

# ESET 雲端防毒主機代管

© 2015 席克資訊有限公司

<http://www.seekinfo.com.tw/>

更新日期：2015/12/19

席克資訊成立迄今已逾十年，我們專注在電腦病毒防護的領域，擁有豐富的經驗，來協助客戶處理病毒相關問題。

現在我們推出一項免費的方案 - **ESET 防毒主機代管**。凡是向我們購買 ESET 防毒軟體企業版的客戶(少數對象例外)，如果公司規模較小，沒有太多的資源與人力來自行建置防毒主機，現在您有更好的選擇，直接使用席克資訊的防毒主機。

首先解釋一下什麼是防毒主機代管？正常來說，公司行號購買 ESET 企業版防毒軟體，會在公司內部架設一部中央控管的主機，負責管理及監控全公司電腦防毒軟體的狀況。例如：更新是否正常，是否有異常的中毒警訊。防毒主機代管的意思是將中央控管主機的角色，移至席克資訊的伺服器。

## 適用對象

- 購買 ESET 企業版的席克資訊 Premium 客戶
- 較小規模的公司，原則上以不超過 50 部電腦為範圍。沒有專屬的資訊人員可以處理防毒相關的事宜，或者不想自行監控防毒主控台的客戶。
- 具備 Internet 網路連線能力。(不必全天候連線，但需要偶爾有連線來回傳相關的訊息)

## 優點

- 不必額外準備一部伺服器，省下這部伺服器的軟/硬體費用，以及維護成本。
- 由席克資訊協助管控設定，以免因不當設定造成防毒上的漏洞。如果有需要調整設定，只要告訴我們您的需求，我們即可幫您處理。
- 由專業的工程師協助您監看防毒軟體的狀況，我們工程師在防毒領域已經超過十年的經驗，同樣的訊息，由他來幫您解讀，或許會更加精準。
- 有不少客戶，安裝了防毒軟體之後就放著不管，經年累月延用過時的舊產品，其防毒效果早已大打折扣。如果由我們協助管理，當 ESET 原廠發佈新版本時，我們會主動安排進行升級。(從防毒主機發佈命令，自動處理，正常狀況下無須人工介入。)
- 如果有發現異常狀況，例如：未更新病毒碼或者疑似中毒的情況，我們會主動設法排除。如果無法排除，我們會通知您，安排透過遠端連線迅速排除狀況。(連線的發起動作，須由客戶啟動特定的程式，我們才能進行連線)
- 不定期主動分析電腦裡的程式是否有可疑的檔案。

## 缺點

- 無法自行監控公司防毒軟體的使用狀況 (但仍然可以在每一部電腦上看到各種相關的資訊)

## 使用條件

- 允許全公司的電腦連線到席克資訊的防毒主機 (era.seekinfo.com.tw, port 443)，如果電腦原本就能連外

面的網站，通常不需要額外調整設定。

- 每部電腦均須安裝 ESET RA Agent。請注意，我們無法知道 貴公司有多少部電腦，如果沒有安裝 ESET RA Agent，我們就無法看到該部電腦的狀況，也就無法監控防毒運作的狀況。

## 用戶端安裝

- 用戶端安裝必須由客戶自行處理，但我們可以提供簡易的安裝程式，讓您可以輕鬆安裝，只要會啟動程式，就可以進行安裝。(如果遇到問題，我們可以透過網路遠端連線進行問題排除)

## 更新

眾所週知，防毒軟體需要持續更新病毒碼或者軟體更新，這裡有二種做法：

- 公司內所有電腦都直接向 ESET 原廠更新
- 公司內找一部電腦負責儲存相關的檔案，其他電腦再透過它來取得病毒碼等相關資訊。不必使用太高級的硬體，只要簡單在這部電腦安裝一個軟體，及相關的設定即可。(軟體的安裝及設定，當然會由我們幫您處理)

視情況，可以選擇以上其中的一個方法。除非電腦數量很少，否則建議採用第二種方法，可以節省 Internet 頻寬的使用量。

## 報表

使用席克雲端防毒主機的客戶，每周會收到一份類似如下圖的報表。

席克資訊雲端防毒週報表				
<a href="#">電腦清單</a>   <a href="#">威脅記錄</a>   <a href="#">電腦發現病毒排行檢</a>   <a href="#">原意程式排行檢</a>   <a href="#">軟體統計</a>   <a href="#">軟體明細</a>				
電腦名稱	最後連線	病毒碼版本	防毒軟體	作業系統
APOLLO 192.168.1.23	2015-11-18 17:20:20	12584 (20151118)	ESET Endpoint Security v6.2.2033.1	Microsoft Windows 7 專業版 Service Pack 1 v6.1.7601 32-bit
VENUS 192.168.1.87	2015-11-13 20:34:23	12561 (20151113)	ESET Endpoint Antivirus v6.2.2021.2	Microsoft Windows 7 企業版 Service Pack 1 v6.1.7601 64-bit
PLUTO 192.168.1.17	2015-11-18 17:18:53	12584 (20151118)	ESET Endpoint Antivirus v6.2.2033.1	Microsoft Windows 7 專業版 Service Pack 1 v6.1.7601 64-bit
VEGA 192.168.1.39	2015-11-18 17:19:57	12584 (20151118)	ESET Security v4.0.10.0	Ubuntu v14.04 64-bit

