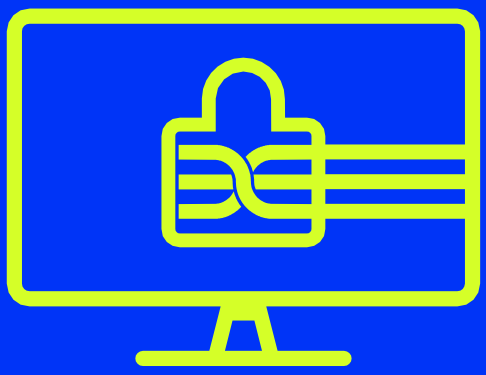
型錄

端點安全



世界上唯一基於
深度學習
的網路安全解決方案

防止
>99%
已知、未知、以及零日 威脅

防止 威脅 所需時間
<20毫秒

每年只需
1-2 次更新

預防未知攻擊在 <20毫秒內

今天駭客有的是時間——而你確沒有時間 。

從惡意軟體在端點上執行的那一刻起，就是在與時間賽跑。傳統的安全解決方案很難快速檢測和回應未知威脅，可能需要幾分鐘、幾小時甚至幾天的時間才能檢測完成。在此漫長的時間檢測，導致惡意軟體已經成功入侵並且竊取機密檔案以及加密重要檔案。傳統的防毒軟體靠更新病毒碼及啟發式的機制只能防止已知攻擊，但對未知和零日攻擊在很大程度上是無效的。

Deep Instinct 可以在端點攻擊前 <20 毫秒內阻止勒索軟體和其他已知、未知的零日威脅。

Deep Instinct的端點安全防禦是輕量級解決方案，Deep Instinct for Endpoint 針對已知或是未知惡意軟體攻擊精準度>99%，精準度高所以誤報率低於0.1%提高現有安全解決方案的有效性，並降低組織的整體風險。您的安全團隊將花費更少的時間來回應良性警報，而將更多的時間用於關注更高價值的優先事項，如威脅搜尋、修補和強化防禦。

Deep Instinct的差異：深度學習與機器學習

端點檢測和回應（EDR）解決方案依賴於基本的機器學習技術。此方法要求攻擊開始執行時，然後才能檢測到它。但是，勒索軟體在15秒內就已經加密完成，而EDR解決方案可能需要幾分鐘或幾小時才能檢測到攻擊並做出回應。當 EDR工具檢測到攻擊時，您的網路端點上已經被駭客安裝了droppers、artifacts等惡意軟體。

借助多個深度學習引擎，Deep Instinct 的多層預防方法可提供最高的效率和最快的檢測速度。這適用於已知和從未見過的惡意軟體，以及無檔案、記憶體中和基於腳本的攻擊。Deep Instinct 還可以檢測可疑行為，以改進您的威脅搜尋、 調查和根本原因分析。

產品優勢

- 在 <20 毫秒內預防已知、未知和零日威脅
- 通過將誤報大幅降低到<0.1%，節省安全團隊的時間
- 確保惡意軟體不會在您的端點上執行
- 阻止多階段、 複雜的勒索軟體攻擊
- 針對最複雜的攻擊實施分層預防
- 抵禦駭客利用AI攻擊
- 不需要雲端分析查找

端點的Deep Instinct

當駭客試圖在其目標端點上放置惡意軟體時，Deep Instinct for Endpoint 會在執行之前阻止它。

Deep Instinct 率先在網路安全中使用深度學習，以防止已知和未知的惡意軟體，零日漏洞，勒索軟體和常見的基於腳本的攻擊，適用於最廣泛的檔案類型，速度更快判斷，誤報更少，有別於依賴於病毒碼、啟發式或基於機器學習的安全工具。

預測和預防：執行前靜態分析

通過Deep Instinct 的靜態分析engine，防止>99%的已知和未知惡意軟體，包括勒索軟體，零日，基於檔案和基於script的攻擊。

- 已知的惡意軟體
- 未知的惡意軟體和變種
- 基於文件的攻擊
- 零日漏洞利用
- 勒索軟體
- 通用腳本

靜態分析檔案類型

- PE
- PDF
- Office
- 巨集
- RTF
- Swf
- JAR
- TiFF
- Fonts
- Mack-O
- ELF
- APK
- JDT
- HWP
- LNK

Script控件覆蓋率

- PowerShell
- JavaScript
- VBScript
- 巨集
- HTML 應用程式（HTA 檔案）
- rundll32

執行時：動態和行為分析

Deep Instinct使用多層次過濾預防方法，採用另外的動態和行為分析層來檢測和自動回應最高級的威脅，包括：

- 無文件攻擊
- 遠端程式碼注入攻擊 (Reflective.NET,Reflective DLL)
- 已知、未知 Shellcode
- 憑據盜竊
- 躲避防毒軟體掃描
- 憑據轉儲
- 間諜軟體，包括銀行特洛伊木馬、鍵盤記錄程式和病毒植入程式(droppers)
- 高級腳本，如未知shellcode
- 多階段攻擊
- 主動對抗性AI攻擊

