，最近一項針對 IT 管理員的防火牆滿意度調查發現，目前大多數使用中的防火牆有多個常見的問題：

- 需要花費非常多的時間查詢，才能取得所需的資訊
- 他們無法充分了解網路上的威脅和風險
- 他們具備多種功能，但是非常困難才能弄清楚如何使用這些功能

Sophos XG Firewall

Sophos XG Firewall 從一開始就專為解決現有防火牆現今的主要問題而開發，同時提供專為因應不斷演變的威脅和網路情勢所設計的平台。XG Firewall 為您帶來識別隱藏的威脅、保護您的網路，以及識別並回應威脅的全新作法。

XG Firewall 可以對高風險使用者、不請自來的應用程式、可疑的裝載程式(Payloads)和持續性威脅提供無可比擬的可見度。它可以緊密地整合一套容易設定與維護的完整新型威脅防護技術。不像之前的其他任何防火牆，XG Firewall 可與網路上的其他安全系統進行通訊，使其有效地成為受信任的實施點，以遏制威脅並阻擋惡意軟體自動且即時地從網路散播或洩漏資料。

Sophos XG Firewall 與其他網路防火牆相比，具有三大優勢：

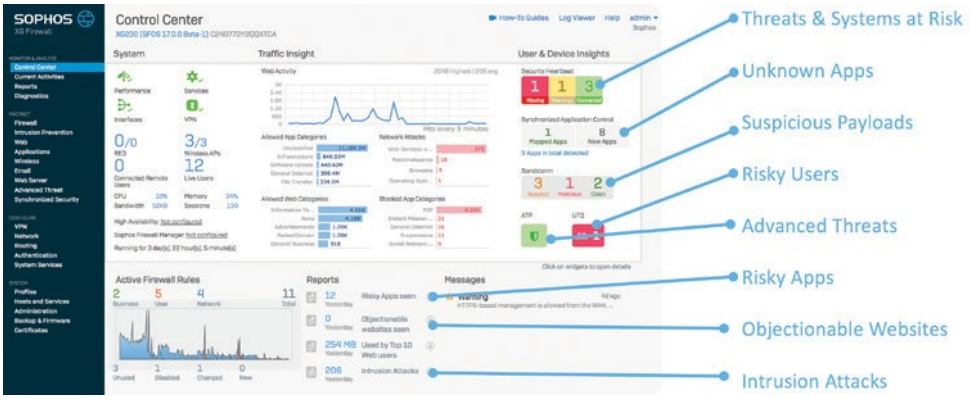
1. 揭露隱藏的風險：XG Firewall 在揭露隱藏的風險方面，使用視覺化的儀表板、立即可用的報告，以及獨特的風險識別，讓 XG Firewall 比其他防火牆做得更好。
2. 阻擋未知威脅：XG Firewall 利用一套非常容易設定與管理的完整進階防護，在阻擋未知威脅方面比其他防火牆更容易而且更有效率。
3. 自動回應事件：歸功於 Security Heartbeat，具有同步安全的 XG Firewall 會自動回應網路上的事件。

揭露隱藏的風險

對於新型防火牆來說，能夠透過所收集的大量資訊剖析、關聯資料(如果可能)，並只摘要出需要回應的最重要資訊非常重要，最好能防範於未然。

控制中心

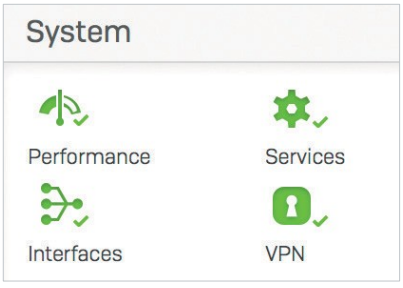
XG Firewall 的控制中心為您網路上的活動、風險和威脅提供前所未有的可見度。

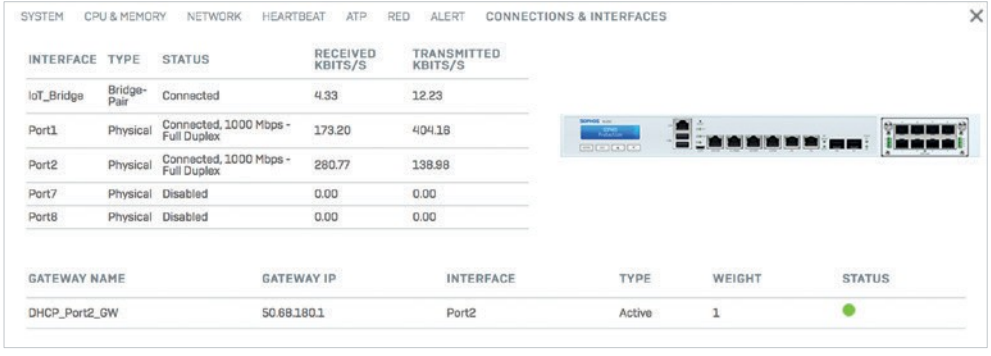


它使用「交通號誌」風格的指標，讓您的注意力放在最重要的事項上：

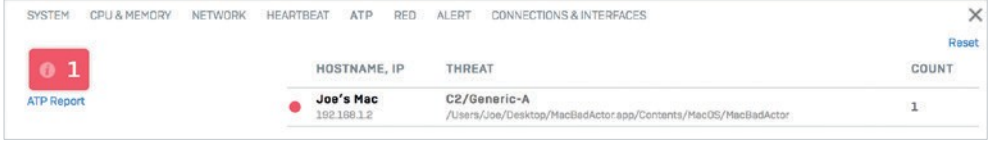
如果亮紅燈，表示需要立即注意。如果亮黃燈，表示可能有問題。如果亮綠燈，則表示不需要採取任何進一步的動作。

此外，控制中心上的每個桌面工具都提供了額外資訊，只要按一下該桌面工具，即可輕鬆顯示。例如，只要按一下控制中心上的「介面」桌面工具，就可以輕鬆取得裝置上的介面狀態。

