

趨勢科技

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、進階威脅掃描、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

更好的防護

- 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



與趨勢科技產品環環相扣的威脅防禦重要環節之一

為了有效因應當前的威脅情勢，您需要多層式的防護平台來涵蓋威脅防禦的所有階段。趨勢科技 Connected Threat Defense 環環相扣的威脅防禦是一套多層式資安防護，為企業提供更好的方法來快速防範、偵測及回應專門針對您而設計的最新威脅，並且提升整體網路的掌握及監控。

- 防範：評估潛在漏洞，主動保護端點、伺服器與應用程式。
- 偵測：偵測一般標準防禦所無法偵測的進階惡意程式、行為及通訊。
- 回應：藉由共享威脅情報和提供即時防護更新來快速回應威脅。
- 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。

DEEP DISCOVERY INSPECTOR 硬體裝置規格

	500/1000 型	4000 型
硬體型號	510/1100	4100
支援的沙盒環境數量	2 (500 型), 4 (1000 型)	20
機身規格	1U 機架式, 48.26 公分 (19 英吋)	2U 機架式, 48.26 公分 (19 英吋)
重量	19.9 公斤 (43.87 英磅)	31.5 公斤 (69.45 英磅)
尺寸 (寬x深x高)	43.4 公分 (17.09 英吋) x 64.2 公分 (25.28 英吋) x 4.28 (1.69 英吋) 公分	48.2 公分 (18.98 英吋) x 75.58 公分 (29.75 英吋) x 8.73 公分 (3.44 英吋)
管理連接埠	10/100/1000 BASE-T RJ45 x 1 iDrac Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 x 1 iDrac Enterprise RD45 x 1
資料連接埠	10/100/1000 BASE-T RJ45 x 5	10Gb SFP+ (SX 收發器) x 4 10/100/1000 Base-T RJ45 x 5
交流電輸入電壓	100 至 240 VAC	100 至 240 VAC
交流電輸入電流	7.4A 至 3.7A	10A 至 5A
硬碟	2 x 1 TB 3.5吋 SATA	4 x 1TB 3.5吋 NLSAS
RAID 組態	RAID 1	RAID 1+0
電源供應器	550W Redundant	750W Redundant
電力消耗 (最大)	604W	847W (最大)
發熱量	2133 BTU/hr (最大)	2891 BTU/hr (最大)
頻率	50/60 Hz	50/60 Hz
作業溫度	10-35 °C (50-95 °F)	10-35 °C (50-95 °F)

Deep Discovery Inspector 虛擬裝置可提供/500/1000/4000 Mbps 的吞吐量，支援 VMware vSphere 5 或更新版本以及 KVM。

其他 DEEP DISCOVERY 產品

Deep Discovery Inspector 能在您企業最重要的環節上提供進階威脅防護，包括：網路、電子郵件、端點，或是現有的資安解決方案。

- **Deep Discovery Analyzer** 可提供進階沙盒模擬分析，進一步強化資安產品的價值，例如：端點防護、網站與電子郵件開道防護、網路防護以及其他 Deep Discovery 產品。Deep Discovery Analyzer 可偵測惡意程式或網址所引來的勒索軟體、進階惡意程式、零時差漏洞攻擊、C&C 通訊，以及多重階段下載，保護 Windows 和 Mac 作業系統。
- **Deep Discovery Email Inspector** 提供進階惡意程式偵測，包括電子郵件沙盒模擬分析。Email Inspector 可設定攔截經由電子郵件散布的進階惡意程式。

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



Securing Your Journey to the Cloud

©2017 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、t 形標誌、Smart Protection Network 與 Deep Discovery 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。
(DS06_DD_Inspector_1701161TW)