SOPHOS

Security made simple.

轉換到新世代端點安全防護

新世代防毒最佳作業準則

威脅的動態變化越來越快，迫使企業同時要防禦傳統惡意軟體和新型進階攻擊。因此越來越多企業需要且已經轉換到SOPHOS新世代端點安全防護，並獲得創新防禦保護杜絕加密勒索的威脅。本指南說明SOPHOS新世代端點安全防護如何提供您最需要的保護，並提供5個步驟輕鬆換裝SOPHOS防毒，讓您不再為日新月異的威脅而煩惱，加上湛揚科技專業用心的服務，給您最滿意的新世代防毒最佳作業準則。

更高明、更有效率的駭客 促使網路攻擊大幅成長[1]

面對網路攻擊大幅成長下的隱憂，例如，資料外洩、事件警示等等。企業必須更重視自身的資料保護工作。實際面的威脅動態變化比以往更加快速。根據Verizon 2015年資料外洩調查報告[2]中的資料顯示，持續增長的攻擊數量、快速的變化和複雜性，都令人為威脅環境感到十分擔憂。

- 在2014年，安全事件增加了26%，已確認的資料遺失則增加了55%。
- 在 60% 案例中，攻擊者可在數分鐘內入侵組織，造成損害性的破壞。
- 70-90% 的惡意軟體對許多組織來說都是第一次碰到並中毒。

此外，其實企業對於網路威脅的認識也繼續有所增長。引用自Verizon報告：「在2014年，紐約時報有超過700篇與資料外洩相關的文章，而前一年只有不到125篇。」相對的，對於有更廣泛員工人數的企業和主管來說，組織內部的網路威脅意識也正在上升當中。

安全防護成本不斷墊高

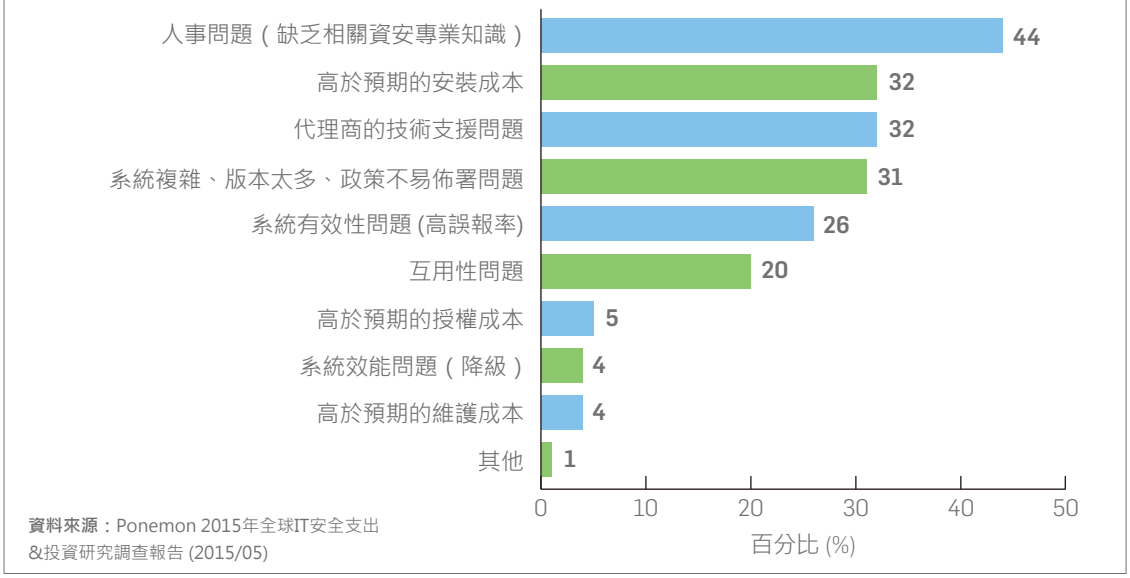
隨著企業內部的安全意識增強，企業持續增加IT安全支出也就不會讓人感到意外。根據Ponemon 2015年IT安全支出和投資的全球研究調查顯示[3]，46%的組織在過去兩年增加了安全防護支出，有50%預期在未來兩年會增加IT安全防護支出。

然而，Ponemon的研究中也提出關於安全投資運作上的問題：部分企業表示對於某些技術採購感到失望。根據受訪者表示在過去兩年之中，在支援安全技術的所有投資中平均有37%低於預期表現。

當被問到為什麼會對這些安全投資感到失望時，
依據Ponemon的研究調查顯示出的前五大問題原因如下(見圖1)：

1. 人員缺乏相關資安專業知識
2. 產品安裝成本
3. 代理商的技術支援
4. 系統複雜、版本太多、政策不易佈署
5. 系統有效性問題 (高誤報率)

圖表 1。為什麼企業對其在推動技術方面的投資感到失望。



資料來源：Ponemon 2015年全球IT安全支出&投資研究調查報告 (2015/05)

