

本院新設置賽門鐵克防毒系統(SEP)宣導

自 98 年度起，本院電腦防毒系統配合法務部資訊處的更新計畫，更換為 Symantec Endpoint Protection 端點安全防護架構，此一新的防護軟體不但是一套完整且功能強大的防護系統，且能加強防毒架構的檢查維護工作與有關病毒威脅資訊及各作業系安全性漏洞等相關資料收集與查詢，對於本院的資訊系統而言，不論是電腦伺服器主機或是個人電腦及周邊設備，均提供了更進一層的安全防護。

Symantec Endpoint Protection 是新一代的產品，可提供進階的威脅防護功能，以保護端點如筆記型電腦、桌上型電腦和伺服器，使其不受已知威脅和未知威脅的攻擊，並可防範惡意軟體，例如病毒、病蟲、特洛伊木馬程式、間諜軟體和廣告軟體，甚至可以躲避傳統安全措施的最複雜攻擊，如 Rookit、零時差攻擊和變種的間軟體等。

Symantec Endpoint Protection 用戶端，整合下列威脅防護技術：

1. 「防毒和防間諜軟體防護」新增了 Rootkit 偵測和移除功能，同時對改善了資源所使用的記憶體大小。
2. 「網路威脅防護」提供新的規則型防火牆和「一般攻擊程式攔截」(GEB)，可在惡意軟體進入電腦之前便加以攔截。
3. 新增「主動型威脅防護」功能，透過此新增功能，可在沒有特徵條件規則下，強化零時差攻擊威脅防護。
4. 新增「應用程式及裝置控制」可針對用戶端作業系統中的應用程式及週邊裝置進行管控，透過此新增功能，以政策管制的方式，管制使用者的動作，強化用戶端防護。

本院同仁使用中的電腦均設置有 Symantec Endpoint Protection 端點防護顯示，每月應至少一次打開該防毒系統，查看該系統是否安全或是有警告標示，並進行手動掃描威脅、檢視各項安全日誌，如發現有問題，立即通知資訊人員處

理，以確保使用人及本院整體資訊系統之安全。