SOPHOS
Security made simple.

Intercept X
常見問與答

一、產品資訊

1. 什麼是 Intercept X?
2. Intercept X 主要提供什麼功能？
3. 什麼是 anti-exploit 漏洞攻擊防禦?
4. 什麼是 exploit 漏洞攻擊?
5. 我是如何受到漏洞攻擊的?
6. 當今人們如何對抗防禦漏洞攻擊？
7. Intercept X 如何協助對抗防禦漏洞攻擊？
8. 什麼是加密勒索軟體？
9. 什麼是加密勒索軟體防護？
10. 為什麼我們有了 Intercept X，仍需要 SOPHOS 或其他廠商的病毒防護 / 惡意軟體防護 / 端點防護產品？

二、關於授權和部署

1. 如何獲得 Intercept X 授權或試用？
2. 本地部署 SEC(SOPHOS Enterprise Console)管理端點安全的客戶是否可以使用 Intercept X？
3. Intercept X 是否有計劃加入到本地部署 SEC(SOPHOS Enterprise Console)管理的端點安全防護？
4. 使用 Intercept X 需要安裝伺服器嗎？

一、產品資訊

1. 什麼是 Intercept X?

Intercept X 是一個 100%的新世代端點安全產品，目的在於阻止現今漏洞攻擊和勒索軟體，提供易於了解的攻擊分析。它包括漏洞防禦，勒索軟體防護，根本原因分析和先進的病毒清除技術，這些通常是不會在一般病毒防護產品或端點安全產品中找到。這使得 Intercept X 非常適合或者與競爭對手基於病毒防護的端點安全產品一起安裝，或者做為集中端點安全防護產品的擴充 - 做為整合的代理程式和控制台來運行。 Intercept X 是基於 SOPHOS Central 的其中一個解決方案。

Intercept X 提供：

- 針對任何規模而且已擁有 CEA（Central-managed Endpoint Advanced ）的客戶一個提升銷售機會；
- 針對目前 SEC 管理的端點安全客戶遷移到 SOPHOS Central 的一個很好理由；
- 客戶尋求新一代端點安全防護資料的絕佳方式，或者透過與他們目前的病毒防護產品同步運行 Intercept X 或者完全切換到 SOPHOS Central Endpoint Advance + Intercept X 的整合方案。

2.Intercept X 主要提供什麼功能?

Intercept X 提供三種主要的功能：

- 漏洞攻擊防禦，詳情請參考下面說明
- CryptoGuard 惡意加密防禦的勒索防護技術。詳情請參考下面說明
- RCA - 根本原因分析，Intercept X 可以根據最近 30 天的資料分析查到哪一個用戶端是第一個被入侵，是漏洞的根源，該用戶端透過何種方式再感染到其他用戶端

3. 什麼是 anti-exploit 漏洞攻擊防禦?

漏洞攻擊防禦是阻止攻擊者透過系統或應用程式的漏洞傳遞惡意軟體。阻止這些技術代表著您不需要知道惡意軟體本身的任何內容，因此我們不必識別數百萬種不同的惡意軟體，而是專注於用於傳遞惡意軟體的 10 餘種攻擊技術 。

4. 什麼是 exploit 漏洞攻擊?

我們每天使用的軟體，如 Microsoft Office，Adobe Acrobat，您最喜愛的網路瀏覽器等等軟體都有代碼錯誤或漏洞。攻擊者尋找這些錯誤或漏洞，並嘗試使用它們做為將惡意軟體傳送到電腦的途徑。攻擊者甚至可以租用漏洞攻擊工具包來傳送惡意軟體入侵到企業的網路中。

5. 我是如何受到漏洞攻擊的？

存取一個網站，打開一個檔案附件、點選連結，是我們日常常做的事情。一般的網站可以載入部分來自不同網站的頁面。如果你正看著你最喜歡的新聞網站，它可能從不同地方載入廣告、影片和其他內容。如果其中一個網站遭到攻擊，並且其內容帶有惡意程式碼，您就可能會面臨風險，但您所做的一切都是存取瀏覽喜愛的新聞網站而已。

6. 當今人們如何對抗防禦漏洞攻擊？

Patch修補是用來對抗防禦軟體漏洞的最常用方法。如果你幸運的話，軟體供應商可能會發現或被告知有關漏洞的資訊，並在攻擊者知道前對其進行Patch 修補。前題是假設每個人都會安裝供應商推出的 Patch。

7. Intercept X 如何協助對抗防禦漏洞攻擊？

我們的漏洞防禦是會尋找被用於漏洞攻擊的技術。我們阻止使用任意其中一個技術的攻擊，並防止惡意軟體被傳遞。這並不代表著你不必安裝Patch，但它確實透過提供一個全新的、額外的保護來解決要迅速得到這些Patch 的壓力。

8. 什麼是勒索軟體？

加密勒索軟體，也被認為只是另一種形式的惡意軟體。它加密你的檔，導致你不能存取這些文件，直到你被迫支付特定金額給攻擊者。

9. 什麼是勒索軟體防護？

Intercept X 具有 CryptoGuard 惡意加密防禦的勒索防護技術。監控磁碟活動，尋找由加密勒索軟件惡意加密檔案的活動。如果它看到任何異常加密活動，它會立即停止它，並回溯可能已被加密的任何檔案。CryptoGuard 是您對抗勒索軟體的最後一道防線。

10. 為什麼我們有了Intercept X，仍需要SOPHOS或其他廠商的病毒防護/惡意軟體防護/端點防護產品？

Intercept X是對於已知的攻擊行為進行防禦，非傳統特徵碼比對惡意軟體的防護技術，故無法透過病毒特徵碼比對偵測到的惡意軟體可透過Intercept X的技術進行阻擋。但仍需要透過病毒防護/惡意軟體防護/端點防護產品在前端防範已知的病毒威脅，而無法透過端點或病毒防護產品的偵測到惡意軟體，則透過Intercept X來進行最後一道防線的防禦。

二、關於授權和部署

1. 如何獲得授權？或試用

a) Intercept X 可以被單獨銷售並和協力廠商防毒解決方案共存。
b) Intercept X 可以與端點安全防護產品
（Central-managed Endpoint Advanced CEA）搭配銷售。
c) 可以透過 SOPHOS 官網申請 30 天的免費試用。

2. 本地部署 SEC(SOPHOS Enterprise Console)管理端點安全的客戶是否可以使用Intercept X？

不能。如果本地部署 SEC 管理的端點安全客戶希望使用 Intercept X，則必須遷移到中央管理的端點（Central-managed Endpoint Advanced）或（Central-managed Endpoint Stardard）產品。

3. Intercept X 是否有計劃加入到本地部署 SEC(SOPHOS Enterprise Console)管理的端點安全防護？

我們計畫在 2017 年第一季會在 SEC(SOPHOS Enterprise Console)管理的端點新增漏洞防禦和 CryptoGuard 惡意加密防護。

4. 使用 Intercept X 需要安裝伺服器嗎？

Intercept X 是基於 SOPHOS Central 雲端的 SaaS 解決方案，使用者不需要安裝任何伺服器，只需要登入 SOPHOS Central 下載用戶端後在用戶端上運行即可，Intercept X 會透過網際網路進行更新，系統管理員可以透過 SOPHOS Central 進行政策與日誌報表的查看。