對於現在端點防護使用的失望

SOPHOS從新用戶中了解他們想要更換端點安全解決方案的因素，這些因素也印證了Ponemon研究報告中所提出的問題。其中包含了缺乏專業的客戶支援、產品複雜度、以及需要更廣泛的整合型防護。扣除以上問題之外，還有面對病毒爆發的無奈，和端點安全代理造成的效能緩慢問題。

告別過去的失望

考量到這些問題，要如何避免用戶對新安全投資的反感，幫助他們告別過去的失望？這方面想來應該很顯而易見， 企業需要開始仔細選擇與內部人員技能水平匹配的安全解決方案。

對於具有較少純熟IT安全資源的企業組織而言，自動化和易用性成為關鍵的選擇標準。此外，還需要密切留意代理商的支援服務，例如，服務適用的支援等級，以及根據現有用戶等級所能獲得提供的支援服務項目。最後，建議對整體解決方案成效進行更全面的評估。有效性關係到整個預防、偵測和修復技術的可用範圍。易用性關係到這些技術是否能夠輕鬆呈現自動化應用。效能表現關係到每個元件整合的完整性和對端點用戶產生的影響程度。

對於許多企業組織來說，SOPHOS Endpoint Protection新世代端點安全防護是一個告別傳統端點安全解決方案的絕佳選擇。如果上述問題在您衡量現有端點安全解決方案時有符合，那麼也許是一同加入到SOPHOS成千上萬用戶行列的時機到了。

SOPHOS 為端點提供最佳安全防護

為了與現今威脅相互抗衡，必須投資最有成效的IT安全解決方案，且可與現有的員工和專業人員一起使用。SOPHOS新世代端點防護不僅整合了各種先進的安全技術，還為您的企業組織提供智能情報和世界級的支援服務。

創新防護技術

SOPHOS將最新的進階威脅防禦與經過驗證的惡意軟體防護技術無縫結合：

Sophos System Protector
SOPHOS端點安全防護系統的核心是透過自動協調各種端點技術來優化保護

減少威脅感染機會	防範威脅和資料遺失	偵測進階威脅
• **應用程式控制** 按類別或名稱點擊阻擋應用程式。	• **弱點防護** 識別並阻擋嘗試利用應用程式或作業系統漏洞的行為。	• **進階分析** 使用行為和啟發式分析來識別未知（零時差）威脅。
• **網頁控制** 可在企業網路內或外實施以類別為基礎的網頁篩選。	• **網頁安全** 阻擋用於傳遞威脅的惡意指令碼和重新導向。	• **執行模擬** **模擬在受保護環境中執行的軟體，以驗證是否存在惡意行為。**
• **網址信譽** 阻擋已知的惡意網頁，並結合檔案屬性來阻止網路傳遞的威脅。	• **裝置和資料控制** 管理存取卸除式裝置和行動裝置的動作，並使用預設或自訂規則進行資料遺失防範。	• **惡意流量偵測** **當惡意軟體嘗試與C&C伺服器通訊時，能即時識別並警示。**
• **下載信譽** 能提示用戶有關未被確定為惡意但是可疑的檔案。	• **線上防護** 與SophosLabs即時通訊，以符合可疑檔案的簽章查詢URL和下載信譽，並將高度可疑的檔案提交給實驗室進行進一步的沙箱分析。	• **同步安全** **端點和防火牆可透過安全心跳進行通訊，以加速威脅發現和自動事件回應。**

使用者分享

「近乎只在一夕之間，我們就擺脫了過去陽春的安全防護和貧乏的支援服務，轉換到一個不僅有效、易於管理，並且具有卓越支援服務的解決方案。」

ROBERT TALLEY
IT Director, Lassen County Office of Educaton

「我們原先就有Symantec產品，但在兩個小時內竟然可以部署Sophos到大約800台的機器上。實在是太棒了！

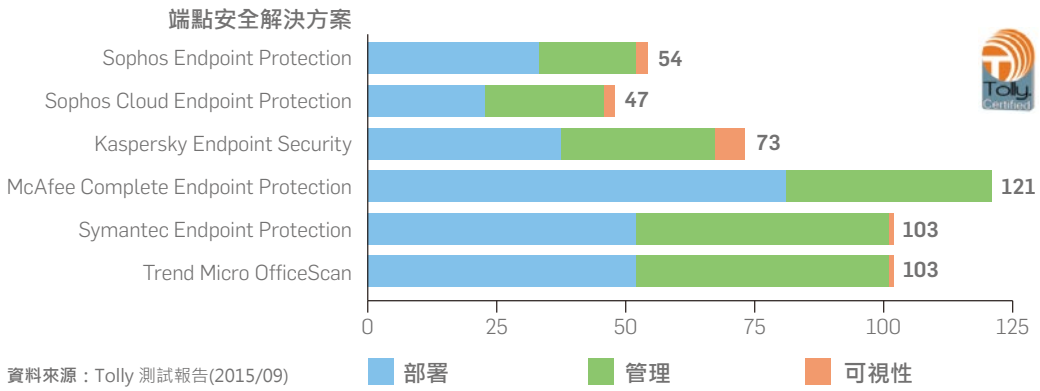
STEVE
Network Manager, Gaming Industry

簡化複雜的易用設計

若想要這些防護功能順利在企業環境中運作，其產品設計必須易於配置、部署和管理。明確的預設政策和功能操作可協助您快速部署防護、直覺易用的儀表板能提供環境的高可視性，並可便於存取日常管理工作。

