白皮書

惡意軟體分類在威脅預防中的重要性

deep instinct™

www.deepinstinct.com

內容提要

快速決策資安事件的優先處理順序，有賴於對惡意軟體能夠精準分類。透過瞭解上述分類，能讓工作繁重的安全營運團隊，能同時處理最緊急的威脅與忽略誤報訊息。為了成功做到這點，你需要了解為何你的網路安全供應商能通過準確的分類和威脅嚴重性評比分級，來阻止或是預防威脅。使組織可以更深入地了解當下的環境威脅，並可以利用這些訊息來降低整體風險。

對威脅立即進行分類

大多數安全解決方案都在威脅事件發生後才對惡意軟體分類，而且都是根據目前已知記錄的病毒資料庫所做出的決定。(ps:如果分類已經完成的話) Deep Instinct 在網路安全上的角色是預防威脅，這是建立在深度學習下，也是首創於深度學習的成果。深度學習使 Deep Instinct 能夠立即準確地對以下網絡威脅進行分類，而這些威脅程度超過任何已知的網路威脅，如零日、勒索軟體和前所未見也未知的惡意軟體。有了這些分類訊息，能讓安全運營團隊可以立即就預防和報告的安全事件做出關鍵決策。

專注於真正重要的事件

你可以從預防和報告事件中，立即優先知曉威脅事件的分類是勒索軟體還是間諜軟體引起的。舉例來說，Deep Instinct的巨大優勢就是能透過事件區分出這是一個低優先級的廣告軟體事件，還是這是一個高優先級的勒索軟體所做的初期攻擊活動。

將威脅樣貌導入到MITRE

因為 Deep Instinct 可以預先防止威脅被執行。對 SOC 團隊來說，他們可以聰明地優先調查高嚴重性警報，而且不必擔心即將發生的違規行為。而不是只能決定如何處理已常見的 “被阻止” 事件。透過使用 Deep Instinct 的自動分類，能將威脅樣貌導入到 MITRE，您可以獲得威脅類型和嚴重性的完整上下鏈接，從而進一步加快調查時間。

您應該堅持立即分類的惡意軟體類型包括：

- 勒索軟體
- 病毒植入程式
- 間諜軟體
- 蠕蟲
- 後門程式
- 潛在有害威脅應用程式 (PUAs)
- 病毒

為什麼要關心威脅分類？

隨著現代 IT 環境變得越來越複雜和分散，警報越來越難以管理和維護，大量的誤報與需要分類的威脅加劇了這種情況，導致安全運營中心 (SOC) 團隊正淹沒在警報的海洋中，這讓駭客攻擊成了無窮無盡的打擊手段。誤報會使得安全運營中心(SOC)在處理安全事件的量能被限制，這通常會導致讓可能包含潛在有害威脅的應用程式 (PUA)之警報會被忽略。

警報的大量湧入有一個很大的原因，就是事件的分類與優先級判斷不夠快，無法做出決策。錯誤的分類或是無法分類的警報導致訊息不正確的過濾，使得這些成千上萬的文件，導向您的EDR、SIEM 或其他 SOC 審查的分析工具做無用的解析。

前面我們提到警報會迅速增加的一個原因，就是在事件的分類或優先權處理上不夠快，導致無法做出決策。往上再追溯，還可以追溯到傳統的防毒(AV)、端點保護(EPP)與端點偵測與回應(EPP)等工具。這些工具基本上是建立在機器學習(Machine Learning)上，因為保護過多(減低機器學習速度與增加大量誤報，導致淹沒了SOC團隊)，基於上述導致這類產品缺乏精準度、速度與可擴充性，無法預測與預防未知惡意軟體和零日威脅，最終導致這些威脅滲透到您的組織。

立即對惡意軟體進行分類並不容易。因為它需要對威脅環境有廣泛了解，並且要有效的自動化才能使分類如閃電般的快速進行。透過深度學習應用於網路安全，這提供了在軟體執行前預防威脅的機會，並實現了自動化對即時惡意軟體分類。

本白皮書將涵蓋的主題：

- 惡意軟體威脅分類至關重要的三個原因
- 深度學習：預防和分類威脅
- 更深入地瞭解惡意軟體分類
- Deep Instinct： 開創性的即時威脅分類

為什麼惡意軟體分類很重要？

1.您需要立即瞭解和理解威脅

現今的SOC團隊，他們在關鍵所需要的資源上是短缺的。而這個關鍵資源就是人才，一個能應對警報和安全事件的合格專業安全人員。雖然缺乏經驗豐富的安全專業人員並不是一個新的問題，但事實上這問題正在惡化中。

