保安資訊14.3RU6(14.3.9205.6000) --9種安裝套件不同功能說明

NEW **SEP14.3 自 RU3/RU4 起，特別針對加密勒索軟體最棘手的就地取材(living-off-the land) 攻擊的強化防護技術提升，是業界的創新技術，對用戶有明顯感受得到安全效益。**

SEP 14 是 Symantec Endpoint Protection V14 的簡稱。SEP 14第一版(RTM：Release To Manufacturing)是在2016/10/28正式釋出的。最新版次為2022/11/07釋出的14.3RU6核心版次為：14.3.9205.6000。SEP 14最佳化的安裝是透過中央主控台(SEPM)來安裝並設定最適化的安全政策。但某些狀況您可能無法由主控台(SEPM)來佈署SEP 14的用戶端(Client)但仍然需要SEP 14所提供的多層次防護與進階管理功能，則您可以採用由主控台客制化的安裝套件，讓使用者自行安裝或透過其它的自動化安裝方案來裝。SEP 14已經不支援：Windows XP/2003/2003 R2。前一版本--SEP 12.1的最後一個版本(SEP.12.1.6MP10c)已經停止病毒定義檔更新、停止版本更新及支援(EOL/EOS)。由於該作業系統，微軟已經停止更新及支援。建議即刻升級或採用更嚴謹的白名單防護解決方案，像是Symantec data Center Security 或 Symantec Critical system protection.

許多人取得原版安裝光碟後，就直覺地按照安裝程式的自動執行指導，依序按『下一步』來安裝，成為單機模式。結果造成非常的不如預期。例如：許多功能都不能調整，速度變慢了，網路不通了。其實，SEP 14 的正統安裝方法是需要由主控台來生成安裝檔再派送給用戶端的。xxx直接由原版的光碟來安裝用戶端是非常不妥的(建議由SEPM來配置精準的政策，可以明顯增強防毒軟體達不到的安全等級效益)，也就是它的條件鎖得很緊，又無法強制因地制宜的安全政策，當然無法滿足需求。xxx

為提供用戶更快享受SEP14的好處，保安資訊已設定好之SEP安裝套件：共9組(本光碟為繁體中文的64位元，**本版本不提供32位元**)請依需求擇一最適安裝即可(單機模式/沒有中央主控功能)。SEP 14能達到的安全等級非常高，端賴政策如何制定及強化。相關產品資訊請參考以下網頁：http://sep.savetime.com.tw。

一般而言，運行 Win7/Win8(.1)/Win10/Win11的電腦等非Server等級的作業系統，諸如桌上型電腦及筆記型電腦，安裝第一個安裝套件(Pack1)是較多人推薦的。安裝第一個安裝套件對於防止隨身碟型態的病毒，非常有效。但如果您的隨身碟有autorun.inf這個檔案，則會被禁止存取。autorun.inf這個檔案給乎都會存在已感染隨身碟型態病毒的隨身碟或記憶卡上。所以第一個安裝套件是透過啟動SEP的應用程式與裝置控管來防止感染隨身碟病毒。有標示禁止存取USB的安裝套件，會讓USB完全失效(除了鍵盤與滑鼠以外)，這對防止資料透過USB被Copy出去很有幫助。

如果是要安裝在伺服主機上，則pack6及pack7 是較合適的。當然重要伺服主機安裝防毒軟體之前，最好與專業的 IT 人員聯絡。尤其那台伺服主機上有運行非常重要或特殊的應用系統。某些較老舊及記憶體較少的個人電腦，也建議安裝 pack6 及 pack7。

安裝檔案說明：以底下的兩個安裝檔為例

SEP14.3 RU6_pkgB_ENG64：
pkg1~pkgB：代表由1到B的共9種不同安全政策檔。(如以下的表格說明)
TW代表台灣用的繁體中文版／ENG代表英文版

64 代表作業系統是 64 位元 (Win7/win8/Win10/Win 11有許多都是64位元)。另外，較新的 Server 雖以 64 位元居多，但安裝前還是需特別再次確認。

項目 \ 安全政策檔	pack1 (packA)(packB)	pack2	pack3	pack4	pack5	pack6	pack7
主防毒功能	✓	✓	✓	✓	✓🔒	✓	✓
SONOR	✓	×🔒	✓	×🔒	✓🔒	✓	未安裝
E-mail 防護	✓	✓	✓	✓	✓🔒	✓	✓
防火牆	✓	✓	✓	✓	✓🔒	未安裝	未安裝
入侵偵測	✓	×	✓	×	✓	未安裝	未安裝
應用程式及裝置控管	禁止存取autorun.inf→✓	禁止存取autorun.inf→✓	禁止存取autorun.inf→✓ 禁止存取USB→✓	禁止存取autorun.inf→✓ 禁止存取USB→✓	禁止存取autorun.inf→✓	未安裝	未安裝
備 註	除應用程式管控外，皆可更改設定	SONOR、入侵偵測功能關閉	除應用程式管控外，皆可更改設定	SONOR、入侵偵測功能關閉	主防毒功能、SONOR E-mail防護、防火牆皆更改設定	用戶端控制，所有已安裝的功能設定皆可更改	用戶端控制，所有已安裝的功能設定皆可更改

