趨勢科技

Deep Discovery Inspector 網路惡意行為偵測系統

全網路的鎖定目標攻擊偵測

鎖定目標攻擊與進階威脅都是專為滲透您獨特的 IT 基礎架構而客製化，不僅能躲過傳統的防禦，而且能持續躲藏在您的企業內竊取資料。為了偵測這類駭客入侵，分析師和資訊安全專家皆認為企業應部署一套進階威脅防護來提升安全監控策略。

趨勢科技 Deep Discovery Inspector 是一套進階威脅防護系統，可提供全網路的掌握與 報來偵測並回應鎖定目標攻擊與進階威脅。Inspector 能監控所有連接埠及 80 多種通訊協定的應用，幾乎所有網路流量都能分析，為您提供市面上最全面的防護。其特殊的偵測引擎與客製化沙盒模擬分析，能發掘並分析惡意程式、C&C 通訊以及一般標準防護無法偵測到的隱匿攻擊活動。其深入的情報能協助 您快速回應，並自動與其他防護產品分享情報，建立一個即時的客製化防禦系統 來防範駭客攻擊。

主要功能

完整的威脅偵測

監控所有連接埠及 80 多種通訊協定的應用，發掘您網路的攻擊。

惡意程式、C&C 通訊、駭客活動 採用特殊偵測引擎、交叉關聯分析以及客製化沙盒模擬分析來偵測鎖定目標攻擊的所有面向，不光只是針對惡意程式。

客製化沙盒模擬分析 可制定與您系統組態一致的沙盒模擬分 析，來偵測專門針對您企業的威脅。

Smart Protection Network 情報

提供您全球威脅情報，以及 Threat Connect 來協助您調查攻擊來源。

廣泛保護各種系統

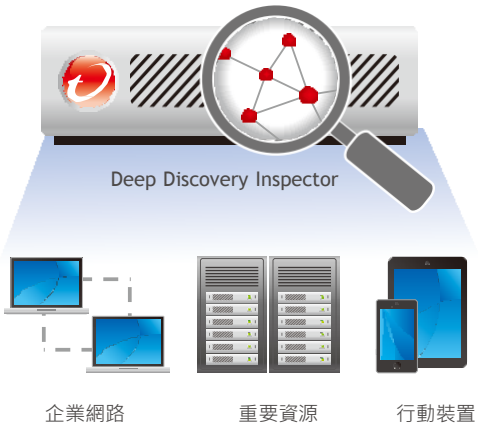
能偵測針對 Windows、Mac OS X、Android、 Linux 及任何系統的攻擊。

單一裝置的簡易與彈性

單一裝置提供多種容量的選擇。

Custom Defense 客製化防禦解決方案

分享入侵指標 (Indicators of Compromise， 簡稱 IOC) 情報，自動將最新情報提供給趨勢科技產品和其他防護產品，防止您遭到進一 步攻擊。



主要效益

鎖定目標攻擊防護 發掘傳統防護產品所無法偵測的威 脅。

360 度的資訊掌握與偵測 全方位監控所有網路流量來偵測攻 擊跡象，呈現您真正的安全情勢。

快速分析和回應 完整剖析威脅與風險因子的特性， 加快回應速度。

更低的整體持有成本 採用單一裝置來簡化防護與管理， 進而降低整體持有成本 (TCO)。

客製化防禦的基石 與其他防護解決方案分享入侵指標 (IOC) 情報，建立一套整合且即時的 客製化防禦來防範鎖定目標攻擊。

偵測及防範

- 鎖定目標攻擊與進階威脅
- 零時差 (zero-day) 惡意程式與文件 漏洞攻擊
- 駭客網路活動
- 網站威脅，包含漏洞攻擊與 drive-by-download(偷渡式下載)
- 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
- 殭屍程式、木馬程式、蠕蟲、鍵盤側 錄程式
- 影響營運的應用程式

Deep Discovery Inspector 可提供網路流量檢查、進階威脅偵測以及即時分析: 全都專為偵測鎖定目標式攻擊而打造。它採用一種三層式的偵測方法，第一層是初步偵測，第二層是沙盒模擬分析，第三層是事件關聯，目的就是為了發掘隱匿的攻擊活動。