為了提高處理惡意軟體的分類效率，通常的做法就是上傳到雲端檢查，但是這動作不會被即時處理，在處理過程中造成了等待延遲與反應過慢。此外，大多數的安全廠商都是基於已知的惡意軟體去分析，對於未知變種的惡意軟體卻沒有任何措施。這樣導致了因延遲識別和回應勒索軟體、零日威脅與未知威脅，造成可能產生災難性的後果。

當 SOC 團隊擁有相關即時並精確的惡意檔案、威脅分類和威脅嚴重性之細節時，他們就會獲得針對回應駭客的關鍵優勢。而且分類減少了對人工互動的需求，減輕了僱用更多熟練分析師的壓力。

2.您的反應必須快速準確

時間就是金錢。如果威脅能在被預防的同時也進行分類，SOC 和 IR 團隊將擁有準確、即時的資訊，如此就能在不會影響生產環境下，確定優先順序並做出快速回應。這將最終提高企業的效率，因為它不會浪費分析師寶貴的時間來追逐誤報資訊。

那些在威脅攻擊後再對其進行分析，才能確定被什麼攻擊的企業，通常會讓受影響的系統離線，並且對其進行隔離和分類，然而到這時候以為時已晚。

要進行詳細調查，還要找出還有哪些系統受到影響或哪些其他系統受到感染，需要更多的時間和資源。最後，補救和清理工作(包括刪除和重新恢復系統)，通常這會導致代價高昂的生產停機時間，並可能導致更大的財務和企業營業損失。

惡意軟體類型的自動分類，能讓安全管理員針對威脅嚴重等級與惡意軟體類型，規劃更細緻的策略規則。

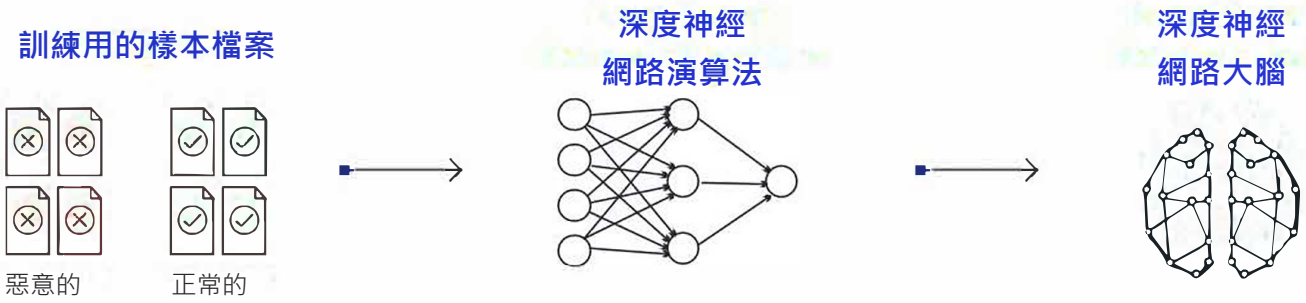
3. 政策需要精細度、自動化和可控制的

在大多數環境中，安全策略的限制越嚴格，會使得使用者的生產力越有可能受到不利影響。通過即時對惡意軟體類型進行分類，組織可以設置自動策略，以立即阻止具有惡意評分的所有惡意威脅檔案。

