SOPHOS
Security made simple.

Intercept X Deep Learning 深度學習

Intercept X 結合了深度學習與同級最佳漏洞利用攻擊防禦、CyptoGuard 防勒索軟體、根本原因分析等，成為業界最全面的端點保護產品。這項獨特的技術組合讓 Intercept X 得以阻止當前和未來最廣泛的端點威脅。

重點功能

- 排名第一的惡意軟體偵測引擎
- 防禦已知和前所未見的惡意軟體
- 在惡意軟體執行之前加以阻擋
- 不需要仰賴特徵碼
- 即使主機離線也能提供保護
- 約 20 毫秒內即可偵測到惡意軟體
- 經過數億個樣本的訓練
- 自 2016 年 8 月起備受 VirusTotal 驗證
- 將檔案歸類為惡意、可需要的應用程式 (PUA) 或良性
- 無需額外訓練即可立即運作
- 佔用空間相當小 (小於 20MB)
- 鎖定在 Windows 可攜式執行檔

現今的許多安全措施都是被動式的，而且太慢了。隨著端點攻擊的數量和複雜度持續增加，傳統方法一直在奮力掙扎才能勉強跟上腳步。例如，SophosLabs 每天分析超過 400,000 個新的惡意軟體樣本。讓因應此一挑戰更困難的是，SophosLabs 發現有 75% 的惡意軟體是針對單一組織而來的。

深度學習是一種先進的機器學習形式，有助於改變我們處理端點安全的方式，而引領變革的正是 Intercept X。藉著整合深度學習，Intercept X 正在將端點安全從被動式轉變為預防式，以防禦未知威脅。

深度學習對比其他機器學習類型

「Intercept X 使用了一個類似於人類大腦的深度學習神經網路 ... 其對現有和零時差的惡意軟體都有很高的準確率，並且誤報率更低。」

ESG Lab 報告，2017 年 12 月

雖然許多產品都聲稱使用機器學習，但並非所有機器學習的設計都一樣強大。在 Sophos 我們使用深度學習來偵測惡意軟體。深度學習亦稱為「深度學習神經網路」或「神經網路」，其靈感來自於人類大腦運作方式。這也是臉孔辨識、自然語言處理、自動駕駛汽車及其他電腦科學與研究先進領域中常用的同一種機器學習類型。

深度學習不斷超越其他機器學習模型，包括隨機森林 (random forest)、K-means 分群演算法或貝氏網路 (Bayesian networks)，但是需要大量資料和運算能力才能建立有效的模型。在 Sophos，由於過去 30 年 SophosLabs 的惡意軟體收集和分析工作，以及我們每天從 1 億多個端點收到的遙測數據，使得這一切變得很簡單。

相較於端點安全中常用的其他機器學習類型，深度學習具有一些先天優勢：

更聰明：深度學習透過多個分析層來處理資料，就像人類大腦中的神經元，每一層都讓這個模型更加強大。它會分析不同輸入功能之間的複雜關係。這使它能夠自動發現最佳的輸入組合和操控，而這是人類所無法做到的。這表示，Sophos 深度學習惡意軟體偵測模型能夠偵測其他機器學習引擎忽略的惡意軟體。

更具可擴展性：深度學習可簡潔地擴展到數億個訓練樣本。有鑑於 SophosLabs 每週要分析 280 萬個新惡意軟體樣本，這一點更形重要。因為能夠持續接收龐大的訓練資料，

所以我們的模型可以「記住」整個可觀察到的威脅態勢，作為訓練過程一部分。由於深度學習可處理更龐大的輸入，因能夠更準確預測現今的威脅，並且隨著時間持續維持最新此狀態。

更輕巧：傳統的機器學習方式會導致龐大的模型，有時可能需要好幾 GB 的磁碟空間；不過，Sophos 的深度學習方法是高度壓縮的模型。Sophos 深度學習模型小得令人難以置信，在端點上佔不到 20MB 空間，對效能幾乎毫無影響。

Sophos 深度學習功能

Sophos 採用業界最高效能的惡意程式偵測引擎，提供深度學習專門範疇的產品與服務：

經驗豐富：與競爭對手不同，我們長期以來一直是網路安全機器學習專家，而且多年來一直在生產環境中使用我們的惡意軟件偵測深度學習模型。Sophos 惡意軟體偵測模型是由我們資料科學家利用 DARPA 推動的技術所建立的。2010 年，美國國防部高級研究計畫局 (DARPA) 建立了 Cyber Genome Program (網路基因組計畫)，用以找出惡意軟體與其他網路威脅的 “DNA”。這正是現在 Intercept X 內部演算法的起源。

經過驗證：我們對自己的模型一直保持開放與透明。除了在 Black Hat 等業界會議上介紹我們方法的詳細資訊之外，我們也不畏懼讓獨立的第三方測試我們的模型。我們的模型自 2016 年 8 月起，經過 VirusTotal 驗證，並且獲得第三方測試者 (例如 NSS Labs) 的高評分。在所有情況下，它已經過證明相當有效，而且誤報率很低。

> 「這是我們在效能測試中見過的最好成績之一。」
>
> AV-TEST 技術長 Mailk Morgenstern

高效能：Sophos 深度學習技術快得令人難以置信。我們的模型能夠在不到 20 毫秒內，從檔案中擷取數百萬個特徵、進行深度分析，並確定其為良性還是惡意。這整個過程都在檔案執行之前就完成。

SophosLabs：不論什麼模型，最重要的一點是用來訓練的資料。我們的資料科學家團隊是 SophosLabs 小組的一部分，他們可以存取數以億計的樣本。這讓他們能夠在我們模型中建立最佳預測。這兩個小組的整合也造就了更好的資料標籤 (因此建立更優秀的模型)。資料科學家團隊和威脅研究人員之間，威脅情報與真實世界回饋的雙向共用，提升了我們模型的準確性。

> 「Intercept X 擋住了我們測試的每一個複雜的進階型攻擊。」
>
> ESG Lab 報告，2017 年 12 月