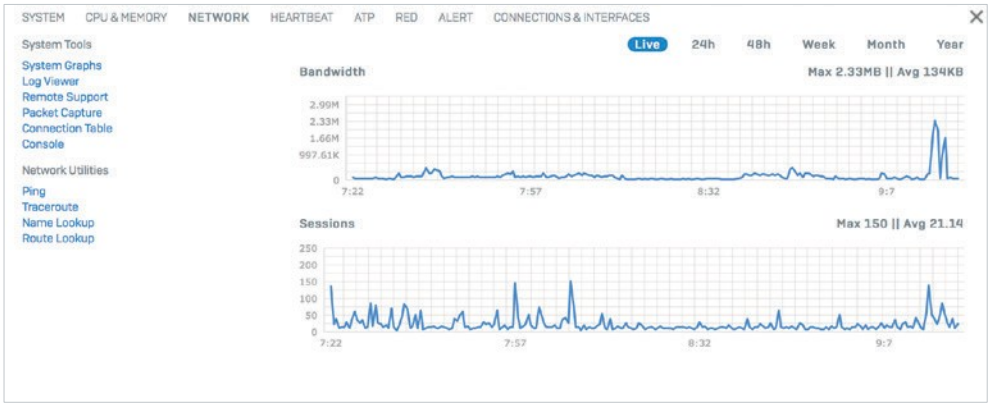




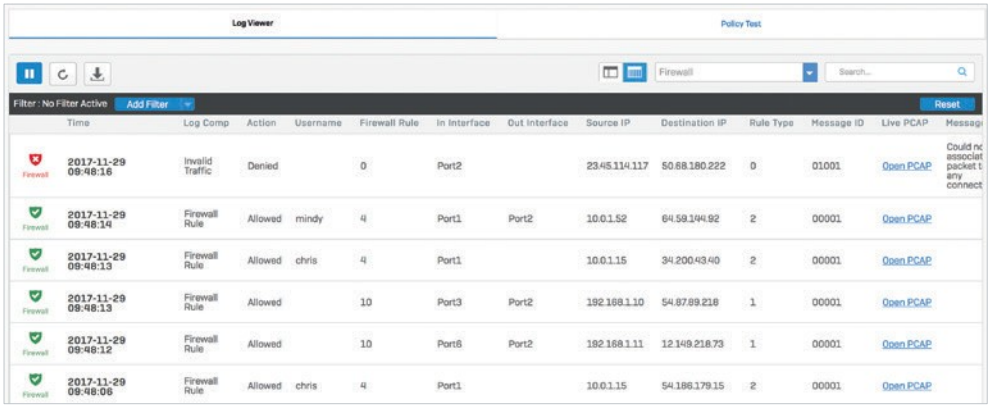
只要按一下儀表板中的 ATP(進階威脅防護)桌面工具，也可以輕鬆確定進階威脅的主機、使用者和來源。

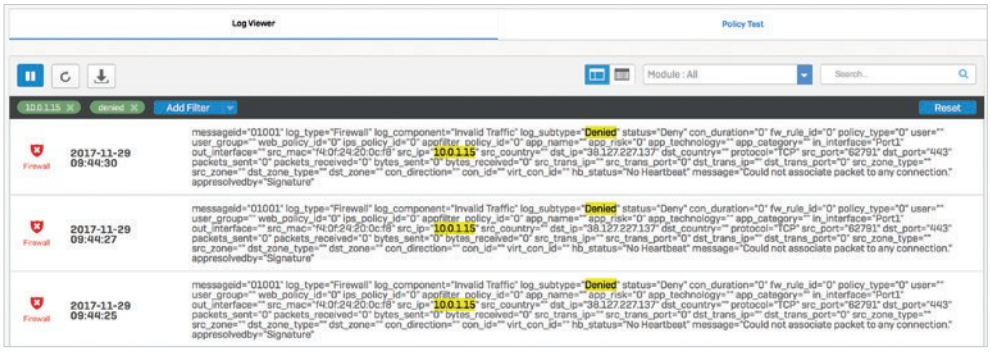


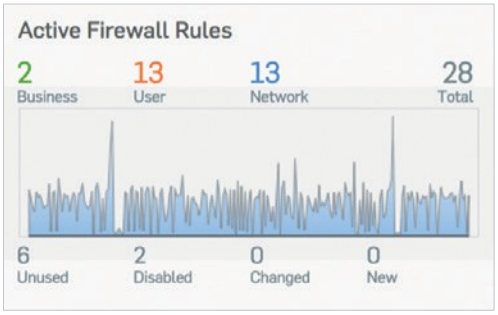
系統圖表可選擇時段進行查詢來顯示一段時間的效能，無論是最後兩小時到上個月或是到去年。此外，這些圖表還可以讓您快速存取常用的疑難排解工具。



只要按一下滑鼠，就可以從每個畫面取得即時日誌檢視器。您可以在新視窗中開啟該檢視器，就可以在主控台上作業的同時，留意相關的日誌。即時日誌檢視器提供兩種檢視模式：一種是較簡單的欄位型格式(依防火牆模組)，另一種是更詳細的統一檢視模式，其中包含功能強大的篩選和排序選項，可將整個系統的日誌彙總成單一即時檢視。







如果您屬於大多數的網路管理員，可能會懷疑防火牆規則是否太多、哪些是真正必要的防火牆規則，以及哪些是實際上不會用到的防火牆規則。有了 Sophos XG Firewall，您就無須猜疑了。

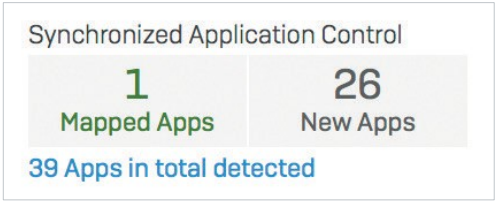
「使用中的防火牆規則」桌面工具可針對防火牆處理的流量，依下列規則類型，顯示其即時圖表：商業應用程式、使用者和網路規則。它也可以依狀態顯示使用中的規則計數，包括您有機會對未使用規則進行管理。