設置策略規則的能力對於確保正確分類和防止惡意檔案至關重要，例如創建規則以僅防止被歸類為間諜軟體的可疑檔案，而允許其他檔案運行。

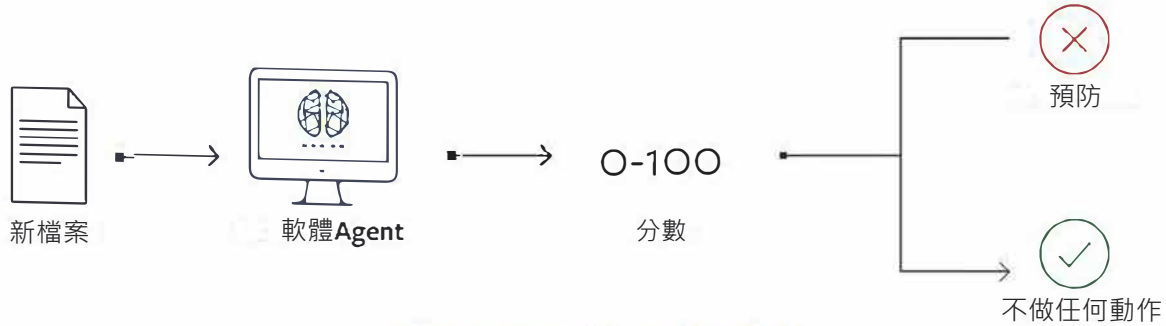
更早、更快地預防和分類威脅

首先，企業需要在惡意軟體執行和爆發大規模感染之前防止更多的威脅。這需要充分了解隱藏在每個檔案或腳本中的潛在威脅。早期分類是在這一努力中取得成功的關鍵要素。Deep Instinct在預防和分類威脅方面的速度和準確性是通過我們的深度神經網路（DNN）大腦實現的，它是在數以億計的訓練樣本上訓練出來的--包括惡意和良性的。培訓的結果是一個輕量級模組，分佈在端點、伺服器和行動裝置的軟體agent中。 該模組還可以作為 SDK提供給第三方系統做整合。



大腦的深度學習訓練

一旦部署，任何嘗試訪問設備的新檔案、程式或記憶體注入都會被深度神經網路大腦（DNN）掃描並給出分數，所有動作都在<20毫秒以內判別，比已知勒索軟體的最快加密速度還要快上750倍。該分數表示檔案的惡意級別。根據預先定義的策略閾值，軟體agent決定檔案是惡意的還是良性的，並且根據此結果，它將阻止或允許它運行。



檔案的評估與操作

深入瞭解惡意軟體分類

基於深度學習的解決方案不僅可以防止惡意檔案寫入磁碟或在記憶體中運行，它還可以通過針對企業的惡意軟體的類型進行分類，提供額外的威脅情報。

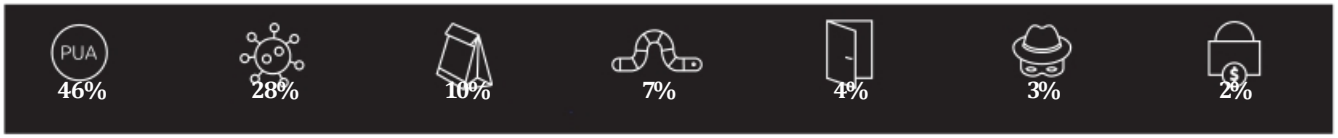
這方面的一個完美例子是潛在的不需要的應用程序（PUA）。PUA 很容易讓安全團隊不知所措，警報往往被忽視或關閉。惡意軟體駭客深知這一點，並經常在PUA 中隱藏惡意程式碼。由於大多數安全解決方案只查看文件的一小部分 bits 和bytes，並在文件運行後進行一種分類，因此武器化的 PUA 往往被忽略，直到發現感染時，已經為時已晚。

Deep Instinct 的深度分類檢查了檔案的完整內容，而不僅僅是 bits 和 bytes，並將二進位檔案分解成其各個部分（見下圖）。 這種分解使 Deep Instinct 能夠輕鬆確定 PUA 構成的威脅級別，並在感染發生之前防止它。

只要有 1%的 PUA 包含勒索軟體，則可以 100% 保證在忽略 PUA 時，惡意軟體將執行。 雖然像 MDR 或 EDR 這樣的安全工具可能會在運行時之前發現已知的威脅，但依靠它們進行檢測和回應意味著未知的惡意軟體將運行並執行，然後您依靠執行後的行為分析來阻止威脅的發生。

