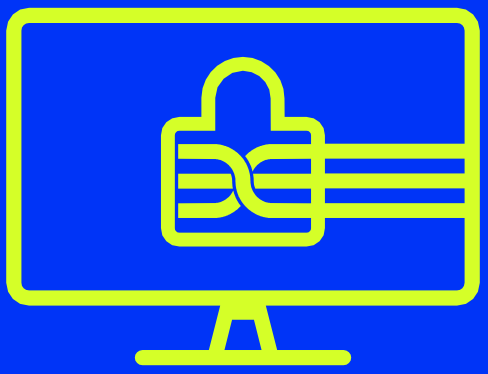
DATASHEET

Deep Instinct for Endpoint



全球唯一
基於深度學習
的網絡安全解決方案

可防禦
超過99%
已知、未知和零日威脅

在
20毫秒以內
預防威脅

每年僅需
1-2次更新

在<20ms內阻止未知攻擊

今天的對手在時間上有很大的優勢，而您則不然。

從惡意軟體在端點上執行的瞬間開始，要阻止它就成了一場與時間的賽跑。傳統的安全解決方案在快速檢測和應對未知威脅方面表現不佳，需要花費數分鐘、數小時甚至數天的時間—在此期間，惡意軟體已經成功入侵您的環境。傳統的防毒、特徵碼、規則和啟發式工具可以防止已知攻擊，但對未知和零日威脅效果則有限。

Deep Instinct能在端點上被執行攻擊之前，以不到20毫秒的速度，阻止勒索軟體和其他已知、未知、零日威脅。

透過輕量化的端點解決方案，Deep Instinct for Endpoint 可預防超過99% 的已知和未知惡意軟體威脅且誤判低，提升現有安全解決方案的效能並降低組織的整體風險。您的安全團隊將花更少的時間回應無害的警報，可以有更多時間集中於高風險的事件。

Deep Instinct的區別：深度學習與機器學習

端點檢測和響應（EDR）解決方案依賴於機器學習技術。這種方法需要惡意軟體開始執行後，才能偵測到。例如，勒索軟體在15秒內開始加密，但平均的EDR解決方案可能需要數分鐘或數小時才能檢測到，這對於阻止入侵來說太慢。在EDR工具檢測到攻擊的時候，惡意的下載和工具已經被部署在您的網路端點上。

憑藉多個深度學習引擎，Deep Instinct的多層次防護方法提供了最高效能和最快速的偵測與預防。這適用於已知和從未見過的惡意軟體，以及無文件、記憶體中和基於腳本的攻擊。Deep Instinct還能夠檢測可疑行為，以提升您的威脅搜尋、調查和根本原因分析。

產品優勢

- 在20毫秒內阻止已知、未知和零日威脅
- 將誤報率大幅降低於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被執行
- 阻止多階段、複雜的勒索軟體攻擊
- 對最複雜的攻擊實行分層預防
- 保護免受對抗性人工智能的威脅
- 不需要進行雲端分析

對端點的Deep Instinct

當駭客試圖在目標端點上部署惡意軟體時，Deep Instinct會在端點執行之前阻止它。

Deep Instinct在網路安全領域首創使用深度學習，預防各種檔案類型中已知和未知的惡意軟體、零日攻擊、勒索軟體以及常見的基於腳本的攻擊，相對於依賴於特徵碼、啟發式或基於機器學習的安全工具，較快速且較少誤判。

預測和預防：執行前的靜態分析

使用Deep Instinct的靜態分析引擎，可預防超過99%的已知和未知惡意軟體，包括勒索軟體、零日攻擊、基於檔案和基於腳本的攻擊。

- 已知惡意軟體
- 未知的惡意軟體和其變種
- 基於檔案的攻擊
- 零日漏洞利用
- 勒索軟體
- 常用腳本

靜態分析檔案類型

- PE
- PDF
- Office
- Macro
- RTF
- SWF
- JAR
- TIFF
- Fonts
- Mach-O
- ELF
- APK
- JTD
- HWP
- LNK

腳本控制涵蓋範圍

- PowerShell
- JavaScript
- VBScript
- Macros
- HTML applications (HTA files)
- rundll32