[回頁首](#)

威脅類型	電腦名稱	類別	威脅名稱	處理方法	物件	程序名稱	使用者	發生時間
防毒軟體	APOLLO	蠕蟲	INF/Autorun.gen	透過刪除來清理	file:///E:/Autorun.inf	C:\Windows\System32\svchost.exe	NT AUTHORITY\SYSTEM	2015-11-15 21:56:10
防毒軟體	APOLLO	木馬	Win32/Kryptik.AEFP	透過刪除來清理	file:///E:/tillnow/fighter.exe		Apollo\Juni Lai	2015-11-15 21:56:15
防毒軟體	PLUTO	潛在不需要的程式	Win32/Hao123.A		http://music.baidu.com/pc/spec/download614/ttpsetup_614cht-57039028.exe/hao123inst.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	Pluto\Steve	2015-11-16 11:52:46
防毒軟體	PLUTO	潛在不需要的程式	Win32/Hao123.A	已刪除	file:///C:/Users/Steve/AppData/Local/Temp/hao123inst.exe	C:\Users\Steve\Downloads\ttpsetup_614cht-57039028.exe	Pluto\Steve	2015-11-16 11:53:24
防毒軟體	PLUTO	潛在不需要的程式	Win32/Hao123.A	中斷連線	http://update.music.baidu.com/tpsetupNSIS_cht.exe	C:\Users\Steve\Desktop\迅軒\bdupdate.exe		2015-11-16 11:54:23
防毒軟體	PLUTO	潛在不需要的程式	Win32/Hao123.A	中斷連線	http://update.music.baidu.com/tpsetupNSIS_cht.exe/hao123inst.exe	C:\Users\Steve\Desktop\迅軒\bdupdate.exe		2015-11-16 11:54:23

[回頁首](#)

## 電腦發現病毒排行榜

電腦名稱	所需數量
pluto	4
apollo	2

[回頁首](#)

## 惡意程式排行榜

惡意程式名稱	數量
Win32/Kryptik.AEFP	1
Win32/Hao123.A	4
INF/Autorun.gen	1

[回頁首](#)

## 軟體統計

軟體名稱	數量	軟體名稱	數量	軟體名稱	數量
7-Zip 9.20	1	7-Zip 9.20 (x64 edition)	1	Adobe Acrobat Reader DC - Chinese Traditional	1
Adobe Flash Player 18 ActiveX	1	Adobe Flash Player 19 ActiveX	1	AhnLab Online Security	1
Bdsyn手机助手	1	CCleaner	2	CHT Up2Date Service	1
ESET Endpoint Antivirus	2	ESET Endpoint Security	1	ESET Remote Administrator Agent	4
ESET Remote Administrator Console	1	ESET Remote Administrator Server	1	ESET Server Security	1
Evernote v. 5.9.1	1	Flip PDF	1	Foxit Reader	1
FreeMind	1	Garena 戰時通	1	Garena 英雄聯盟 (台灣)	1
Google Chrome	2	HICOS PKI Smart Card Client v2.1.9.1u	1	IPInstaller	1
ImgBurn	1	Intel(R) Management Engine Components	2	Intel(R) Processor Graphics	1
Intel(R) Rapid Storage Technology	1	Intel(R) USB 3.0 eXtensible Host Controller Driver	2	Java 7 Update 55	1
LINE	1	LibreOffice 4.2.4.2	1	McAfee Security Scan Plus	1
Microsoft .NET Framework 4 Client Profile	1	Microsoft .NET Framework 4 Client Profile 繁體中文語言套件	1	Microsoft .NET Framework 4.5.1	1
Microsoft .NET Framework 4.5.1 (繁體中文)	1	Microsoft .NET Framework 4.5.2	1	Microsoft Office Excel Viewer	1
Microsoft Silverlight	2	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	1	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	1	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	1	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	2