如同控制中心的其他區域般，按一下其中任何一個區域將會深入探索，在此案例中，可以看到依規則類型或狀態排序的防火牆規則表。

同步應用程式控制

現今每個新一代防火牆的應用程式控制問題都是，無法識別大部分的應用程式流量：未分類、未知、通用 HTTP 或通用 HTTPS。

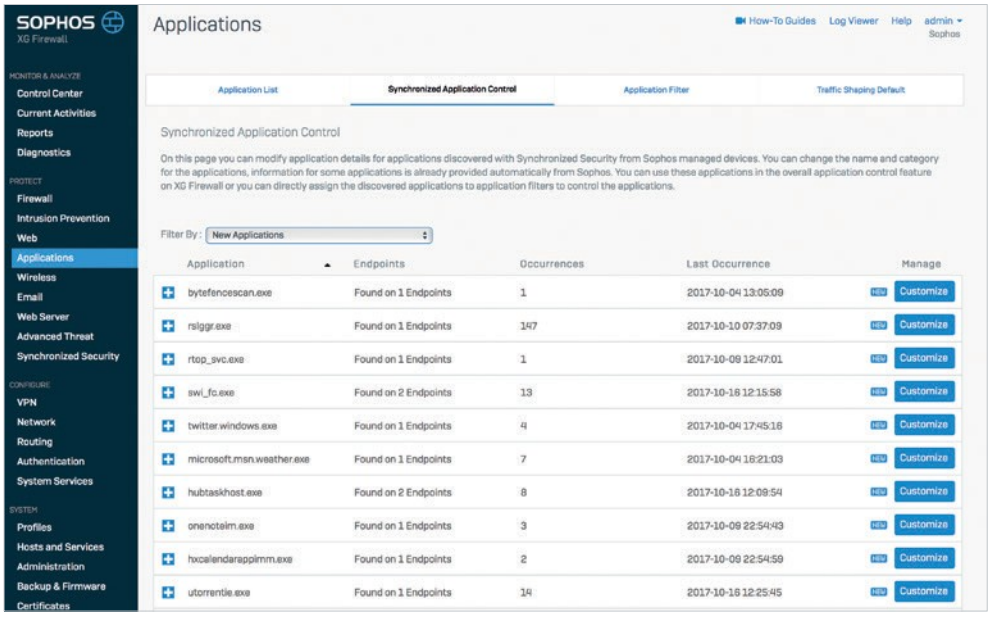
原因很簡單，因為所有防火牆應用程式控制引擎都依賴特徵碼和模式來識別應用程式。此外，如同您所預料，任何自訂的垂直市場應用程式(Vertical market application)例如醫療或財務應用程式，絕對都不會有特徵碼，而部分隱匿性應用程式(如 BitTorrent 用戶端或 VoIP 和即時通訊應用程式)會一直改變其行為與特徵檔，以逃避偵測和控制。許多應用程式現在使用加密用來躲避偵測，而某些應用程式只是使用類似於通用網頁瀏覽器的連接，通過防火牆向外進行通訊，因為連接埠 80 和 443 在大多數的防火牆上通常暢通無阻。



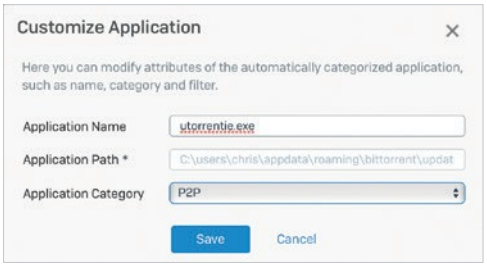
最終的結果是完全看不到網路上的應用程式，而看不到就無法控制。

這個問題的解決方法非常簡潔且有效：同步應用程式控制，其使用我們獨特的同步安全連線搭配 Sophos 受管理端點。

當防火牆看到無法利用特徵碼識別的應用程式流量時，可以詢問端點哪個應用程式產生該流量。接著，端點可以分享可執行檔、路徑，通常還有其類別，並將該資訊傳回防火牆。之後在大部分的情況下，防火牆就可以利用該資訊自動分類並控制該應用程式。



如果 XG Firewall 無法自動判斷正確的應用程式類別，系統管理員可以設定所需的類別，或將應用程式指派給現有的政策。



一旦將應用程式分類(自動或透過網路管理員)之後，該應用程式就會受到與該類別中其他所有應用程式相同的政策控制，使其非常容易阻擋您不需要的所有無法識別的應用程式，並優先考慮您需要的應用程式。

同步應用程式控制是應用程式可見度和控制方面的一項突破，可對在網路上運作的無法識別且不受控制的所有應用程式提供絕對的明確性。

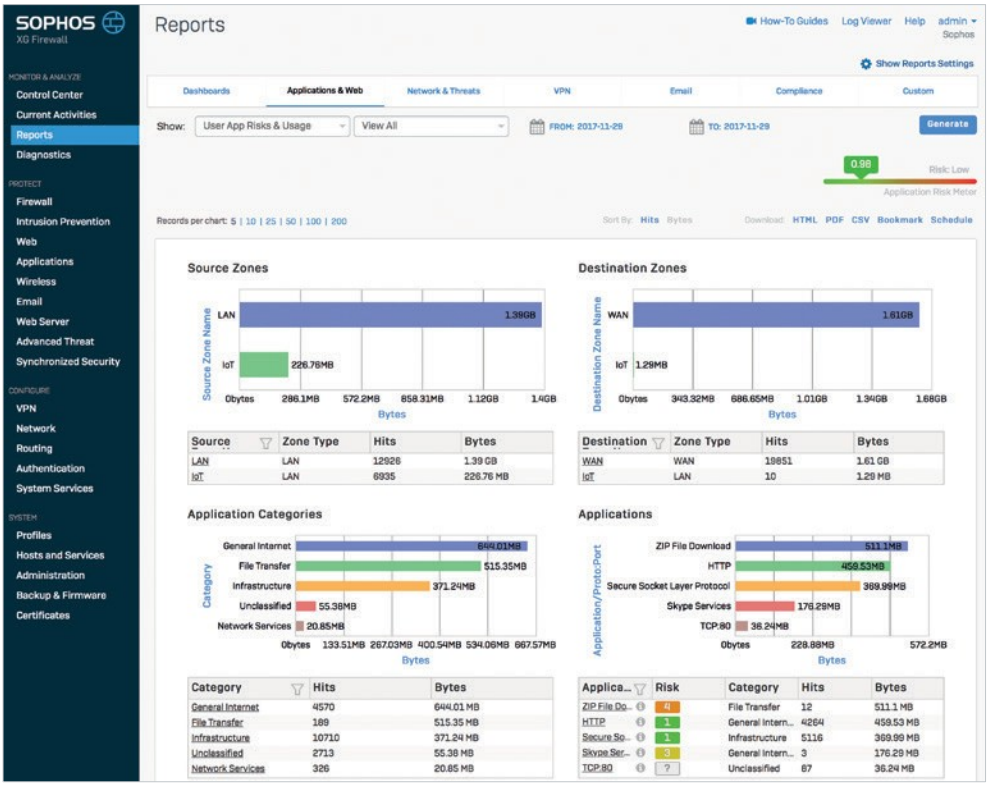
風險最高的使用者 研究證明，使用者是安全鏈中最薄弱的環節，人類行為模式則可以用來預測和預防攻擊。此外，使用模式有助於說明公司資源的利用效率，以及使用者政策是否需要進行微調。

