deep instinct

傳統防毒已失效

在 20 毫秒內阻止 >99% 的未知威脅

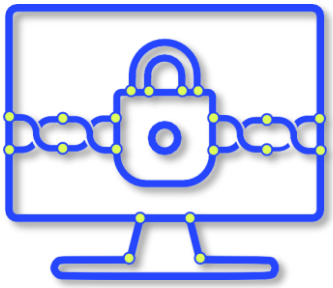
替換您的傳統和次世代防毒（NGAV）工具，以更快、更準確地預防勒索軟體和未知威脅，同時減少誤報和警報。

取代傳統防毒

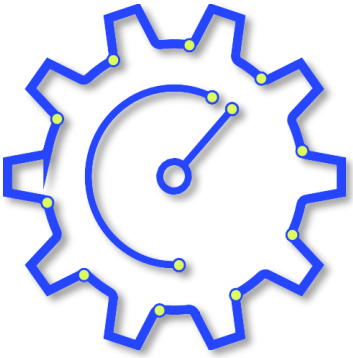
真正的預防，無需病毒庫

傳統的防毒如 Symantec、McAfee、BitDefender、趨勢科技、卡巴斯基等解決方案，尚未發展到能夠保護您免受未知威脅。**Deep Instinct** 實現了其他人幾十年來一直承諾的事情—**在執行之前阻止超過 99% 的已知和未知威脅，實現真正的預防為先的保護。**

防止勒索軟體和零時差威脅（執行前）



傳統的防毒和次世代防毒解決方案無法保護您免受零日威脅。每天都有數以十萬計的新勒索軟體變種和未知惡意軟體被釋放到網路上，而您的傳統防毒安全措施無法阻止它們。 Deep Instinct 可在勒索軟體和未知攻擊執行前 20 毫秒內預先阻止他們。



速度和規模無需持續不斷調整

傳統的防毒解決方案並不是為了防止未知攻擊而設計的—它們使用基於簽名的機器學習(ML)模型，需要不斷的人工更新和調整模型才能有效用。Deep Instinct 可防止超過 99% 的已知和未知威脅，且無需雲端檢查或持續更新。

低誤報率，提高 SOC 生產力

防毒解決方案通常雜訊很多，而且容易出現誤報。Deep Instinct 的誤報率低於 0.1%，可確保安全團隊不會在真正的威脅繞過控制時追逐誤判的警報。

真正以預防為主的安全軟體

透過 Deep Instinct 最先進的深度學習預防解決方案步入未來。

	deep instinct	防毒軟體
對勒索軟體	**執行前預防** 在攻擊洩漏資料或加密系統之前，預先防止執行勒索軟體、未知威脅和零時差威脅。	**反應式機器學習** 依賴啟發式和行為分析，決策通常會被延遲到威脅執行後。
速度	決策時間<20 毫秒 在 20 毫秒內對已知和未知威脅做出高度準確的惡意與良性判斷，無需額外威脅情報來源。	**數分鐘到數小時** 依賴雲端檢查簽名和威脅情報，導致對已知威脅反應緩慢，且無法捕捉未知威脅。
誤報率	**<0.1%** 業界最低的誤報率 (<0.1%) — 提高營運效率。	**雜訊眾多** 以高誤報率著稱，導致警報疲勞和 SOC 生產力降低。
離線保護	**時刻受保護** 全天候、無論在線還是離線，提供全面保護。	**無離線支援** 需要持續的保持連網以維持效能。
功效和準確性	**阻止超過 99%的未知威脅** 直觀判斷文件是否包含惡意內容，包括潛在的垃圾程式（PUA），以預防未知威脅。	**會錯過未知威脅** 需要持續的模型更新，決策會被延遲並降低準確性。且必須在先進的沙盒中"引爆可疑檔案"，以告知其是否有害。
對高級攻擊	**創新的** 了解攻擊的真實 DNA。Deep Instinct 神經網路可識別並防止包括對抗性人工智慧在內的高級複雜攻擊。	**傳統** 不是設計用於識別和阻止無檔案攻擊(如程式碼注入或記憶體攻擊)。並非旨在阻止基於機器學習的新攻擊。
創新/人工智慧	**主動深度學習** 原生建立在唯一基於深度學習的網路安全框架上，專門開發用於在執行之前預防當今複雜的未知威脅，而不是威脅執行之後阻止。	**基於簽名反應** 有限且需改進的機器學習功能無法有效應對當今的挑戰。基於簽名的引擎必須不斷更新才能有效。
Agent 複雜	**輕量** 單一、輕量級 Agent，低 CPU 和記憶體消耗。	**資源密集型** 需要多個 Agent 和模組、高 CPU 和記憶體。

傳統防毒已經過時了

透過 Deep Instinct，您可以實現以下目標：

在勒索軟體執行前將其停止。
避免資料外洩以及被勒索。

預防未知威脅。
降低風險，避免後續重建成本。

提升安全運營效能。
減少誤報，人員能夠專注於最關鍵的問題。