

# Sophos端點安全防護成功案例

## 單一介面給足所有資訊

### 協助企業完成終極端點防護任務

**對**於企業而言，員工端點電腦一直飽受來自各種管道之不同惡意程式的威脅，過去單一防毒之安全防護早已不敷所需，企業需要更全面性的端點安全防護方案。但如何從中尋找到兼具多功能、資源順暢、成本與管理效益的方案才是最符合企業需求的解決方案。

身為傳統機械製造業的亞崴機電也面臨端點安全的難題，亞崴機電副理鄔忠慈指出，在因應數量龐雜之各類型端點威脅上，該公司很快意識到既有所部署的防毒軟體，不論功能性、防護面與嚴謹度上都明顯不足。最令人感到無奈的，雖然只是單純的防毒方案，但卻是專吃系統資源的怪物，對於員工例行作業會造成極大的困擾與影響。

為了改善這個問題，該公司在經過一番審慎的評估之後，毅然決然地將既有防毒軟體全面汰換成Sophos Endpoint Protection端點安全防護方案，該方案除了防毒、防駭等基本功能外，還支援應用控管、裝置控管、資料外洩防護(DLP)與硬碟加密機制，整個防護範圍涵蓋所有端點、行動、Web、資料、網路與郵件，不失為符合當前企業端點安全需求的解決方案。

#### 老舊系統 vs 多功能端點防護的難題

面對傳統防毒軟體，鄔忠慈一針見血地指出，系統不堪負荷一直成為嚴重影響正常端點作業與工作效率的最大問題所在。由於亞崴機電屬於傳統產業，端點電腦汰舊換新的速度相對較慢，所以系統規格相對老舊。正因為如此，傳統防毒軟體不論進行掃毒或安全政策派送時，端點電腦不但無法負荷，甚至難以動彈。再者，由於亞崴機電中國大陸廠的員工一直會有使用無界瀏覽器的習慣，但站在企業資安政策的角度，不論翻牆軟體或綠色軟體難免會有形成資安漏洞的疑慮與風險可能，所以該公司非常需要應用控管的安全機制來協助。如此一來，該公司勢必需要在既有防毒之外，另需應用控管方案的建置。

不僅如此，當前仍然還有許多安全議題需要面對，其中尤以裝置控管、硬碟加密、資料外洩與個資法規遵循等議題最為緊要。面對如此多的議題，對於全公司IT人員僅3人的亞崴機電而言，一一分別建置宛如不可能的任務，別說管理與採購成本無法因應，光在老舊端點電腦上安裝這麼多方案，系統絕對難以負荷。

除此之外，該公司還面臨許多安全需求與挑戰，舉凡零時差漏洞攻擊、假冒合法軟體的應用風險與Web威脅，以及個資法規遵循與資料外洩等議題，莫不為企業安全防護帶來空前嚴峻的挑戰。其中尤以面臨法規遵循與資料外洩的壓力最大，畢竟當前因應資料外洩最熱門的防護方案莫過於DLP，但DLP的導入需要龐大的時間與導入成本，對於IT人力資源有限的亞崴機電而言，會有預算與導入上的困難。

#### 系統不卡卡 安全管理精準又方便

基於大環境的挑戰與亞崴機電自身的需求，該公司急需一個兼具成本、管理與資源效益的多功能端點安全防護方案。在經過一番市場方案調查與評估作業後，身兼多功能安全防護機制的Sophos Endpoint Protection端點安全防護方案雀屏中選。

鄔忠慈表示，首先Sophos Endpoint Protection方案舉凡防毒、防駭、應用控管、裝置控管、DLP與硬碟加密機制盡皆支援，防護面涵蓋所有端點、行動、Web、資料、網路與郵件，所以非常符合該公司在安全嚴謹度、法規遵循與預算成本上的需求。再者，即使該方案擁有這麼多的功能，仍能成功建置並順暢運行在只有512K記憶體資源的端點環境上，由此可見，其對系統資源的耗用與負荷甚低。

站在IT管理的角度，鄔忠慈十分激賞地指出，Sophos Endpoint Protection的管理介面一目了然，對於IT人力有限的亞崴機電而言，無異是有效提升管理效益的一大利器。透過清楚分明的儀表板，舉凡中毒、更新等所有安裝Sophos電腦的即時狀況都能立即回報、清楚檢視，管理者可以很快掌握狀況並立即加以處理回應。同時，IT管理人員並可透過中控台，進行諸如病毒碼統一派送更新，以及遠端移除端點系統中的病毒等作業。

在部署上，該方案支援自動派送安裝機制。最方便的，莫過於在安裝之前還會協助進行之前舊防毒軟體的反安裝作業，這對IT人員負荷的減輕，以及加速軟體部署時間有很大的幫助。除此之外，由於亞崴機電研發人員不時會進行相關產品的測試開發，所以為確保環境的穩定性，並避免應用相容性問題，所以會有移除端點防護方案的需求。為了方便其日後安裝端點防護方案，Sophos並特別提供方的自動安裝包。相關人員只要到特定頁面上點選連結，便可方便快捷地完成安裝。

鄔忠慈認為，Sophos Endpoint Protection的授權模式也不失為另一個值得一述的優點，其與其他端點防護方案採用賣斷的方式不同，而是採用每年訂閱授權的模式。同時，其他方案任何更新、維護或功能添增都要額外付費，反觀Sophos方案則會依不同端點功能的不同組合提供不同套件之訂閱，企業可方便地依需求來選擇適合的套件。



亞崴機電副理鄔忠慈

#### 滿足使用者、管理人員與企業所有安全需求

對於亞崴機電的端點使用者而言，Sophos Endpoint Protection方案的導入，首先立即感受到的效益，莫過於再也不會因為掃描、更新等作業，而有系統卡卡或無法動彈的情形出現。端點使用者不但在安全上受到全面性的保護，同時工作效率也不會因為系統資源不足而再有打折的情況。

站在管理者的角度而言，過去防毒方案管理介面層次太多，需要在不同頁面轉換檢視，可能會因資源擷取不連貫而有誤判情形的可能。如今Sophos Endpoint Protection方案單一畫面就能給足所有資訊，甚至不同系統平台，也能提供單一管理介面，這讓IT管理人員能夠快速掌握所有端點安全狀況，即使有任何事件發生，也能做出迅速而精確的回應。

再就公司角度而言，具備多功能端點安全防護能力的Sophos Endpoint Protection，讓公司能達到以最低預算發揮最大安全防護功效的目標與效益。更重要的，過去該公司面對即時通訊、P2P與綠色軟體的濫用，根本沒有能力控管。如今透過Sophos方案的應用控管機制，便可對任何不法應用存取加以封鎖。針對有需求員工，也可透過使用申請書的申請與主管批准後予以開放。

鄔忠慈表示，許多方案會硬塞一些用不到的功能，Sophos Endpoint Protection則可以讓企業選擇符合自己需求的套件加以訂閱，而且額外功能也不會有餘花費，不失為兼具多功能、資源順暢、成本與管理效益的最佳CP值方案之一。