



不管上不上雲？何時上雲？

Symantec WPS 總能隨時保護

您的網頁、雲端存取安全以及管理需求

根據統計招致企業感染病毒等惡意程式（會衍生更嚴重的資安損害）的主要來源為：電子郵件、網頁瀏覽以及隨身碟之類的行動儲存媒體(佔98%的約有50幾種)，其中電子郵件約佔了整體的70%以上，電子郵件中的附件以及連結是引發感染惡意程式最主要的感染途徑，攻擊者很容易透過社交工程的手法，誘導受害者開啟惡意的附件及連結，特別是現在的攻擊者多為商業型營利的駭客組織或國家級資助的專業網軍，所以使用傳統的防護機制，往往看似風平浪靜，但只要一出事，總是迅雷不及掩耳般地造成山崩地裂的大災難。其實是針對性的攻擊，在埋伏一段時間後，只要時機成熟，就可在很短的時間，遍地開花，讓企業瞬間束手無策舉白旗。

您知道嗎？電子郵件中的**附件**以及**連結**是引發感染惡意程式最主要的感染途徑，特別是**連結**的部份，由於最終的連結目的地網址是可以隨時變動及偽裝的，所以它就是一串隨時變動可以規避傳統電子郵件防護機制的變數，也是很容易讓人信以為真的騙術，這也是一般郵件防護解決方案捉襟見肘、最力不從心的死穴。

如果您是IT安全人員，您一定常常聽到終端使用者向您回報：我只是瀏覽網頁，什麼事都沒作，然後電腦就變成這樣了！終端使用者的確什麼都沒作，但全世界的網站有一半以上是從來不曾針對安全性作修補的，很容易被駭人成為惡意程式的更新及散播中心，更別說被駭客拿來專作壞事存活不到12小時的幽靈網站，要追溯更是困難。當我們

瀏覽網頁的時候，更常因為瀏覽器版本太老舊破洞百出，成為通往網路煉獄的門戶、外掛程式常有漏洞或設定不周全，甚至被安裝了惡意程式下載器或資料竊取的外掛而不自知，所以終端使用者的電腦，即使沒有瀏覽網頁，其實已經是被操控的殭屍電腦，正在默默地犧牲自己的效能，為害企業也危害全世界。

企業開放上網並提供一個安全的上網環境，除了能滿足友善職場生態的趨勢，對於上網的工作效益提升更有期待，所以上網的管理與稽核以及網頁的分類與過濾，對現代企業而言，是一門顯學，也與電子郵件安全等同重要。

賽門鐵克新推出的網頁及雲端安全/管理解決方案組合，可以完全解決上述的問題，更不止於解決這些問題，就叫作：WPS (Web Protection Suite)--網頁防護套裝組合--顧名思義就是物超所值並且可以自由搭配的多重組合。WPS就是這種概念：幾乎所有網頁/雲端應用的管理/防護最高階的功能都有了，不管地端自建、雲端服務或兩者的混合(目前企業多有上雲的需求，但時程跟急迫性都不一樣，WPS就是滿足所有情境的方案，讓網頁/雲端應用安全配合上雲與否與時程)，都是一個價格，同時地端/雲端安全政策也可以共通，以每人/每年的費用計價，沒有級數之分，以快速完成交易(目前的價位是以2,000人的價格為基準，所以相對很便宜)，附上型錄說明(WPS)，歡迎洽詢討論。

這個吃到飽的滿漢大餐包含 8 個原先需

單獨購買的解決方案，大抵而言，如果是雲端服務的，它讓您全部都能使用。如果是要自建在地端的，它也有提供虛擬機的版本，則會依照您所購買的授權數，去換算核心數的虛擬機版本。如果要採用實體主機的平台，則是要額外購買實體機硬體主機(就不用再買授權了，套用已採購的WPS授權即可)：這8個解決方案的各別型錄如下連結：

- **WPS(Web Protection Suite)--網頁防護套裝組合**：包含以下8種功能
- **網頁安全雲端服務**--Web Security Service
- **安全網頁閘道虛擬機版**--Virtual Secure Web Gateway
- **威脅情資及網頁分類過濾服務**--Intelligence Services and WebFilter
- **企業級管理與報告**--Management Center and Reporting
- **內容分析與沙箱**--Content Analysis & Sandboxing
- **網頁威脅隔離**--Web Isolation
- **加密流量管理**--Encrypted Traffic Management
- **網頁應用程式防火牆(WAF)及反向代理**--Web Application Firewall and Reverse Proxy