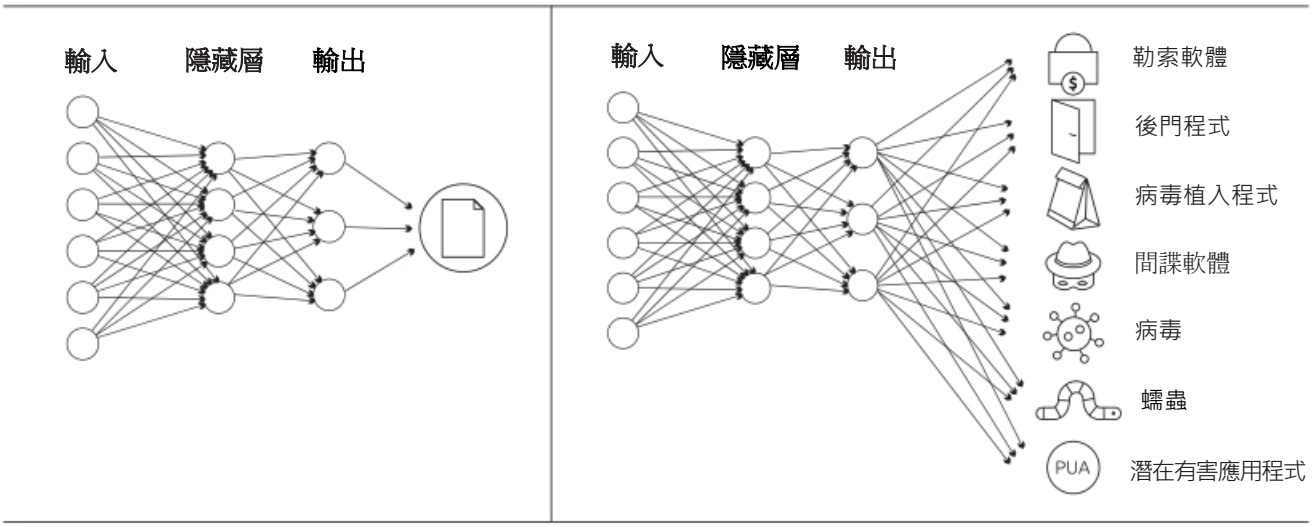
深度分類

深度分類細分示例：



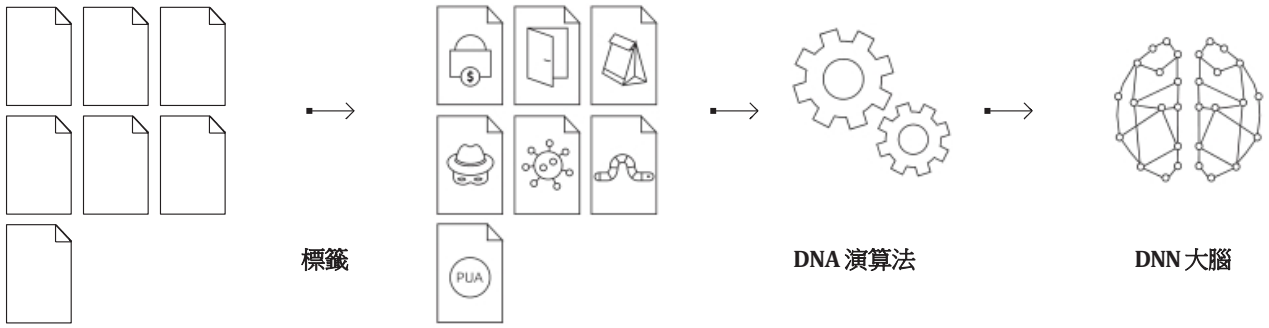
利用深度學習對惡意軟體進行分類，實現實時威脅情報

想一想您如何確定威脅的優先順序。如果您的系統上發出了三個警報，您將如何確定回應的優先順序？例如，如果您立即知道兩個警報是用戶設備上的廣告軟體，另一個是關鍵生產伺服器上的勒索軟體，則您會很明確的決定將在哪裡分配資源。



使用 Deep Instinct 的深度神經網路大腦，用於識別檔案惡意性的輸出層為 1 到 100。 但是，要對惡意軟體類型進行分類，DNN 將具有多個輸出，並且它們在分析期間將根據發現的惡意軟體類型和系列特徵分解為百分比。

一個惡意軟體樣本擁有不同惡意軟體家族類型的多個元件是很常見的。Deep Instinct 可以識別這些特徵，並為分析的每個文件提供按百分比分列的項目。



利用 Deep Instincts 的深度學習進行分類過程的高級流程。

我們的深度神經網路大腦是如何訓練的

1. **標籤** - 數以百萬計的惡意軟體樣本根據其惡意軟體類型進行了標注。
2. **餵養和訓練** - 然後將這些標籤樣本輸入到深度學習演算法中，該演算法確定惡意軟體的特徵和模式。訓練使 Deep Instinct 能夠在檢查檔案時快速準確地識別每種惡意軟體類型的關鍵特徵，並應用適當的威脅即時分類。