使用者威脅商數(UTQ)可協助安全管理員根據可疑的網路行為、威脅和感染歷史記錄，找出暴露在風險下的使用者。使用者的 UTQ 風險分數高，可能表示由於缺乏安全意識、惡意軟體感染，或蓄意的惡意行為而導致的意外行為。

知道造成風險的使用者和活動有助於網路安全管理員採取所需的動作。例如教育風險最高的使用者，或實施更嚴格或更適當的政策，使其行為受到控制。

立即可用的報告

XG Firewall 在防火牆和 UTM 產品中是獨一無二的，可免費提供全方位且立即可用的報告。當然，如果您想要在單獨的伺服器或設備上做報告，我們也提供一個獨立報告平台 Sophos iView 且其可以收集多台防火牆的報告。但大多數的中小型組織都非常喜歡能夠在單一設備上，免費取得完整的歷史報告。



XG Firewall 提供了一套完整的報告，方便按類型組織，而且有數個內建的儀表板可供選擇。在防火牆的所有區域(包括流量活動、安全、使用者、應用程式、Web、網路、威脅、VPN、電子郵件以及合規性)都有數百個可自訂參數的報告。您可以輕鬆地排定將定期報告以電子郵件傳送給您或您指定的收件者，並將報告儲存為 HTML、PDF 或 CSV。

阻擋未知威脅

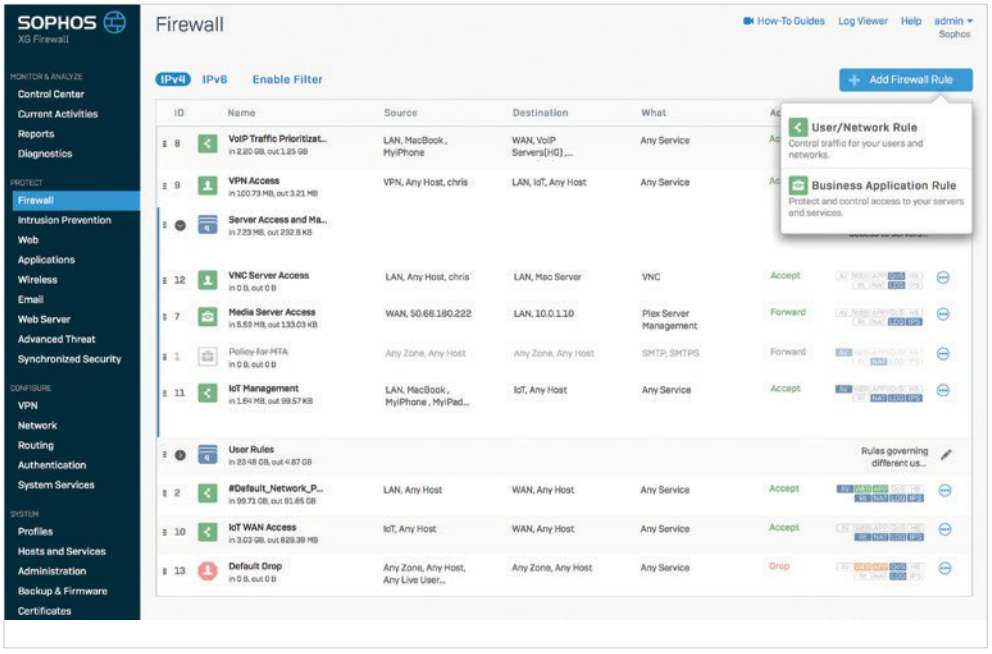
防禦最新的網路威脅需要所有相關的技術共同運作，並由網路管理員指揮。遺憾的是，大部分的防火牆產品更像是一邊雜耍一邊演奏的一人樂隊，也就是在一個區域設定防火牆規則、在另一個區域設定網頁政策、在其他區域設定 SSL 檢測，並在產品完全不同的部分設定應用程式控制。

在 Sophos，我們不僅相信您需要最先進的保護技術，而且我們也相信，該技術必須易於設定與管理日常工作，因為設定錯誤的保護往往比沒有保護更糟糕。

讓安全變得簡單的承諾一直是 Sophos DNA 的關鍵部分。但或許更重要的是，Sophos 非常樂意接受變化，並採取大膽的步驟以不同的方式運作，以提供更好的保護和更佳的使用者體驗。

XG Firewall 用不同的方式完成工作，這是非常重要的。

統一式規則管理 管理多個規則、政策和安全設定分佈在各個功能區域的防火牆可能非常具有挑戰性，因為這通常需要有數個不同的規則來提供必要的保護。



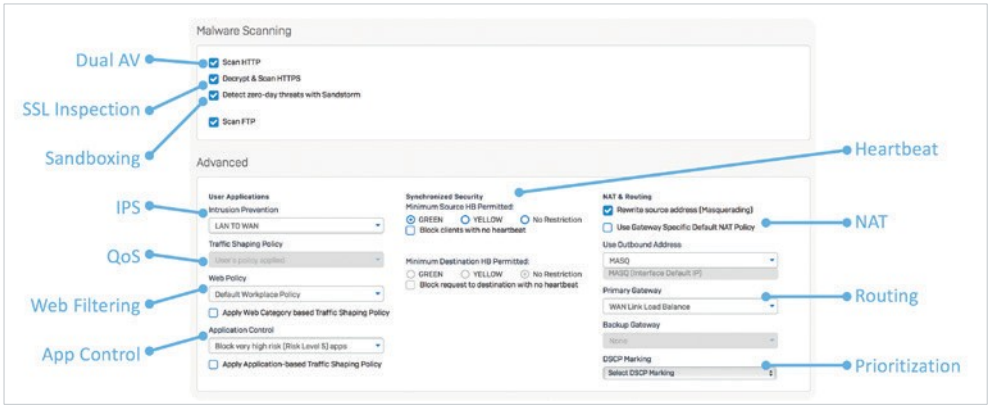
藉著新推出的 XG Firewall，我們徹底重新思考了防火牆規則的組織方式，以及安全態勢的管理方式。我們將所有防火牆規則和實施管理集合到一個統一的畫面中，而不必在管理控制台上尋找適當的政策。您現在可以在同一個頁面位置上進行檢視、篩選、搜尋、編輯、新增、修改所有防火牆規則。