以下是這個解決方案的前世、今生與未來，有興趣聽**真實**故事的朋友，佔用您幾分鐘的時間：

在頻寬很貴的網際網路初期，大型的ISP、企業或大型學校，會大量地建置Blue Coat的CacheFlow--就是地端的快取，來提供快速網際網路內容服務並節省昂貴的頻寬費用。

CacheFlow一開始就是走全代理(Proxy)的技術，一直維持好幾年近90%以上的市佔率之後，還是不敵頻寬越來越便宜的現實，有好幾年幾乎快要撐不下去。

好運總在堅持後來敲門，因為網頁進展到Web 2.0之後的豐富多元與互動性，讓網頁

成為資安的大破口，也讓上網管理成為公司治理的顯學。

所以運用全代理的技術(Proxy)，WebFilter網頁分類及過濾系統於焉誕生，它運用了WebPulse的動態即時分類專利技術，讓95%的網頁絕對是即時有效正確的分類，剩餘的4%約在30分鐘後，也會經過自動化及專家驗證後被正確分類。更強的一點是同一個網頁，WebFilter 最多可以把同一個網頁，歸類到四種類別，讓網頁的控管更精準，更能發揮最大的效益。

因為全代理技術(Proxy)，所以針對安全性的檢查，它比最新次世代防火牆可以更深入且完整地(不是分段的)偵測惡意內容，特別是在加密的網路流量的解析上，BlueCoat就是翹楚。BlueCoat定位成為內容分析的平台框架，把多廠商的最新安全檢查技術都納進來，滿足苛求的安全要求。

過往這些超強功能都是買了基本的快取服務功能之後，再依需求購買管理/安全選項。地端自建型的環境要先購買硬體裝置(SWG-後來也有推出VA版本)，而地端自建與雲端服務的購買方式不同，政策也很難共用。更讓人怯步的是授權的購買是以連線數(Session)來計價，搞得買個授權要先修好工程數學般的擁有天賦異稟。現在採購方式比買手搖杯飲料還簡單--單一價格，以每人/每年為計價標準，沒有人數級距的不同單價，所有的功能全部讓您使用，而且非常的物超所值，因為計價基準就是以過往2,000人的級距去算，即便組織內只有200人，您只要買200套的授權，卻享有過往2,000套的優惠級距。

完善的資安防機制必須透過電子郵件、網頁以及端點這三個控制點的分工與協同運作，以該控制點最有利的防護技術與管理機制來降低威脅的探勘、攻擊以及入侵，並能

隨時監控內部是否已被入侵及埋伏甚至橫向移動以及資料的外洩，採用Symantec 完整解決方案，可以非常容易達成資安目標。現在大家都意識到在端點安裝防毒軟體或更強大的端點安全系統甚至EDR的重要性，如果能在更外層的網頁存取層，也導入Symantec 完善的網頁安全防護/管理機制，其成效會更為明顯，也能大大提升端點的運行效率，提高員工工作效率，並為現有的電子郵件防護技術補上精準過濾偵測內嵌網頁連結的盲點偵測系統。

Symantec在端點、電子郵件以及網頁防

護，皆有最完整的防護機制，同時也能在這三個控制點，透過AI為後盾的關聯分析與情資交叉比對的協同運作，能在第一時間就發現目標式攻擊，更能發現入侵後的初期入侵跡象、中期橫向移動以及後期的資料外洩及更大的危害，都能有效偵測。在2019/11，博通併購賽門鐵克後，更加重投入資源在RD上，同時也大大降低交易複雜性，將料號精簡為功能多合一、實體與虛擬、地端與雲端等符合全功能多情境--並以極具競爭力的價格來提供最完整的安全防護，讓顧客更喜歡、更容易使用／採購賽門鐵克。



更多資訊 請造訪我們的網站 <http://www.SaveTime.com.tw>
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。



- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承 (Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有IT Team的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準SOP 文件的提供，

以及基於比原廠更熟悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。

- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入Symantec解決方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊：
保安資訊有限公司
<http://www.savetime.com.tw>
0800-381500、0936-285588