國際影音平台技術部
資安防毒軟體及端點偵測防護授權採購案
需求說明書

中華民國113年3月

目　次

壹、　採購項目 3
一、交付項目 3
二、交付時程 3
三、驗收方式 3
貳、採購概述 4
一、採購名稱 4
二、採購範圍 4
三、契約時程 4
四、廠商資格 4
五、組織與人力需求 4
六、服務建議書撰寫格式 4
參、採購規格 5
一、防毒軟體(含EDR端點偵測應變機制及MDR託管服務) 5

壹、 採購項目

一、交付項目

項次	內容說明	數量	單位
1	**防毒、端點威脅預警及MDR託管服務採購案** # 交付端點防毒軟體，1年授權(360台電腦) # 交付端點偵測回應系統，1年授權(282台電腦) # 交付MDR遠端託管偵測回應服務，1年授權(360台電腦)	1	式

二、交付時程

113年5月31日前。

三、驗收方式

得標廠商依交付項目、數量及時程完成交付「Kaspersky Endpoint Security for Business – Advanced (端點防毒軟體)1年授權」、「Kaspersky Endpoint Detection and Response (端點偵測回應系統)1年授權」、「Kaspersky Managed Detection and Response(遠端託管偵測回應服務)1年授權」相關授權文件後，辦理書面驗收。未於約定期限內完成驗收所需交付項目、數量和相關文件，則每逾期一日處千分之一懲罰性違約金。

貳、採購概述

一、採購名稱

國際影音平台技術部「資安防毒軟體及端點偵測防護授權」採購案 (以下簡稱本案)。

二、採購範圍

(一)防毒軟體(含EDR端點偵測應變機制及MDR託管服務)

三、契約時程

113年5月31日前完成提供授權證明，授權使用期間為113年6月1日起一年。

四、廠商資格

為確保資訊安全及得標廠商所提供之服務水準，投標廠商不得為經濟部投資審議委員會公告之陸資資訊服務業者。

五、組織與人力需求

(一)本團隊人員須具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

(二)為確保本案服務水準，團隊成員應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

六、服務建議書撰寫格式

依本招標規範「採購設備數量表」各項次，逐項編製確認表（compliance table)。確認表再依項次展開答標，投標廠商應檢附設備型錄及相關證明文件，並以螢光色筆標示應答之規格，註明符合招標規範之 要求，以便本會逐項對照審核。若所附文件為外文內容，需自行翻譯成中文並加蓋公司章以便查驗。

(一)建議書及其附件之書面格式宜採直式A4尺寸（若有A3尺寸請摺頁為A4尺寸），橫式書寫，編妥目錄頁次並於左側裝訂成冊，儘量採雙面列印，建議書經提出後不得退換或更換補件。

(二)建議書封面標題統一為『國際影音平台技術部「資安防毒軟體及端點偵測防護授權」採購案』，並標示廠商名稱及加蓋廠商及負責人印章，另註明本案聯絡人姓名與電話。

(三)投標廠商應於「服務建議書」內報列全案標價總額及依據工作項目內容，提送報價清單並分明列各項目單價及全案。

參、採購規格

一、防毒軟體(含EDR端點偵測應變機制及MDR託管服務)

(一)需要整合現行運作的防毒架構，提供與防毒系統相同廠牌的授權與服務平台產品，進行端點威脅預警作業及 MDR 託管服務平台的運作機制功能，至少包含：

1. 防毒端點防護需支援下列最新作業系統包含：Windows、MAC、Linux：譬如： Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022、MAC、Linux。