Tolly[4] 的獨立可用性測試證實SOPHOS比其他端點安全解決方案更加易於操作使用(圖表 2)。

圖表 2。實現部署、管理和可視性所需的步驟數量（數字越小越佳）。



資料來源：Tolly 測試報告(2015/09)

專業支援服務

無論解決方案是多麼優異，都會有需要協助的時候。SOPHOS擁有來自全球的技術專家團隊，提供全天候的服務。最重要的是，SOPHOS支援團隊保有始終如一的用戶優質服務，以回饋用戶對於SOPHOS的持續愛用和肯定。在台灣我們有專業的代理商湛揚科技，為企業客戶及合作夥伴提供用心的售前、POC及售後專業服務，以達成客戶滿意。

參考資料
1. “Smarter, faster hackers cause huge spike in cyberattacks” , USA Today, 15 April 2015.
2. 2015 Data Breach Investigations Report, Verizon Enterprise Solutions, April 2015.
3. 2015 Global Study on IT Security Spending & Investments, Ponemon Institute LLC, May 2015.
4. Tolly Test Report, September 2015.

只需5步驟即可轉換到SOPHOS新世代端點安全防護

以大多數企業組織的立場預想，轉換到新世代端點安全防護的最大困擾， 應該就是移除安裝的問題。而多年以來SOPHOS已協助成千上萬的客戶輕鬆完成轉換作業程序。在大多數的情況下，這項過程可以在幾小時內完成。

1 選擇並安裝管理主控台

SOPHOS提供可彈性選擇的內部或雲端管理選項。

- **SOPHOS Central** 提供了一個完整操控且快速的管理主控台。啟動 SOPHOS Central帳號後，不到五分鐘內即可完成設置和部署。
- 對於偏愛企業內部管理的主控台的客戶，請安裝和配置 **SOPHOS Enterprise Console** 和相關的管理元件。

2 準備端點部署套件

SOPHOS部署套件包含競品軟體移除工具，可進行自訂以完全刪除在您環境中使用的特定端點軟體。刪除舊版端點安全軟體後，SOPHOS Endpoint Protection安裝套件將會完成SOPHOS Endpoint Protection軟體部署。該過程包括互動式或靜默安裝選項。靜默安裝選項能最小化對端點用戶產生的影響。

3 配置 Sophos Endpoint Protection 政策

SOPHOS Endpoint Protection包含一系列端點安全防護功能，這些功能在您的傳統端點安全解決方案中也許已有或沒有。首先，以在先前解決方案中啟用的任何安全功能來配置端點防護政策，如病毒防護。

您也可以選擇在SOPHOS Endpoint Protection中啟用新的安全功能，例如惡意流量偵測、應用程式控制和網頁控制。您可在最初部署SOPHOS Endpoint Protection的時候，或者在之後視情況使用這些新的安全功能。

4 啟動初始軟體測試

任何新端點軟體發布（包括SOPHOS Endpoint Protection）的最佳方式是，透過將新軟體部署到有限數量的端點來測試部署過程，並驗證新端點安全軟體的正常執行。請選擇易於存取並操作頻繁的測試端點，以快速測試部署並驗證操作的正確性。

5 完成企業內部軟體部署

在進行初始測試之後，您就可以開始準備在整個企業組織中完成SOPHOS Endpoint Protection的部署。對於大型的企業組織，可以根據地理位置、組織單位或適合您組織的其他方法將其進一步劃分為多個階段來進行。

就跟部署任何新技術一樣，在經驗熟悉之後，與SOPHOS Endpoint Protection的配合操作將可以更有效率。而實際上，大多數人在使用後都認為SOPHOS解決方案確實非常容易使用，不僅簡化管理節省寶貴時間，同時還獲得更豐富的端點安全防護能力。

總結

隨著網路威脅的蓬勃發展，企業必須持續尋找新方案來優化IT安全投資。以傳統端點安全解決方案的狀況來說，許多企業藉由轉換到SOPHOS新世代端點安全防護，來成功脫離過去無奈的困境。

若想更換現有端點安全解決方案，請評估以下項目：

1. 評估現有資安防毒的人員配置和技能水平。
2. 評估現有的防毒產品是否已經許久沒有提出創新產品技術，以防護更多的最新威脅。
3. 評估您過去是否有因端點防毒產品效能，使用戶發生使用中斷或抱怨。
4. 評估現有防毒廠商給您的技術支援是否足夠?
5. 現有防毒廠商是否逐年調漲價格，不符合您的預算內?

如您發現上述項目您有任何一項問題或多個不滿意，請趕快與我們聯繫，我們有專業的資安團隊提供您詳細的產品簡報、產品免費測試，以及新世代防毒最佳作業準則的建議。歡迎現在拿起電話洽詢**湛揚科技**(02)2735-3512、(07)972-7388，讓您快速體驗SOPHOS強大有效的防護能力！