## 軟體明細

電腦：APOLLO

軟體名稱	廠商	版本	容量(MB)	軟體名稱	廠商	版本	容量(MB)
7-Zip 9.20				Adobe Flash Player 19 ActiveX	Adobe Systems Incorporated	19.0.0.185	17
CCleaner	Piriform	4.13		CHT Up2Date Service	中華電信研究所	1.0	
ESET Endpoint Security	ESET, spol. s r.o.	6.2.2033.1	116	ESET Remote Administrator Agent	ESET, spol. s r.o.	6.2.190.0	
ESET Remote Administrator Console	ESET, spol. s r.o.	5.1.34.0	28	Evernote v. 5.9.1	Evernote Corp.	5.9.1.8742	233
Flip PDF	FlipBuilder Solution		167	Foxit Reader	Foxit Corporation	6.1.1.1031	72
FreeMind		0.8.1		Google Chrome	Google Inc.	46.0.2490.86	
HICOS PKI Smart Card Client v2.1.9.1u	Chunghwa Telecom	v2.1.9.1u		ImgBurn	LIGHTNING UK!	2.5.8.0	
Intel(R) Management Engine Components	Intel Corporation	9.5.15.1730	20	Intel(R) Processor Graphics	Intel Corporation	10.18.10.3621	74
Intel(R) USB 3.0 eXtensible Host Controller Driver	Intel Corporation	2.5.0.19	18	Java 7 Update 55	Oracle	7.0.550	118
LibreOffice 4.2.4.2	The Document Foundation	4.2.4.2	425	Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938	38
Microsoft .NET Framework 4.5.1 (繁體中文)	Microsoft Corporation	4.5.50938	2	Microsoft Office Excel Viewer	Microsoft Corporation	12.0.6612.1000	332
Microsoft Silverlight	Microsoft Corporation	5.1.40728.0	155	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219	11
Microsoft 滑鼠和鍵盤中心	Microsoft Corporation	2.3.188.0		Mozilla Maintenance Service	Mozilla	24.5.0	0
Mozilla Thunderbird 38.3.0 (x86 zh-TW)	Mozilla	38.3.0	79	Notepad++	Notepad++ Team	6.5.1	
Python 2.7 MySQL-python-1.2.3	Andy Dustman	1.2.3	3	Python 2.7.6	Python Software Foundation	2.7.6150	52
Realtek Ethernet Controller Driver	Realtek	7.67.1226.2012		Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	6.0.1.7071	
Skype(TM) 7.13	Skype Technologies S.A.	7.13.101	75	VLC media player	VideoLAN	2.1.5	
WhoCrashed 4.01	Resplendence Software Projects Sp.		6	XnView 2.12	Gougelet Pierre-e	2.12	16
綜合所得稅電子結算申報繳稅系統	聯發網路股份有限公司	16.21.104.0501	24				

[回頁首](#)

## 免責聲明

席克資訊提供的這項服務並沒有額外收費，目的是希望透過我們的能力，來協助我們的客戶有更好的防毒機制。但是我們不保證永續提供此項服務，若有某些其他意外狀況，導致我們無法繼續提供雲端防毒主機，**席克資訊有權主動終止此項服務。**

## 常見問答

- Q: 如果使用此項服務，可以要求中止嗎？

隨時可以中止。可以由客戶自行移除每部電腦上所安裝的 ESET 軟體，或者由我們透過主控台解除管理狀態。

- Q: 此項服務可以永久使用嗎？

您必須具備席克資訊 Premium 客戶的身份，且 ESET 企業版授權尚未到期，才可以繼續使用此服務。前述任一條件未具備，即喪失資格。

- Q: 電腦裡的檔案是否會被竊取？

我們可以理解客戶的這種考量，但請恕我直言，我們想不到任何理由要浪費時間去找 貴公司電腦裡的檔案。況且如果我們真有心想偷竊您的資料，我們一定不會公開宣告此項服務，甚至我們根本不該浪費時間來建置及維護此套系統；相反地，我們應該要私下研究設計木馬，在神不知鬼不覺的情況下，來取得我們想要的資料，這才是快速又直接的做法。所以這個問題是否存在邏輯上的矛盾？

**席克資訊成立十餘年來，我們專注於病毒防護的領域，盡我們的能力幫助值得幫助的客戶，過去如此，未來依舊如此。如果您對此服務有任何疑慮，您可以選擇自行面對各種惡意程式的威脅，讓我們將資源留給有需要的客戶。**

- Q: 如果使用此服務，是否會消耗大量的頻寬？

這個問題要從兩個角度來看，安裝 ESET 防毒的電腦和雲端主機之間，僅有極少量的資料，例如：目前的病毒碼版本、偵測到病毒的記錄… 每天也許就只有數十 K 的資料，這樣的資料量基本上可以忽略。

其次是病毒碼更新或者軟體的安裝檔案，這部份是直接向 ESET 原廠伺服器取得資料。如果電腦數量較多，確實會是需要注意的地方。然而不要忽略了一點，無論是否使用雲端主機，您的防毒軟體本來就需要持續更新病毒碼，況且在過去採取單機使用的情況下，只能每一部電腦都連上原廠的更新伺服器下載檔案，這樣長久下來浪費了多少頻寬？而我們提供給您的方案，在前面更新的小節裡提到的第二種方法，**在公司內部找一部電腦，擔任更新伺服器，其他電腦所需要的檔案可以就近直接透過此電腦取得，就不需要每一部電腦重覆到 ESET 原廠下載檔案，如此就可以減少消耗不必要的頻寬。**試問這不是比原來的做法更好？

---

如果對以上內容有不了解的地方，請洽詢**席克資訊 雲端防毒主機負責人 賴小姐 TEL: 04-22132276**