趨勢科技

Deep Discovery™ Analyzer

專為防範針對性攻擊的進階防護

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，因此能夠躲藏在您的企業內部暗中竊取您的敏感資料，或者將您的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，防範今日擅長躲避的威脅。

Deep Discovery Analyzer 能強化企業現有投資的趨勢科技或第三方資安防護 (經由網站服務 API)，提供客製化沙盒模擬分析與進階分析能力。此外還能為其他趨勢科技產品提供進階的沙盒模擬分析能力。將可疑的物件傳送至 Analyzer，然後運用多重偵測技巧執行進階沙盒模擬分析。若發現威脅，可自動更新資安解決方案。

主要功能

客製化沙盒模擬分析：採用完全符合您電腦系統組態、驅動程式、應用程式及語言版本的虛擬映像。如此可提高進階威脅的偵測率，因為這些威脅通常能躲避一般採用標準虛擬映像的偵測方法。客製化沙盒模擬分析環境內含安全的外部存取，可偵測並分析多重階段下載、網址、幕後操縱 (C&C) 通訊等等，並且支援手動或自動將檔案與網址送交分析。

彈性的部署：Analyzer 可部署成獨立的沙盒模擬環境，或者搭配 Deep Discovery 一同部署以增加額外的沙盒模擬環境數量。單一裝置最多可擴充至 60 個沙盒模擬環境，甚至可叢集多台裝置來提供高可用性或者建立熱備用或冷備用組態。

進階偵測方法：靜態分析、經驗式分析、行為分析、網站信譽評等、檔案信譽評等，可確保迅速偵測威脅。此外，Analyzer 還可偵測多重階段的惡意檔案、對外連線，以及來自可疑檔案的持續性 C&C 通訊。

- **廣泛的檔案分析：**藉由多重偵測引擎與沙盒模擬分析來檢查各式各樣的 Windows 執行檔、Microsoft® Office 文件、PDF 檔案、網站內容，以及壓縮檔案。可根據檔案類型來自訂政策。
- **文件漏洞攻擊偵測：**採用特殊的引擎與沙盒模擬分析來發掘常用文件格式可能挾帶的惡意檔案和漏洞攻擊。
- **網址分析：**針對電子郵件當中的網址或手動送交分析的樣本進行沙盒模擬分析。
- **網站服務 API 和手動送交分析：**讓任何產品或惡意程式分析師送交可疑的樣本進行分析。自動將新的入侵指標 (IOC) 偵測情報分享給趨勢科技或第三方廠商的產品。
- **支援** Windows、Mac 和 Android 作業系統。

偵測勒索病毒：偵測勒索病毒常用的腳本模擬、零時差漏洞攻擊，以及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病毒。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

- 提供比一般通用虛擬環境更優異的偵測能力。
- 更好的躲避技巧防範能力

具體明確的投資報酬 (ROI)

- 藉由整合與威脅情報共享，並且為高流量環境提供額外運算容量，強化現有投資。
- 消除耗時的可疑檔案手動分析工作。
- 避免為了挽救勒索病毒感染所付出的昂貴代價。
- 彈性的部署選項，可採集中化或分散式分析。

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery

100%

Breach Detection Rate

- 2017 -

RECOMMENDED 4 years in a row

ICSA labs CERTIFIED

趨勢科技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，您需要一套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新的網路資安防護架構，為企業提供更好的方法來快速防範、偵測及回應專門針對企業而設計的最新威脅，同時提升您對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：**透過 YARA 和 STIX 來和趨勢科技防護層以及第三方資安產品共享威脅情報並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。

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

Deep Discovery Analyzer 裝置規格

	硬體型號 1100
處理容量	每日 45,000 個樣本
支援的檔案類型	cell、chm、class、dll、doc、docx、exe、gul、hwp、hwpx、jar、js、jse、jtd、lnk、mov、pdf、ppt、pptx、ps1、rtf、swf、vbs、vbe、xls、xlsx、xml
支援的作業系統	Windows XP、7、8/8.1、10、Windows Server 2003、2008、2012、Mac OS
機身規格	2U 機架式，48.26 公分 (19 英吋)
重量	32.5 公斤 (71.65 英磅)
尺寸	寬度 48.2 (18.98) x 深 75.58 (29.75) x 高 8.73 公分 (3.44 英吋)
管理連接埠	10/100/1000 Base-T RJ45 x 1
資料連接埠	10/100/1000 Base-T RJ45 x 3
交流電輸入電壓	100 至 240 VAC
交流電輸入電流	10A 至 5A
硬碟	2 x 4 TB 3.5 吋 SATA
RAID 組態	RAID 1
電源供應器	750W 備援
電力消耗 (最大)	847W (最大)
發熱量	2891 BTU/hr (最大)
頻率	50/60HZ
作業溫度	50-95 °F (10-35 °C)
硬體保固	3 年

其他 Deep Discovery 產品

Deep Discovery Analyzer 是 Deep Discovery 平台的一環，此平台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 Inspector** 是一套虛擬裝置或硬體裝置，能 360 度全方位偵測網路上的針對性攻擊和進階威脅。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、勒索病毒、零時差漏洞攻擊、幕後操縱 (C&C) 通訊、橫向移動，以及標準資安防禦無法察覺的駭客暗中活動。
- **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，不讓它有機會散布。

TREND MICRO™

Securing Your Journey to the Cloud