執行時：動態和行為分析

Deep Instinct採用了額外的動態和行為分析層次，通過使用多層次的預防方法，檢測並自動應對最先進的威脅，包括以下方面：

- 無文件攻擊
- 遠端代碼注入 (Reflective .NET, Reflective DLL)
- 已知、未知的 Shellcode
- 憑證竊取
- AMSI繞道
- 間諜軟體，如銀行木馬、鍵盤側錄和植入程序
- 高級腳本，如未知的shellcode
- 多階段攻擊
- 主動式對抗性人工智能攻擊
- 憑證轉儲

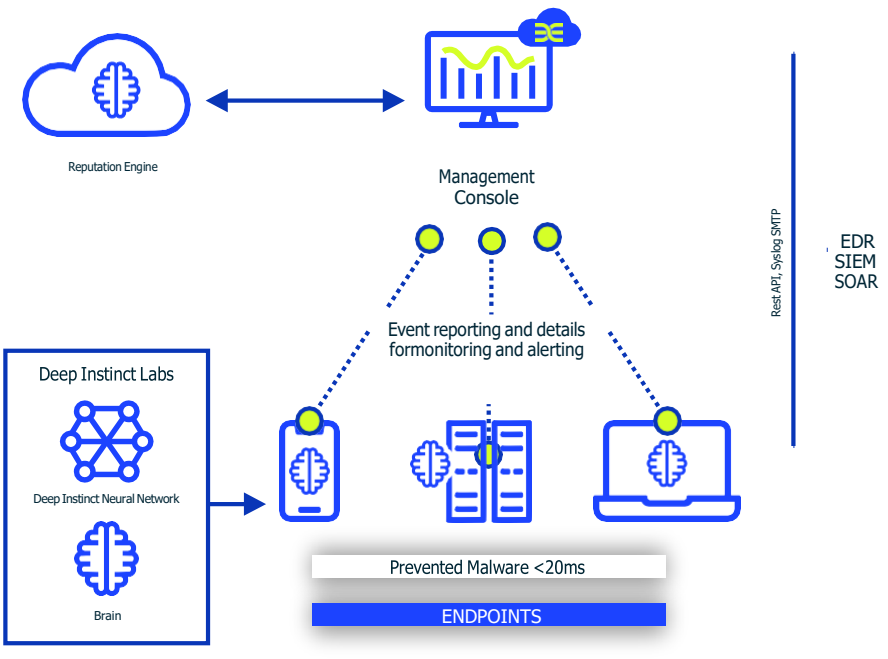
此外，Deep Instinct還提供上下文以理解威脅的嚴重性和策略：

- 對可疑事件發出警報以追蹤威脅
- 映射到MITRE ATT&CK以獲取威脅上下文
- 進行聲譽分析

執行後：自動分析

Deep Instinct包括可選的自動分析和聲譽分析，可以覆蓋基於政策和導入的允許清單的決策。

產品架構



自動響應並與 SIEM、EDR、SOAR 整合

所有已阻止的事件都會被發送到Deep Instinct控制台，並且惡意軟體會立即被分類，以提供有關嘗試的攻擊上下文鏈接。組織可以進行手動或自動回應，進行以下操作：

- 隔離端點設備
- 隔離/刪除/還原
- 更新政策：允許和還原（Hash、簽章、資料夾、腳本、程序）
- 終止進程
- 清理登錄值以刪除持久性
- 將阻止的事件發送到沙箱以進行進一步分析

Deep Instinct透過REST API、Syslog和SMTP與您的SIEM、SOAR、EDR或其他現有的安全工具整合，以提升調查、修復和威脅搜尋效能。

附加功能

Deep Instinct將領先的網路預防能力與直觀的功能集結合在一起，幫助我們的客戶節省時間，更智能地工作。

專業的UI和控制台
易於瀏覽且高度直觀的管理控制台可以進行自訂，以向用戶呈現最重要的內容。

內建報告功能
自動和臨時威脅和趨勢報告。

真正的多租戶架構
針對合作夥伴、MSP和MSSP的原生多租戶解決方案，將所有數據可以保護和隔離，避免交叉污染，並從一個集中的控制台管理多個環境。

增強安全性
對所有管理操作進行完整的稽核/紀錄，基於角色的訪問控制，使用雙因素認證（2FA）和SAML整合。

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

支援虛擬環境

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

支援系統

- Windows
- macOs
- Android
- Chrome OS
- Linux

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments.