SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

端點偵測和回應專為追捕威脅和 IT 營運所設計。

Sophos Intercept X Advanced with EDR 將功能強大的端點偵測與回應 (Endpoint Detection and Response, EDR)，與無與倫比的端點保護整合在一起。追捕威脅可偵測主動攻擊者，或應用在 IT 營運上以保持 IT 健全。發現問題時，可從遠端精準回應。

主要功能

- 結合最強大端點保護的 EDR
- 專為安全分析人員與 IT 系統管理員設計的 EDR
- 主動維持 IT 作法，並在損壞發生之前及時發現威脅
- 解答對過去以及現在發生事件的任何問題
- 立即可用、完全可自訂的 SQL 查詢
- 快速存取磁碟上目前及歷史的資料，長達 90 天
- 使用命令列工具由遠端精準地回應
- 利用機器學習幫助偵測、調查事件並確定優先等級
- 加快調查速度並縮短攻擊者的停留時間
- 支援 Windows、MacOS* 和 Linix

EDR 始於最強大的防護

若要在違規發生之前就加以制止，預防非常重要。Intercept X 將全球最佳的端點保護和 EDR 整合成一個解決方案。這表示大多數威脅均可以在造成損害之前受到阻擋。Intercept X Advanced with EDR 還能夠偵測、調查並回應潛在的安全性威脅，提供額外的網路安全保證。

透過將 EDR 納入持續獲得最高評價的端點保護套件，Intercept X 可以大幅減輕 EDR 的工作負載。隨著阻止更多威脅、產生雜訊更少，分析師可以避免浪費時間處理誤報和大量的警示。

增加專業知識而非人力

使用人工智慧自動偵測、排序優先等級，以及調查威脅：Intercept X Advanced with EDR 會使用智慧學習自動偵測潛在威脅並確認其優先等級。如果發現到可疑的惡意檔案，此時使用者可利用深度學習惡意軟體分析來自動詳細分析惡意軟體、分解檔案屬性和程式碼，並將其與數百萬個其他檔案進行比較。

專業人士所設計，並為所用的立即可用型查詢：有了這些按照使用案例分類且立即可用的 SQL 查詢，安全分析師和 IT 管理員在第一天就可以上手 Sophos EDR。您可以輕鬆地修改上述查詢以進行自訂搜尋、重新建立，或是從我們的社群中取得所需工具。

透過重現市場難尋的分析師角色來回答棘手的問題：Intercept X Advanced with EDR 可以複製一般由熟練的分析人員所執行的工作，因此組織可以獲得額外的專業技術而不必增加人員。

專為追捕威脅和 IT 營運所設計

Sophos Intercept X Advanced 是第一個為 IT 管理員和安全分析師設計的 EDR 解決方案。其可為您解答端點上過去以及現在發生事件的任何問題。追捕威脅可偵測主動攻擊者，或應用在 IT 營運上以保持 IT 健全。發現問題時，可從遠端精準回應。這是藉由利用兩個關鍵功能來實現的：Live Discover (即時發現) 和 Live Response (即時回應)。

* 即將發佈

Live Discover：提出任何問題以保持領先一步 Live Discover 使安全分析人員和 IT 管理員能夠詢問和回答幾乎所有關於端點和伺服器的問題。快速發現 IT 營運問題以保持 IT 健全，並提出詳細問題以找出可疑活動。Live Discover 使用功能強大、立即可用且完全可自訂的 SQL 查詢，可以快速搜尋長達 90 天的目前和歷史磁碟資料。使用案例範例包括：

IT 營運

- 電腦為什麼執行緩慢？是否正在等待重新啟動？
- 哪些裝置有已知弱點、未知服務或未經授權的瀏覽器擴充功能？
- 執行的程式有沒有應該移除的？
- 是否已啟用遠端共用？裝置上有未加密的 SSH 金鑰嗎？是否已啟用訪客帳戶？
- 裝置是否存在特定檔案的副本？

威脅追捕

- 哪些處理程序嘗試在非標準連接埠上建立網路連線？
- 列出偵測到且對應到 MITRE ATT&CK 架構的 IoC
- 顯示最近修改了檔案或登錄機碼的處理程序
- 搜尋有關 PowerShell 執行的詳細資訊
- 識別偽裝成 services.exe 的處理程序

Live Response：從遠端精確地進行回應 發現問題後，Live Response 可讓使用者利用指令直接操作組織內的端點和伺服器。從遠端存取裝置以執行進一步調查或修復任何其他問題。系統管理員可以重新啟動設備、終止作用中的處理程序、執行指令碼、編輯設定檔、安裝/移除軟體，以及執行鑑識工具等。

託管式偵測與回應

Sophos Managed Threat Response (MTR) 服務提供由 Sophos 專家團隊提供的全天候威脅追捕、偵測與回應，是一項完全託管式服務。其他託管式偵測與回應 (MDR) 服務只能通知您攻擊或可疑事件發生，但使用 Sophos MTR，貴組織將取得一群精良的威脅追捕和回應專家的支援，他們可為您採取行動，以遏阻最複雜的威脅。選擇使用 Sophos MTR 的客戶也可以取得 Intercept X Advanced with EDR。

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
基礎技術	✓	✓	✓
深度學習	✓	✓	
反漏洞利用	✓	✓	
CryptoGuard 反勒索軟體	✓	✓	
端點偵測與回應 (EDR)	✓		

立即免費試用

取得 30 天免費試用版本
www.sophos.com/intercept-x

台灣業務窗口
電話：+886 2 7709 1980
電子郵件：Sales.Taiwan@Sophos.com

20-05-12 DS-ZHTW (MP)

SOPHOS