2. 具備有統一管理佈署功能，可以一鍵安裝產品，且提供多種安裝方式，含遠端派送安裝、MSI 封裝包安裝、網域群組原則安裝等。

3. 端點防護軟體必需支援能整合沙箱、EDR、MDR 託管服務整合，延伸端點自動偵測及回應的能力，減少用戶人力資源的負擔。

4. 提供端點控制功能，具備應用程式控制、設備控制、網頁控制及已安裝軟體漏洞檢測、硬碟加密、檔案和資料夾加密。

5. 具備進階威脅防護技術應用程式模擬技術(啟發式技術、弱點利用防護及行為分析等技術)。可提供除了病毒碼比對以外的防毒偵測功能，來偵測及阻擋零時差的攻擊。

6. 防護共用資料夾對抗勒索病毒加密防護能力。

7. 支援增量掃描技術，避免重複掃描未改變檔，以大幅減少掃描時間和資源佔用。並且支援只掃描新建和被修改的檔案，以提高掃描效率。

8. 具有郵件防護並支援標準郵件協定POP3/SMTP/IMAP/NNTP。可針對附件做篩選，將指定的附件類型重新命名或刪除。

9. 支援掃描記憶體和正在運行的檔案，能夠掃描和清除記憶體和檔案中的病毒和蠕蟲。只會掃描新建和被修改的檔案。且具備系統解鎖或離開螢幕保護後自動暫停掃描任務功能。

10. 支援當USB隨身碟插入端點電腦時，自動執行隨身碟掃描功能。

11. 具備應用程式管理功能、裝置控制支援依照裝置類型、連接介面針對外接設備進行控制及網頁控制功能。

12. 具備加密功能並且可以本地和統一管理兩種模式。使用AES 256加密演算法需能做到全硬碟加密(FDE)、檔案級加密(FLE)和卸除式磁碟加密。

13. 端點防護需整合提供 EDR (Endpoint Detection and Response)功能，不需額外進行安裝派送佈署作業。

14. EDR 功能支援當偵測到威脅時，能支援下列響應動作：

    (1). 端點主機隔離：避免感染進一步擴大、並保留與主控台管理操作基本能力。

    (2). 禁止被偵測程序執行。

    (3). 遠端將威脅程序/物件進行刪除。

15. 支援利用端點防護及沙箱進階偵測機制，自動偵測惡意行為並進行自動響應 (Response) 動作，包含：阻擋、刪除威脅檔案或是全機掃描作業等。

16. 自動產生IoC(indicators)及支持匯入第三方 OpenIoC 格式規則進行掃描偵測比對新發現的威脅，將IoC 規則匯出成符合第三方OpenIoC 格式，支援自動產生威脅入侵指標(IoC)，並可在偵測到

惡意行為後自動套用到端點上進行自動響應動作。

17. MDR 託管服務提供持續監控能力，偵測到威脅事件時可即時產生事件並通知用戶，原廠以英文通知用戶。

18. MDR 託管服務平台支援提供偵測事件的建議回應處理內容說明，對應使用的Mitre ATT&CK 攻擊分類資訊，方便安全人員能快速了解相關事件的分類。

19. MDR 託管服務平台提供 API 整合功能，方便用戶透過 API 方式整合至用戶端現有的安全平台。提昇事件處理相關流程的彈性及擴充性。

20. MDR 管理中心必需支援集中更新控管功能，可統一更新各用戶端的病毒資料庫、Windows Update 及已安裝應用程式之更新以及具備應用程式授權管理功能。

21. MDR 管理控制台，需能提供集中管理功能，必且能同時管理端點的防毒功能及 EDR 功能。

22. 管理中心支援統一管理介面，可同時管理包含：工作站服務器、行動裝置、虛擬化防護產品及EDR 功能。

23. 新增端點安全方案可與現有管理主控台相容並統一管理。

24. 廠商需提供一年授權之端點防毒軟體 360 套、端點偵測回應系統 282 套、MDR 遠端託管偵測回應服務360 套。

(二)提供一年的病毒碼更新。並且在授權期間內如果有新版本須免費進行版本更新。

(三)Managed Detection and Response Solution for Enterprise-諮詢服務

1. 提供針對MDR 服務平台的資安建議及問題諮詢服務。

2. 收到警訊事件後，主動協助客戶回應原廠分析師提供之資安建議。

3. 收到分析師建議後應協助電話或郵件通知資訊安全人員並協助後續處理，以降低資安事件衝擊。

(四)健診服務含維護報告乙份-每季到場。

(五)售後維護支援

1. 障礙排除信箱。
2. 遠端障礙排除。
3. 提供產品教育訓練乙次。
4. 協助客戶進行相關回應服務時間為 5x8。