將規則針對使用者、商業應用程式、NAT 和網路分門別類，讓您更容易僅檢視所需的政策，同時提供一個便於管理的畫面。

指標圖示可提供有關政策的重要資訊，例如類型、狀態、實施等等。

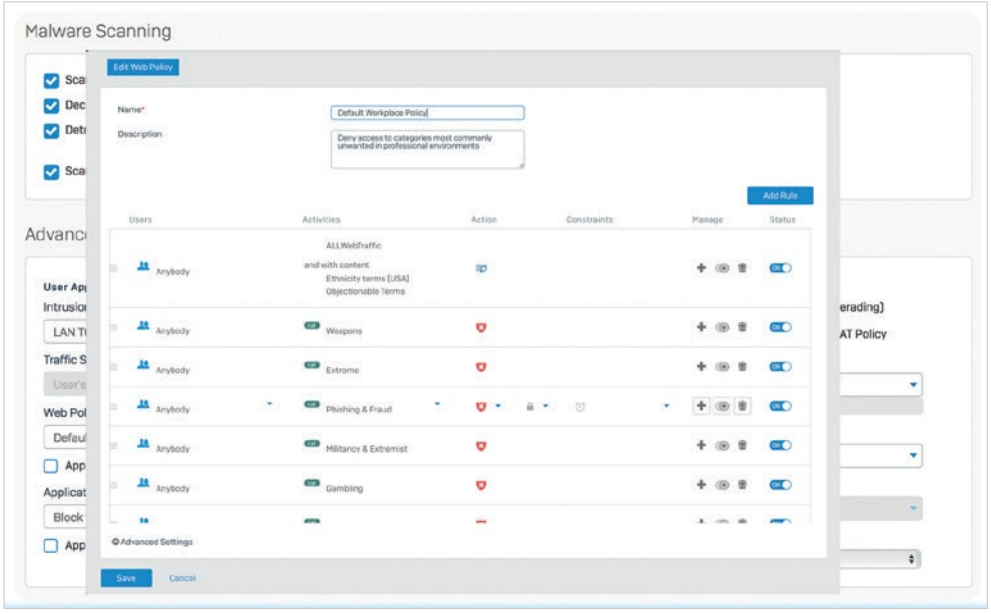
管理安全態勢快速概覽

XG Firewall 可在單一畫面上輕鬆設定與管理所需的所有新型保護。

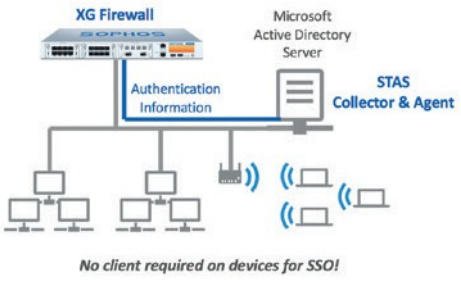


您可以針對防毒、SSL 檢測、沙箱、IPS、流量塑型、網頁和應用程式控制、活動訊號、NAT、路由，以及優先順序，設定與管理安全及控制，全部都在單一位置，而且全部都是以規則、使用者或群組為基礎。

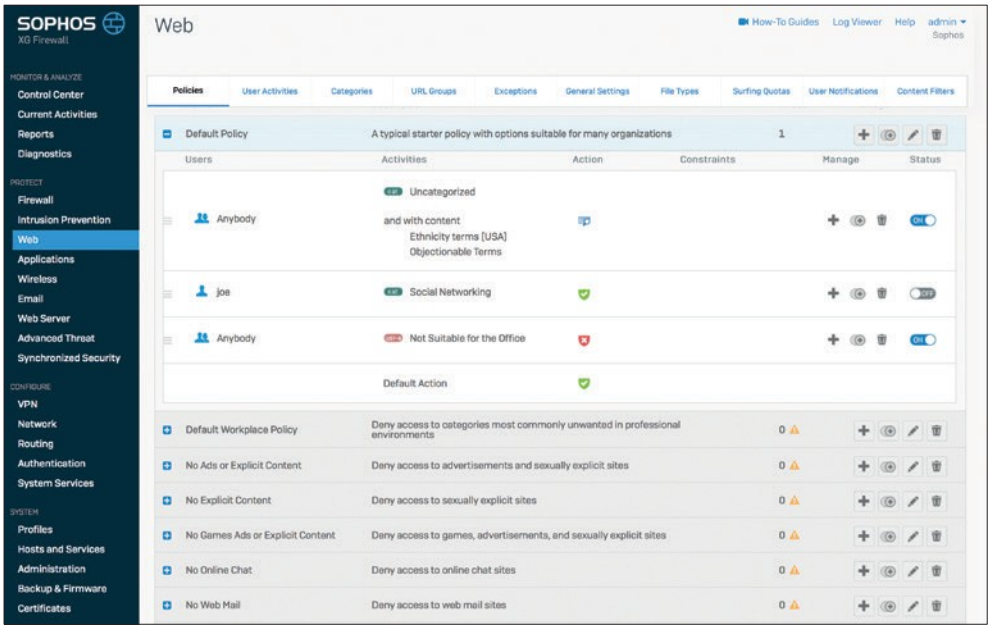
此外，如果您想要查看任何監管的政策正在執行哪些操作，甚至進行變更，則可以在原地進行編輯，而不必離開防火牆規則並存取產品的其他部分。