圖示說明：[✓]表示有啟動此功能　[X]表示此功能已關閉　[🔒]表示已鎖定該功能“無法停用”

說明1

此些個安裝套件程式安裝的功能全都一樣，只是有的功能被關閉並且無法再更改設定。

說明2

所有的應用程式及裝置控管皆無法從用戶端介面設定。(安全軟體的設計本來就是如此)

說明3

此安裝程式SEP若安裝裝於win2000無右鍵選單快速掃瞄。(僅適用於SEP 11.x 版--SEP 11 已於2015/01/05，完全中止病毒定義檔更新及技術支援，也就是說不能再繼續使用了，請務必更新至SEP 14.3 RU4）

說明4

安裝套件使用者皆有權限修改如防火牆、防毒的設定，你停止如防火牆的功能則右下角會出現 圖示，而 SEP 界面則會顯示如下的警告訊息，你可按修正即可再次啟用該功能。

基本上你只要自行手動停止任一小項的防護功能，右下角的圖示即會顯示紅色禁止來警告你SEP的防護可能有問題，這是軟體的設計本來就是如此，並不絕對代表SEP有問題。

pack5說明

此安裝套件把使用者介面[停用]功能拿掉，另要反安裝此套件亦需要密碼，密碼為xxxxxx(請與保安資訊連絡)，算是企業內較標準作法。

pack6及pack7說明

基本的防毒功能。有 SONOR 表示有行為模式的偵測。Symantec 的 SEP 如果只啟動防毒功能，其它功能都不啟動，安全防護等級不會太高，比較適合不存取網際網路及不與其它設備或儲存媒體交換資訊的單純環境。

packA 及 packB 說明

兩者與 pack1 一模一樣並加入 FACEBOOK 禁用功能，A 是禁止 FACEBOOK 所有功能(社交功能及應用程式)。B 是開放社交功能但禁用應用程式(如：種菜遊戲)。

以上是單機的安裝模式不需要安裝主控台(SEPM)就能安裝的非中央集中控管模式。企業如果主客觀環境都適合安裝SEP，還是建議採用中央集中控管模式(SEPM)。因為可以設定的政策非常細。甚至於只能用目前的程式即使病毒或木馬被下載到您的電腦也不讓它運作，當然也可以設定IE不能直接下載或執行特定的檔案。所以它的安全性比所有的防毒軟體都強--有專業資安技術白皮書稱這種功能為應用程式防火牆。如果企業放任一些不安全的電腦使用習慣，IT部門就會疲於奔命。所以發揮SEP內建許多基於管理的強制功能，可以讓企業大大降低接觸威脅的機會，主動提升安全等級。

實際上SEP已跳脫傳統防毒軟體的思維，除了防毒軟體該有的病毒定義檔的更新要很快以外，比較過容易中毒的使用者與幾乎不曾中毒的使用者的習慣--中毒與使用電腦的習慣有很大的關連。一般而言MIS人員很少會中毒，使用的防毒軟體也跟大家都一樣。WHY？因為MIS知道什麼東西是危險的，或是防毒軟體已警告可能為未知的病毒時，MIS不會去開啟它。MIS知道只有安全的檔案、電郵以及網頁才能開啟，而一般人以為安裝了防毒軟體就能為所欲為。等中毒之後才抱怨防毒軟體不好，換過所有品牌的防毒軟體還是中毒不斷。所以SEP是一種能設定遠離危機來源的多功能安全軟體--不是單獨的防毒軟體。就好像有小嬰兒的家裏會把危險的剪刀、玻璃杯瓶、熱水、藥物遠離小孩子的活動範圍一樣，而不只是教小嬰兒不要去拿。因為只要一拿到就有很高的危險，這與一般人隨便開啟來路不明的檔案、電郵與網頁連結很像。小嬰兒與大人是不一樣的，一般電腦使用者與MIS也是不一樣的。這就是SEP除了防毒以外的強制安全政策的原生概念。

而SEP內建的5層式防護功能，包括：1)網路、2)檔案、3)信譽、4)行為、5)修復，除了有防毒軟體的功能外，更要補足防毒軟體的不足。

- **網路**：賽門鐵克的網路威脅防護包含Vantage技術，它能夠在威脅攻擊系統前，分析入埠資料並在威脅透過網路傳輸時加以攔截。它也包含了規則式防火牆與瀏覽器防護功能，以抵禦網頁式攻擊。
- **檔案**：以病毒碼為基礎的防毒軟體能夠尋找並根除系統上的惡意程式，以抵禦病毒、病蟲、木馬程式、間諜程式、Bot傀儡程式、廣告軟體及Rootkit。
- **信譽**：賽門鐵克獨特的Insight™將上百億個使用者、檔案及網站間的連結交叉比對，以迅速判別變種威脅。藉由分析重要的檔案屬性，Insight™可以精準識別檔案是否無害，並且為每個檔案評定信譽分數，有效抵禦目標式攻擊，同時減少高達70%的掃描負荷。
- **行為**：SONAR™運用人工智慧來提供零時差攻擊防護功能。在將近1400種檔案行為執行時，即時監控以判斷檔案風險，可有效阻擋全新的未知威脅。
- **修復**：清除大師(Power Eraser™)能主動掃描受感染的端點以找出進階持續性威脅，並移除頑強的惡意程式。遠端支援可讓系統管理員啟動清除大師的掃描功能，並透過Symantec™ Endpoint Protection管理主控台從遠端矯正感染的問題。