開創性的即時威脅分類

Deep Instinct 是唯一提供即時網路威脅分類和嚴重等級的解決方案，它與嚴重程度評級相結合，在未知威脅感染你的環境之前阻止它們。在評估威脅分類時要檢查的一個關鍵區別是確保它適用於從未見過的威脅和零日威脅，而不僅僅是已知的威脅。在允許惡意軟體執行之前，必須確定它。
Deep Instinct 對七種惡意軟體系列進行了分類。可用的分類如下 ：

勒索軟體 — 一種加密、發佈、擦除或阻止受害者數據的威脅，除非支付贖金。

後門程式— 一種繞過身份驗證、特權或加密來訪問數據、 計算機或網路的威脅。

病毒植入程式（dropper）— 一種在目標系統上安裝惡意軟體的威脅（惡意軟體元件）。

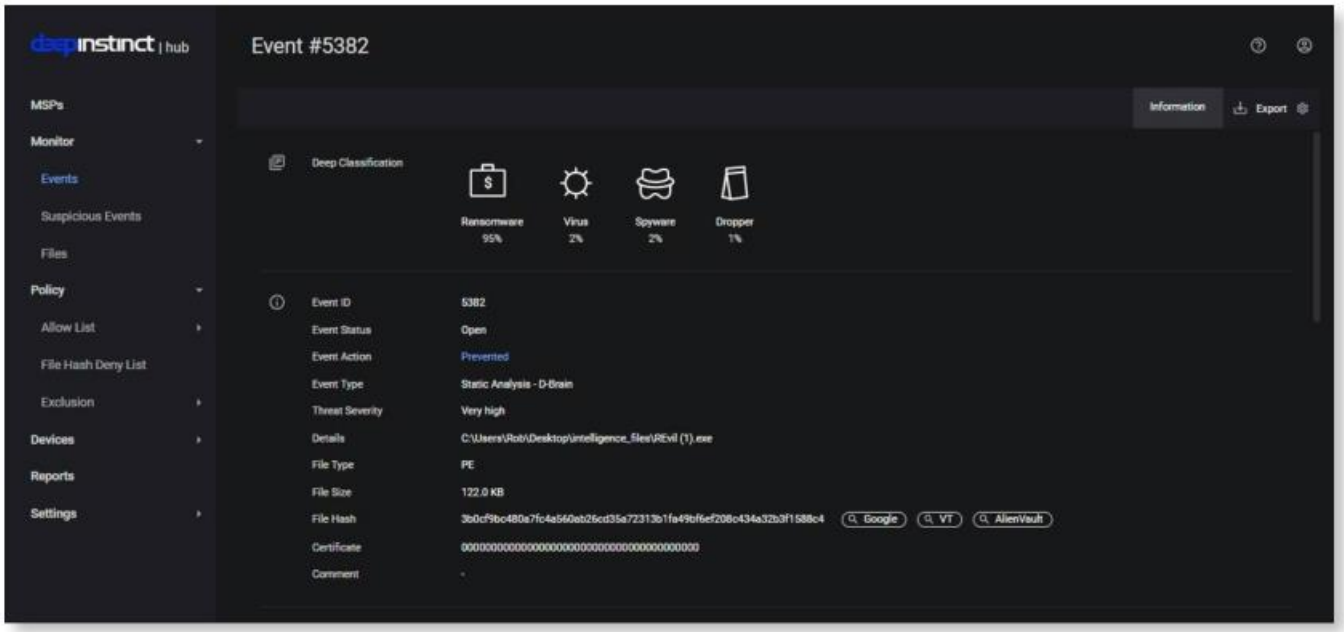
潛在有害應用程式（PUA）—可損害隱私、削弱計算機或網路安全，或下載/安裝其他內容或展示廣告。

間諜軟體 —它收集有關計算機、個人或組織的資訊。

病毒 — 一種威脅，在執行時，通過修改其他計算機程式並插入自己的程式碼來自我複製。

蠕蟲 — 一種威脅（獨立程式），可自我複製以傳播到其他計算機。

下圖取自 Deep Instinct 管理控制台，顯示了一個被阻止的事件，其威脅嚴重程度為 "非常高"。在警報的頂部，「深度分類」部分顯示惡意軟體樣本的細分，並提供威脅分析，然後報告傳回威脅的結構。在此範例中，此威脅主要是勒索軟體（95%），但也包含病毒（2%）、間諜軟體（2%）和病毒植入程式（1%）的特徵。這意味著威脅不僅是勒索軟體，而且還可能從目標系統捕獲資訊，在網路上散布更多惡意檔案，並傳播像病毒一樣。請務必瞭解，如果不加以阻止，此惡意檔案中包含的任何威脅都可能成功。