彈性的驗證選項可讓您輕鬆得知使用者的身分，並包含目錄服務，例如 Active Directory、eDirectory 和 LDAP，以及 NTLM、RADIUS、TACACS+、RSA、用戶端代理程式或管制入口網站。而 Sophos Transparent Authentication Suite (STAS) 則可以與 Microsoft Active Directory 之類的目錄服務整合，以便進行簡單、可靠、透明的單一登入驗證。



企業級安全網頁閘道 網頁保護與控制是任何防火牆中不可或缺的功能，但遺憾的是，這在大多數的防火牆實作中都是事後諸葛。我們打造企業級網頁保護解決方案的經驗為我們提供了實作這種通常僅在企業 SWG 解決方案中才能找到的網頁政策控制的背景和技術訣竅，且其成本只要十分之一左右。我們實作了一種全新的自上而下的繼承政策模式，這使得建立複雜的政策變得簡單且直覺。大多數常見的部署(例如典型的工作環境、教育 CIPA 合規性等等)中都包含了預先定義的現成政策範本。也就是說，您可以利用隨手可得的簡單微調與自訂選項，立即達到並符合標準。



事實上，我們知道網頁政策是防火牆日常工作中經常發生變化的因素之一，這就是為什麼我們在 XG Firewall 裡面導入了企業級的網頁保護方案，使您可以根據使用者和業務需求，輕鬆管理與調整的原因。您可以輕易地自訂使用者和群組、活動(包括 URL、類別、內容篩選與檔案類型)、動作(阻擋、允許或警告)，以及新增或調整時間和日期的限制。

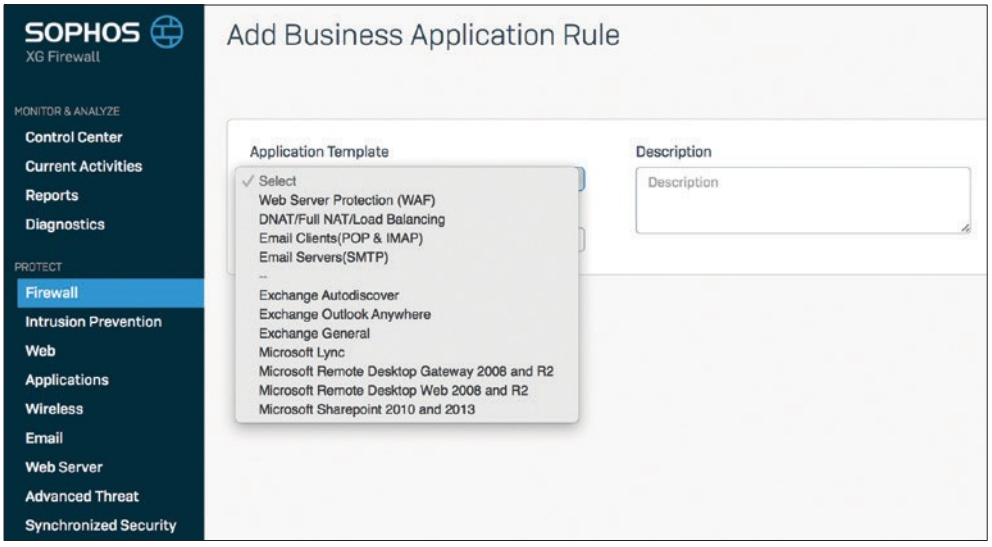
網頁政策現在包含記錄和監視，甚至能夠根據關鍵字清單來強制執行動態內容相關政策的選項。此功能在教育環境中特別重要，可確保線上兒童安全，得知哪些學生使用關鍵字來查詢自我傷害、霸凌、激進或其他不當內容相關。關鍵字庫可以上傳到防火牆，並套用至所有網頁過濾政策作為附加條件，其動作包括記錄和監控，或阻擋包含相關關鍵字的搜尋結果或網站。

提供全面的報告，以識別搜尋或取用相關關鍵字內容的關鍵字比對和使用者，以便有風險的使用者成為真正的問題之前就可以主動介入。

這是簡化過的強大網頁政策。

商業應用程式和 NAT 規則範本

嘗試為 Exchange、SharePoint 或網頁伺服器等設定網頁應用程式防火牆規則的任何人都知道這具有多大的挑戰性以及多容易發生問題。設定的範圍和數量撲朔迷離。但是預先定義的政策範本可協助您快速、輕鬆且有信心地保護常見的商業應用程式伺服器。只要從下拉式清單中選擇所需的伺服器類型即可。



一旦選擇需要使用防火牆保護的其中一個常見商業應用程式之後，設定畫面就會預先填入適當的欄位，讓您的工作變得更簡單。之後，您只要輸入網域、路徑和伺服器資訊之類的一些詳細資訊，就完成了。

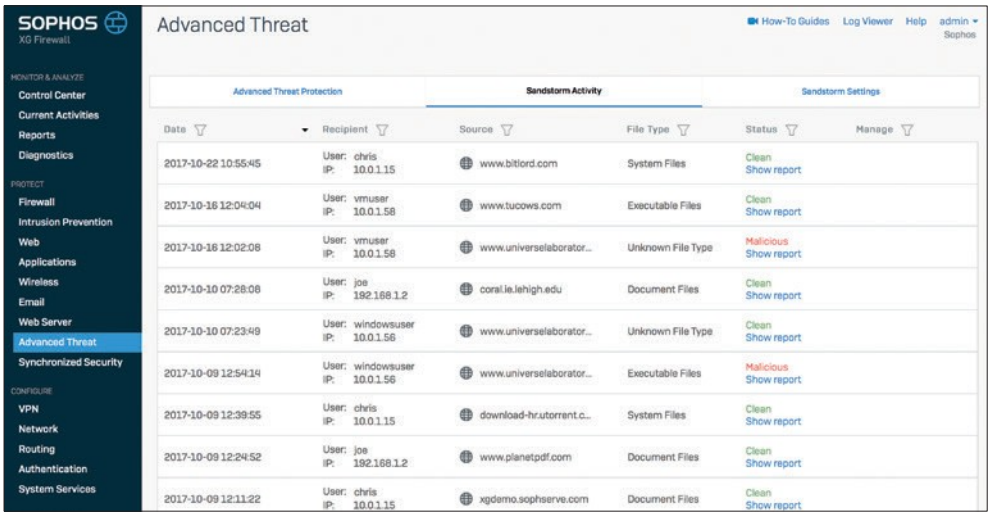
相較於必須在其他任何產品中設定通常需要數個畫面才能完成的 WAF 政策，如果沒有 XG Firewall，設定會更為複雜且令人困惑。

