型錄

趨勢科技

APT 威脅偵測與回應組合包

Deep Discovery Inspector

偵測整體網路上的針對性攻擊、進階威脅以及勒索病毒

針對性攻擊與進階威脅是專門為了躲避傳統資安防禦而設計的惡意攻擊，因此能躲藏在企業內部暗中竊取企業資料、智慧財產以及通訊內容，或者將關鍵資料加密以勒索贖金。根據資安專家與分析師指出，企業必須在整體資安防護策略當中採用一些進階偵測技術，才能有效偵測針對性攻擊與進階威脅。

Deep Discovery Inspector 是一套網路裝置，可 360 度監控您的網路來完整掌握針對性攻擊、進階威脅以及勒索病毒的所有攻擊層面。Deep Discovery Inspector 採用特殊的引擎與客製化沙盒模擬分析來發掘進階與未知惡意程式、勒索軟體、零時差漏洞攻擊、幕後操縱 (C&C) 通訊，以及傳統資安防禦無法察覺的暗中活動。藉由監控所有實體、虛擬、橫向及縱向網路流量來提升偵測能力。此能力讓趨勢科技連續三年榮獲 NSS Labs 評選為「最有效且推薦的入侵偵測系統」(Most Effective Recommended Breach Detection System)。

主要功能

檢查所有網路內容。Deep Discovery Inspector 可監控所有流量，包括實體與虛擬網段、所有網路連接埠以及 100 多種網路通訊協定的應用來發掘針對性攻擊、進階威脅以 及勒索軟體。我們的網路流量分析方法讓 Deep Discovery 能夠從內送與外送流量當 中偵測針對性攻擊、進階威脅及勒索軟體，並且偵測橫向移動(內網擴散)、C&C 以及攻擊行動所有階段的其他駭客行為。

完整豐富的偵測技巧，利用檔案、網站、IP 位址、行動應用程式等信譽評等，再配合經驗式分析、進階威脅掃瞄、客製化沙盒模擬分析，以及交叉關聯威脅情報，來偵測 勒索軟體、零時差漏洞攻擊、進階惡意程式和駭客行為。

客製化沙盒模擬分析採用完全符合企業電腦系統組態、驅動程式、應用程式及語言版本的虛擬映像模擬。可提高進階威脅與勒索軟體的偵測率，因為這些威脅通常能 躲避一般採用標準虛擬映像模擬的偵測方法。

完整的威脅情報，結合本地端網路分析資訊與趨勢科技 Smart Protection Network™ 的全球威脅分析情報，隨時提供立即的資料防護，不論資料所在位置為何。

更快、更高的投資報酬，藉由彈性的架構，可視網路流量而採用單一硬體裝置或 多重裝置的部署方式。藉由威脅情報共享來強化目前已投資的 NGFW/IPS、SIEM 以及閘道。

發掘網路上任何位置的勒索軟體。Deep Discovery Inspector 可偵測勒索軟體常用的腳本模擬、零時差漏洞攻擊，針對性攻擊檔案與密碼保護的惡意檔案。此外還會利用已知威脅的相關資訊，藉由病毒碼和信譽評等分析來發掘勒索軟體。客製化沙盒模擬分析可偵測修改、加密大量檔案以及修改備份檔案的行為。

主要效益

更好的偵測能力

- 多重偵測技巧
- 監控所有網路流量
- 客製化沙盒模擬分析
- 完整的威脅情報

具體明確的投資報酬 (ROI)

- 研究顯示 10 個月內實現 145% 投資報酬率 [1]
- 強化現有投資
- 彈性部署選項
- 手動作業自動化

[1] ESG 經濟價值驗證 (Economic Value Validation)：2015 年 10 月

NSS LABS RECOMMENDED
RECOMMENDED
Breach Detection System
3 YEARS IN A ROW
99.8% Detection Rate

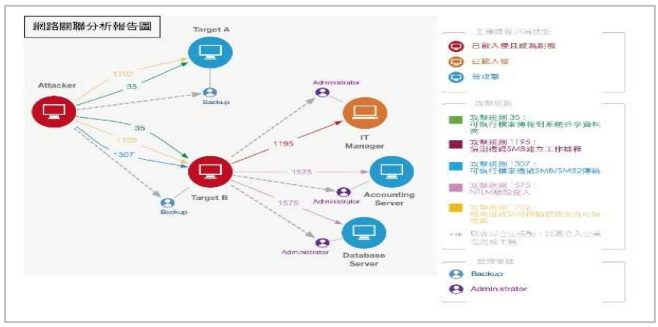
ICSA labs CERTIFIED

APT 威脅專家分析平台

魔鬼藏在細節裡，「駭客內網行為分析服務」利用大數據學習系統，再結合受過 APT 反匿蹤訓練的技術顧問，為企業在看似正常的系統紀錄中發現不尋常，在繁雜的網路活動紀錄中抽絲剝繭，早期發掘攻擊徵兆，成功擊退入侵者。

主要功能

- 偵測紀錄收集：利用大數據技術收集 DDI 所有的偵測紀錄。
- 威脅情資比對：藉由共享威脅情報和提供即時防護更新來快速回應威脅。
- 專家規則關聯分析： 透過 APT 進階規則進行交叉關聯分析，找出隱藏在中、低風險的真正事件。
- **掌握及監控**：集中掌握所有網路和系統的狀況，並且分析和評估威脅的衝擊。



採用 XGen™ 防護為基礎的 Deep Discovery Inspector 是趨勢科技 Network Defense 網路防禦解決方案的一環。

可偵測及防範以下威脅

- 針對性攻擊和進階威脅
- 針對性和已知勒索軟體攻擊
- 零時差惡意程式與文件漏洞攻擊
- 駭客行為與其他網路活動
- 網站威脅，包括漏洞攻擊和網頁掛馬式攻擊 (drive-by download)
- 網路釣魚、魚叉式網路釣魚以 及其他電子郵件威脅
- 資料外傳
- 殭屍病毒、木馬程式、蠕蟲、鍵盤側錄程式
- 破壞性應用程式

組合包內容介紹

趨勢科技提供方案 A 及方案 B 兩種組合包，方便已經採購 DDI 或未採購 DDI 的客戶選擇

A 方案	**DDI 1000 新購一年**	**APT 威脅專家分析平台一年**
B 方案	**DDI 1000 續約一年**	**APT 威脅專家分析平台一年**

TREND MICRO™
Securing Your Journey to the Cloud