通過為企業和安全專業人員提供即時對威脅進行分類和評級的能力，團隊可以確定威脅的優先順序，並更有效地應對他們收到的威脅警報。安全專業人員需要盡可能多的情報來確定對感知到的威脅做出最佳應對，並儘快做出此決定。 Deep Instinct 為組織提供了所需的工具，讓他們可以花更少的時間研究威脅，並更快地回應重要的威脅。

惡意軟體分類是更早阻止攻擊的關鍵元件。在討論分類時，必須同時考慮已知和未知威脅，如惡意軟體和零日變種。

正確的分類使您的 SOC 能夠：

- 對關鍵威脅進行優先排序，並根據風險做出判斷。
- 用meta-data和威脅嚴重程度等級處理關鍵威脅。
- 適當分配關鍵資源，包括人員和時間，以應對安全威脅。

企業需要對被阻止的威脅提出更多問題，以挖掘 "何時和為何"。你目前的解決方案能提供什麼資料，能詳細解釋威脅，按類型和嚴重程度分類，對你的環境意味著什麼？為了領先於威脅，我們需要更多的信息，更早、更快，以優化資源，將惡意檔案擋在外面。

Deep Instinct 是唯一能提供深度分類的解決方案，在威脅感染你的環境之前就加以預防。

為什麼選擇《Deep Instinct》

Deep Instinct 以業內最高的準確度和最低的誤報率來阻止已知、未知和零日威脅。對於您的企業而言，這意味著降低風險、提高 SOC 效率、更全面的安全性，並瞭解駭客攻擊手法。

Deep Instinct 預防平臺基於世界上第一個也是唯一一個專門構建的深度學習網路安全框架，並由模仿的深度神經網路（大腦）提供支援擁有人腦的邏輯和學習能力。深度學習是人工智慧最先進的形式，其靈感來自人腦的學習能力。一旦人腦學會識別一個物體，它的識別就變成了習慣且是自動的。

Deep Instinct 的深度學習演算法能夠處理大量原始數據，從而對所分析的數據有深刻而高度準確的理解。這就是為什麼深度學習是構建自學應用的首選方法，它推動了語音和語言處理、圖像識別、自動駕駛汽車，甚至在診斷高級醫療保健測試方面的創新。

Deep Instinct 可減少誤報，因為它可以更準確地識別和分類惡意威脅。無論威脅是已知惡意軟體還是未知、零日或 APT，Deep Instinct 都能比其他 EPP 和 EDR 工具更精確地識別這些威脅，從而提供要發送到 SOC 進行分析的錯誤分類威脅要少得多。

保證誤報少。

Deep Instinct提供無與倫比的威脅檢測準確性和分類。我們提供業界首個<0.1%的誤報率。這包括未知和零日威脅。

通過關注實際威脅來優化 SOC。

花在追跡誤報上的時間是從尋找威脅和加强安全狀態中抽出的時間。 將時間花在真正的威脅上，而不是誤報上，提高運營效率。

進一步閱讀：

- 8 Reasons Why EDR is Not Enough eBook
- 2022 Cyber Threat Landscape Report
- Voice of SecOps Report
- Ransomware: Prevention is Better than the Cure
- What is Arid Gopher? An Analysis of a New, Never-Before-Seen Malware Variant
- Log4Shell (CVE-2021-44228) – What You Need to Know
- The Re-Emergence of Emotet
- 2022 MITRE Engenuity ATT&CK® Evaluations Highlight Deep Instinct's Unique Prevention-First Approach to Cybersecurity

deep instinct

Deep Instinct 採用預防優先的方法，使用世界上第一個也是唯一一個專門構建的深度學習網路安全框架來阻止勒索軟體和其他惡意軟體。我們在 <20 毫秒內預測和預防已知、未知和零日威脅，比勒索軟體加密速度快上 750 倍。 Deep Instinct 具有>99%的零日準確率，並承諾 <0.1%的誤報率。 Deep Instinct Prevention Platform 是每個安全堆疊的重要補充，可針對混合環境中的威脅提供完整的多層保護。