Sandstorm 沙箱技術

隨著勒索軟體等進階威脅變得更有針對性和隱匿性，因此迫切需要以行為為基礎的裝載分析(Payload analysis)。一直以來，只有最大型的企業才負擔得起提供這種保護所需的沙箱技術。但是現在，歸功於 Sophos Sandstorm 之類的雲端型沙箱解決方案，即使是最小型的企業，也負擔得起。最近一段時間，中小型組織開始採用基於深度學習技術的沙箱，已經遠遠超過了幾年前企業部署數百萬美元的專用內部部署沙箱解決方案。

Sophos Sandstorm 提供了簡單而實惠的終極雲端沙箱解決方案，同時透過深入了解潛伏在電子郵件和網頁裝載中的最新零時差威脅，提供基本防護。Sophos Sandstorm 與 XG Firewall 緊密整合，而且安裝非常簡單，但是由於前者是以雲端為基礎，因此不需要額外的軟體或硬體，也不會影響防火牆的效能。在雲端沙箱中會自動分析可疑的電子郵件附件和網路下載的檔案，以便在它們進入網路之前判斷是否安全。

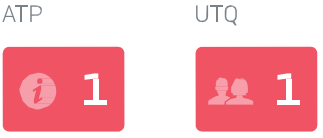
Sophos Sandstorm 在 XG Firewall 控制中心上提供一個裝載分析(Payload analysis)的總覽，並針對防火牆分析並處理過的所有檔案和威脅，提供豐富而詳細的報告。



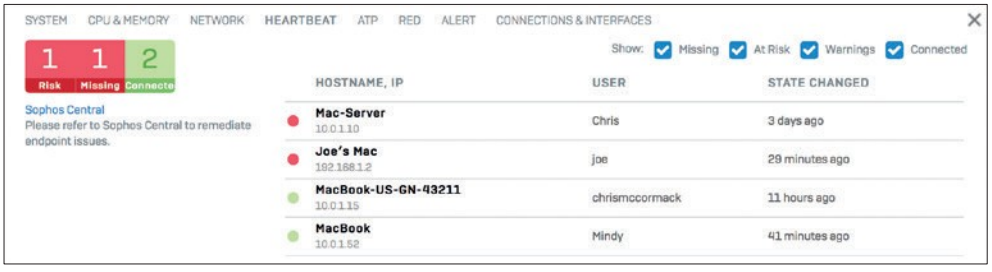
由於沙箱技術變得越來越普遍，因此 XG Firewall 和 Sophos Sandstorm 以非常合理的價格提供了最簡單的保護，使每個人都能夠負擔得起而且相當有效。

進階型威脅防護

進階型威脅防護對於識別 APT、殭屍程式和潛伏在網路上的其他惡意軟體而言是不可或缺的。XG Firewall 使用惡意流量偵測、殭屍網路偵測，以及命令控制(C&C)回傳流量偵測的複雜組合。它結合了 IPS、DNS 和 URL 分析，以識別回傳流量，並立即識別受感染的主機，以及使用者和處理程序。



這個複雜的基礎防護技術可以針對網路上的進階威脅，提供非常簡單但實用的檢視。如稍早所提及，XG Firewall 控制中心可針對網路上的進階威脅，顯示簡單的「交通號誌」風格指標。當燈號為紅色時，表示防火牆已經識別並阻擋進階威脅。此外，如果您是使用 Sophos Synchronized Security 搭配 XG Firewall，則可以更進一步隔離受感染的系統，直到清理完成為止，以防止資料洩露或與駭客的伺服器進行通訊。



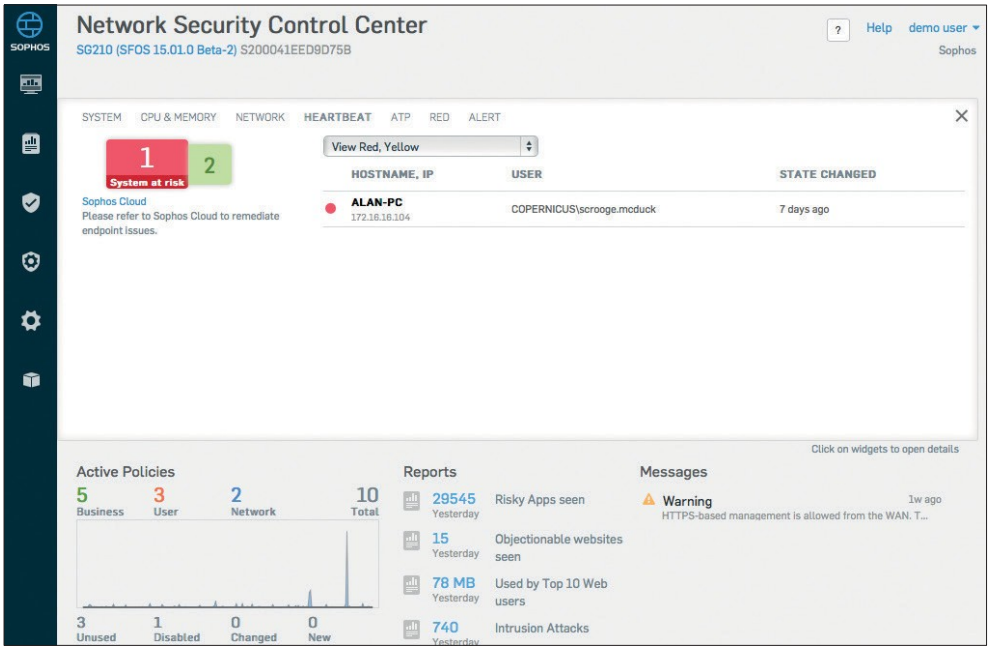
自動回應事件

網路管理員最常要求的防火牆功能之一，就是能夠自動回應網路上的安全事件。

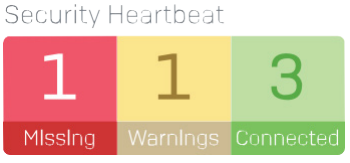
Sophos XG Firewall 是唯一一款能夠完整識別網路上的感染來源，並自動限制存取其他網路資源做為回應的網路安全解決方案。這是透過我們獨一無二的 Sophos Security Heartbeat™所實現，它會共享 Sophos 端點與防火牆之間的遙測功能和健康狀態。XG Firewall 會以獨家專門的技術，將連線主機的健康狀態整合到防火牆規則中，讓您自動限制對任何受感染系統之敏感網路資源的存取，直到清理完成為止。