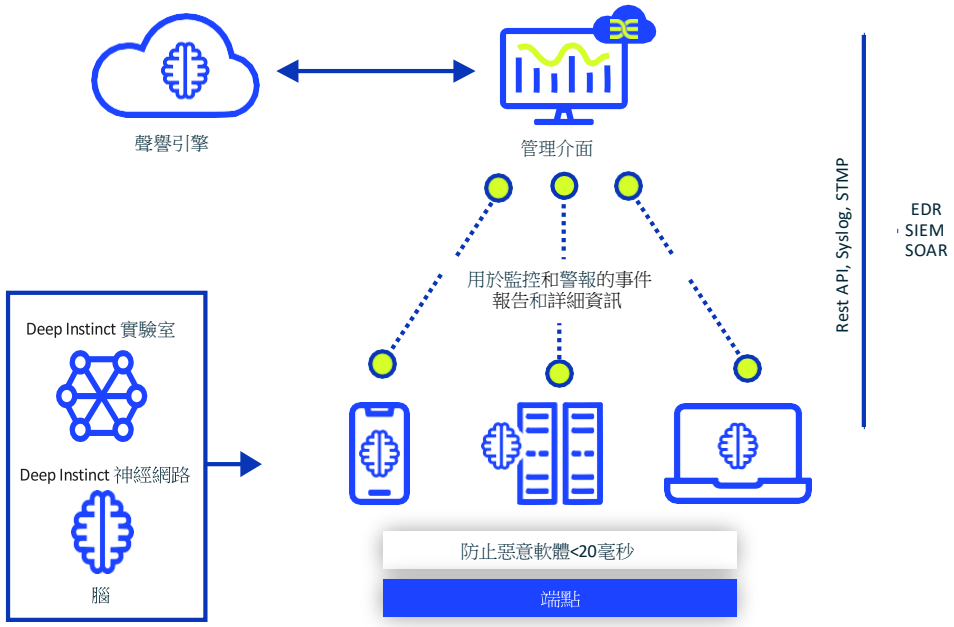
此外，Deep Instinct 還提供了上下關聯性來了解威脅的嚴重性和策略 ：

- 針對威脅搜尋的可疑事件發出警報
- 映射到 MITRE ATT&CK 以用於了解駭客攻擊技術
- 進行聲譽分析

執行後：自動分析

Deep Instinct 包括可選的自動化和信譽分析，可以覆蓋基於策略和導入的允許清單的決策。

產品架構



自動回應並與SIEM、EDR、SOAR整合

所有被阻止的事件都會被發送到 Deap Instinct 控制台，惡意軟體會立即被分類，以提供對嘗試攻擊的上下關聯性 。 組織可以制定手動或自動回應以實現以下目標：

- 隔離裝置
- 隔離/刪除/恢復檔案
- 更新策略：允許和還原（Hash、憑證、 資料夾、 腳本、 程序）
- 終止程序
- 清理註冊表以刪除持久性
- 將阻止的事件發送到沙箱以進行進一步分析

Deep Instinct 通過REST API、Syslog和SMTP與您的SIEM、SOAR、EDR或其他現有安全工具整合，以改進調查、修復和威脅搜尋。

附加功能

Deep Instinct 將我們領先的網路防禦功能與直覺的功能集相結合，幫助我們的客戶節省時間並更智慧地工作。

專業UI和儀錶板
我們易於導覽且高度直覺的管理控制台可以進行定製，以預測對授權最終使用者最重要的內容 。

內置報告
自動和臨時的威脅和趨勢報告。

真正的多租戶
面向合作夥伴、MSP和MSSP的本機多租戶解決方案可確保所有數據安全並隔離交叉污染，並從一個集中式控制台管理多個環境。

增強的安全性
所有管理操作、基於角色的存取控制、2FA和SAML整合的完整審核日誌記錄/記錄。

基於組的策略
根據各種手動或自動標準（包括命名約定、IP、AD、OU等）配置安全策略。

支援的虛擬環境

- Amazon Workspaces
- Citrix Hypervisor and XenDesktop
- Vmware ESX and Horizon
- Microsoft Hyper-V

支援的系統

- Windows
- macOS
- Android
- Chrome OS
- Linux

www.deepinstinct.com | info@deepinstinct.com

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 ，比最快的勒索軟體加密速度快 750 倍。 Deep Instinct 具有>99%的零日準確率，並承諾<0.1%的誤報率。Deep Instinct防護平臺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。