SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

智慧型端點偵測與回應

Sophos Intercept X Advanced with EDR 將智慧型端點偵測與回應 (Endpoint Detection and Response, EDR)，與業界頂尖的惡意軟體偵測、最佳漏洞利用防護，以及其他無人能及的端點保護功能整合在一起。

主要功能

- 結合最強大端點保護的 EDR
- 深度學習惡意軟體分析
- SophosLabs 的隨需精選威脅情報
- 以機器學習方式偵測可疑事件並排定其優先順序*
- 引導式調查使強大的 EDR 簡單易用
- 按一下滑鼠即可回應事件

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 將無人能及的防護和端點偵測與回應 (EDR) 功能整合到單一解決方案中。亦即大多數威脅均可以在造成損害之前受到阻擋，而且 Intercept X Advanced with EDR 能夠偵測、調查並回應潛在的安全性威脅，藉此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。已防範的威脅越多，安全團隊需要調查的雜訊就越少。也就是說，團隊可以將關鍵資源最佳化，進而專注於 IT 業務，不必迷失在誤報和大量的警示之中。

增加專業技術而非人力

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。其他 EDR 解決方案必須依賴技術高超的分析人員提出問題並解讀資料，但是 Intercept X Advanced with EDR 使用機器學習，並經由精選的 SophosLabs 威脅情報強化。

安全專業技術*：Intercept X Advanced with EDR 會自動偵測潛在威脅並排定其優先順序，以讓 IT 團隊取得安全專業技術。其使用機器學習，可以找出可疑事件，並將其提升為最重要且需要立即關注的事件。分析人員可以很快看到需要注意之處，並了解哪些電腦可能會受到影響。

惡意軟體專業技術：大多數的組織都使用專家來對惡意軟體進行反向工程並分析可疑的檔案。這種方法不僅耗時且難以實現，而且大多數組織的網路安全都未達這水平的先進複雜度。而Intercept X Advanced with EDR 使用深度學習惡意軟體分析提供了更好的方法，它會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。分析人員可以輕鬆查看與「已知良好」和「已知錯誤」檔案類似的屬性與程式碼區塊，以判斷應該阻擋還是放行檔案。

威脅情報專業知識：當 Intercept X Advanced with EDR 升級一個可疑的檔案時，IT 系統管理員可以檢視來自 SophosLabs 精選的隨需威脅情報 (每天接收並處理大約 40 萬個前所未見的惡意軟體樣本)，以便收集更多資訊。此一資訊連同其他收集、彙整並加以總結的威脅情報，可以輕鬆地進行分析。也就是說，即使是缺少專屬威脅情報分析人員，或是昂貴且難以理解的威脅摘要工具，安全團隊均可以從這個全球頂尖的網路安全研究和資料科學團隊受益。

引導式事件回應

Intercept X Advanced with EDR 可讓系統管理員掌握攻擊範圍、發動方式、受影響的內容以及回應方式，以便解決有關安全事件的棘手問題。各種技術等級的安全團隊都可以經由提供後續步驟建議、清晰的視覺攻擊呈現，以及內建專業技術的引導式調查，快速了解自身的安全狀況。

調查結束後，分析人員只需要按一下按鈕即可進行回應。快速回應選項包括隔離需要立即修正的端點、清除並阻擋檔案，以及建立鑑識快照。

智慧型 EDR 使用案例

智慧型 Endpoint Detection and Response 讓安全團隊具有所需的可見度和專業知識，可以解決處理事件回應工作時所發生的棘手問題。

解決有關事件的棘手問題：

- 了解安全事件的範圍和影響
- 偵測可能沒有注意到的攻擊
- 搜尋網路上的遭駭指標
- 排定事件優先順序以供進一步調查之用
- 分析檔案以判斷它們是威脅還是可能不需要的檔案
- 在任何特定時刻都能自信地回應組織的安全狀況

EDR 之外

為了阻擋最廣泛的威脅，Intercept X Advanced with EDR 採用全面性的深度防禦方法進行端點保護，而不只是依賴一種主要的安全技術。這就是“加乘的力量”，領先的基礎技術和現代技術的結合。Intercept X Advanced with EDR 將業界頂尖的惡意軟體偵測、最佳漏洞利用防護，以及智慧型端點偵測與回應 (EDR) 整合在一起。

現代技術包括深度學習的惡意軟體偵測、漏洞利用防禦和反勒索軟體等專屬功能。基礎技術則包括防毒、行為分析、惡意流量偵測、資料遺失防禦等。

Intercept X Advanced with EDR 將端點偵測與回應功能，和 Intercept X 中的嶄新功能與 Sophos Central Endpoint Protection 中的基礎技術結合在一起。 然後整合成使用單一代理程式的一個解決方案。

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
基礎技術	✓	✓		✓
深度學習	✓	✓	✓	
防漏洞利用	✓	✓	✓	
CryptoGuard 防勒索軟體	✓	✓	✓	
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

* 將在 2019 年年初上市

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

18-10-02 DS-ZHTW (3098-DD)

SOPHOS