Security Heartbeat

Sophos Security Heartbeat 會使用您端點與防火牆之間的安全連結，即時分享情報。這個同步安全產品的簡單步驟(以往是獨立運作的)，可建立更有效的保護，抵禦進階惡意軟體和目標式攻擊。



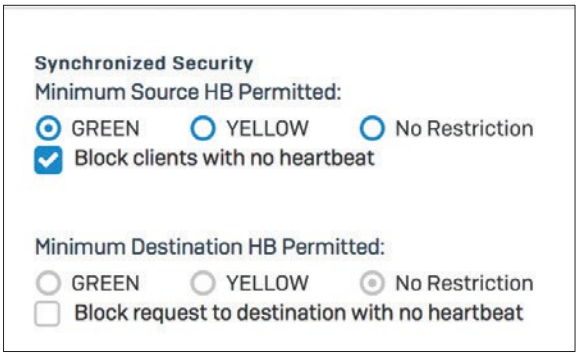
Security Heartbeat 不僅可以立即識別進階威脅是否存在，還可以用來傳達有關威脅性質、主機系統以及使用者的重要資訊。或許最重要的是，Security Heartbeat 也可以用來自動採取動作，以隔離或限制對受感染系統的存取，直到清理完成為止。這項令人振奮的技術正在徹底改變 IT 安全解決方案識別和回應進階威脅的方式。



適用於防火牆後面受管理端點的 Security Heartbeat 可以處於下列其中一種狀態：綠色活動訊號狀態表示端點系統狀況良好，而且可以存取所有適當的網路資源。

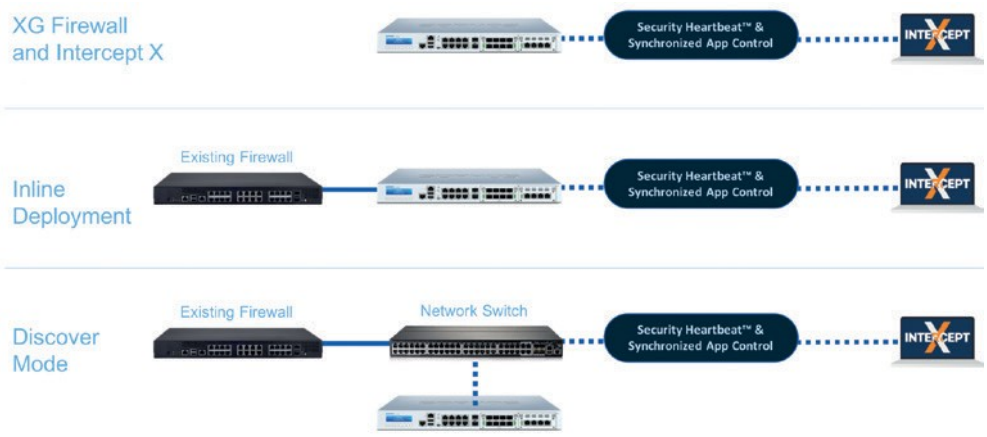
黃色活動訊號狀態表示系統中可能含有可能不需要的應用程式(PUA)、可能不符合規範，或可能有其他特定問題的警告。您可以選擇在問題解決之前，黃色活動訊號可以存取的網路資源。

紅色活動訊號狀態表示系統可能有受到進階威脅感染的風險，而且可能會嘗試回傳到僵屍網路或命令與控制伺服器。在防火牆中使用 Security Heartbeat 政策設定時，可以在清理完成之前，輕鬆地隔離具有紅色活動訊號狀態的系統，以降低資料遺失或進一步感染的風險。



只有 Sophos 可以提供諸如 Security Heartbeat 的解決方案，因為只有 Sophos 是端點和網路安全解決方案的領導者。雖然其他廠商都開始意識到這是 IT 安全的未來，而且正在爭先恐後地實施類似的解決方案，但它們都處於明顯的劣勢：它們沒有同時擁有業界領先的端點解決方案以及業界領先的防火牆解決方案可以整合在一起。

輕鬆地將 XG Firewall 加入至任何網路



我們最新的 XG 系列硬體設備提供了更為靈活的部署，現在所有 1U 機型都具有標準的開放旁路連接埠(Fail-open bypass)，而且新的 FleXi Port 模組也有提供，以便在最新的 2U 設備上也能啟用此功能。新的旁路連接埠(Fail-open bypass)可讓 XG Firewall 依照現有的防火牆，以橋接模式安裝，而且如果 XG Firewall 需要關機，或更新韌體進行重新開機，旁路連接埠(Fail-open bypass)將允許流量繼續通過，以確保網路不中斷。此功能允許使用完全沒有風險而且簡單的新部署選項，而不需要替換任何現有的網路基礎架構。更重要的是，我們的新一代端點保護 Intercept X 可與任何現有的桌面防毒產品搭配使用，從而在任何網路中部署完整的 Sophos Synchronized Security 解決方案，無需進行任何替換。讓安全變得更簡單。

關於湛揚科技

湛揚科技為SOPHOS台灣專業代理商，同時也為安克諾斯Acronis台灣總代理，協同通路合作夥伴為各產業使用者提供高效能的防毒、防火牆、備份解決方案，為企業與政府機關提供性價比最佳的資安服務及產品，建置最適合的防護及專業技術服務。如您對 SOPHOS 想瞭解更多，或進一步需求，歡迎洽詢湛揚科技，我們有專業資安團隊提供您詳細產品簡報，產品免費測試，讓您快速體驗SOPHOS強大有效的防護能力！

SOPHOS 專業代理商 湛揚科技 www.t-tech.com.tw
台北：(02)2735-3512 技服電話：(02)7718-5588
高雄：(07)972-7388 技服信箱：support@t-tech.com.tw