除了以上五大核心防護技術外，Symantec™ Endpoint Protection 14也提供了擴充的精細政策控制功能包含：

- **系統鎖定**：藉由只容許執行白名單的應用程式(已知沒有疑慮者)，或封鎖黑名單應用程式的執行(已知有疑慮者)，加強營運關鍵系統的防護。
- **應用程式與裝置控管**：藉由監控應用程式行為，以及對檔案存取、系統登錄檔存取、允許執行的程序以及可寫入的裝置資訊進行控制，協助防止內部與外部的安全漏洞。

- **主機完整性檢查與政策執行**：可讓使用者在其端點上執行程序檔，以確認並回報遵循狀況；隔離位置、點對點強制執行鎖定，以及隔離未遵循規範或受感染的系統。
- **位置偵測**：自動偵測系統從哪個位置連線，例如旅館、熱點、無線網路或VPN，並且針對該環境調整安全性以提供最佳防護能力。

以上都能依據不同的安全等級，設定最佳化的安全政策。例如：

- 隨身諜病毒的防護(即使不更新病毒定義檔也作得很好)，目前最好的隨身碟病毒的防治方法。
- 不讓IE直接開啟如容易中毒的檔案格式或特定連線。
- 不讓Outlook/Outlook express直接開啟如容易中毒的檔案格式或特定連線。
- 一鍵就能禁用網路分享。
- 您只要想得到可能會中毒的途徑，SEP幾乎都能透過政策設定，有效地防止它。
- 關於SEP的安全政策制定，保安有非常多的成功經驗。歡迎來電討論……

上述的安全政策，並不是安裝了SEP之後就會自動產生的，因為不同的環境有不同的安全政策需求，必需經過討論及分析與演練才能保證是可行的。沒有技術支援的用戶，連安裝方法都不對，更不用談及安全政策如何設定。當然裝了SEP還是會中毒。因此之故，保安貼心預先設定了幾個不是很嚴厲的安全政策，讓擾人的隨身碟病毒、USB資料外洩或感染病毒的問題都能大大改善，而且盡可能不影響現有使用電腦的習慣。如果您還要更安全，我們也有提供專家級的收費顧問服務及到場安裝設定服務。

從2020年自今，採用兩用工具所發動的「就地取材」攻擊增加了2,000%；利用IOS和ANDROID的漏洞攻擊增加了80%；同個時段，鎖定企業的加密勒索攻擊增加了62%，單單賽門鐵克的IPS入侵預防系統，平均每個星期攔截近2億次攻擊。任何一家防毒軟體都有其偵測不到的病毒及惡意程式。如果還在用傳統比較我的掃描可比別人多幾千隻，那又如何？還不是照樣中毒，所以啟用IPS系統往往比防毒功能效益更高。

只要設定好SEP的安全政策，我們相信您對SEP一定會愛不釋手，因為SEP的安全政策的元件的前身是Sygate的enterprise Security--許多金融服務公司、國防等級的單位都是使用這一套。

SEP不是單獨的防毒軟體，如果還用傳統防毒軟體的思考模式--貓抓老鼠。那永遠都在檢討為什麼會中毒？建議您啟用其它有用資訊：

- 養成安全使用電腦及網際網路的好習慣
  http://www.savetime.com.tw/new_symantec/Good-Habits-for-PC-users-sep.asp
- 如何評估防毒(端點安全)軟體
  http://www.savetime.com.tw/new_symantec/How2_evaluate_AV.asp
- 企業版與家用版防毒軟體之比較
  http://www.savetime.com.tw/new_symantec/AVHome_VS_AVBiz.asp
- 使用免費軟體之效益與風險評估
  http://www.savetime.com.tw/new_symantec/FreeAV_Pro_and_con.asp

賽門鐵克的其它第一名解決方案

- **資安界最完整的端點安全方案組合--賽門鐵克端點安全完整版**
  http://www.savetime.com.tw/sesc.asp
- 郵件安全閘道第一品牌
  http://SMG.savetime.com.tw
- 符合 NIST 資安框架的端點偵測與回應(EDR)
  http://ATP.savetime.com.tw
- 端點安全(企業防毒)第一品牌
  http://SEP.savetime.com.tw
- 正統企業備份第一品牌
  http://BE.savetime.com.tw
- 重要伺服主機快速整機備份第一品牌
  http://SSR.savetime.com.tw