其偵測與關聯分析引擎提供了最卓越的即時防護，還有趨勢科技 Smart Protection Network™ 的全球威脅情報以及專職的威脅研究人員為後盾。因此能達到高偵測率、低誤判率，還有深入的情報資訊來加快回應攻擊的速度。

Deep Discovery Inspector 如何運作

威脅偵測引擎 多種特殊的偵測引擎與事件關聯規 則，專門發掘惡意程式、C&C 通訊 以及攻擊活動，幾乎涵蓋所有的網 路流量，不單只有標準的 HTTP 和 SMTP。此外 Smart Protection Network 和專職的威脅研究人員會 不斷更新這些引擎和規則。

虛擬化分析單元 客製化沙盒模擬分析，採用符合您 系統組態的虛擬環境來進一步分 析可疑檔案和網站內容。客製化 沙盒模擬分析可準確偵測專門針 對企業設計的威脅，防止駭客的 躲避技巧，還可排除沒有影響的 惡意程式。

可擴充模組

進階攻擊防禦包
-郵件模組
-網頁模組
-沙盒模組

即時威脅主控台

Deep Discovery Inspector 主控台讓您即時隨手掌握威脅情報與深入分析能力。讓您透過程式來快速掌握關鍵資訊、追蹤威脅源頭、利用觀察名單來監控重要資源、還有 Threat Connect 威脅情報入口網站查詢攻擊的特性。

觀察名單 在一個專門的檢視頁面中顯示高危險性 威脅與高價值資產的風險監控。可以針 對指定的系統特別追蹤是否有可疑的活 動和事件，以進一步詳細 分析。

Threat Connect

Threat Connect 是一個獨特的資訊入口網站， 藉由趨勢科技 Smart Protection Network 的全球情報，為您所遭遇的攻擊提供完整詳盡的相關資訊，包括：風險評估、惡意程式特性、源頭位置、變種、相關 C&C 伺服器 IP 位址、駭客背景資料，以及建議的矯正措施。

集中管理與 SIEM

Deep Discovery Inspector 有自己的管 理主控台，也可透過趨勢科技 Control Manager 來集中管理。此外，亦能與市 場主流的安全資訊與事件管理(SIEM)平 台密切整合，包括：HP ArcSight、IBM QRadar 及 Splunk。

入侵指標 (IOC) 資訊分享

Deep Discovery Inspector 能將沙盒模擬分析偵測的最新 IOC 資訊分享給其他 Deep Discovery、趨勢科技或第三方產品，建立一套即時的客製化防禦來防範駭客攻擊。

彈性、高容量的部署 提供滿足各種不同容量與部署需求的硬 體裝置，從 100 Mbps 到 4 Gbps 不 等。

Deep Discovery 如何偵測威脅

監控 80 多種通訊協定與應用程式，涵蓋所有的網路連接埠

	攻擊偵測	偵測方法
進階惡意程式	• 零時差 (Zero-day) 惡意程式及已知惡意程式 • 含有文件漏洞攻擊附件的電子郵件 • drive-by download (偷渡式下載)	• 解碼及解壓縮內嵌檔案 • 客製化沙盒模擬分析 • 瀏覽器漏洞攻擊套件偵測 • 惡意程式掃瞄 (特徵和經驗式)
C&C 通訊	• 惡意程式的 C&C 通訊：殭屍程式 (Bot)、檔案下載程式、資料竊取、蠕蟲、混合式威脅等等 • 駭客後門程式活動	• 目的地分析 (網址、IP、網域、電子郵件、IRC 通道...等等)，採用動態黑名單與白名單技術 • 利用 Smart Protection Network 信譽評等資料檢查所有欲連接的網址與內嵌 URL • 通訊特徵規則
駭客活動	• 駭客活動偵測：連接埠掃瞄、暴力破解、工具下載等等 • 資料外傳 • 惡意程式活動：散布、下載、散發垃圾郵件等等	• 規則導向的經驗式分析 • 更豐富的事件關聯分析與異常偵測技巧 • 行為特徵規則

為何客製化沙盒模擬分析有其必要

網路犯罪集團會針對您的特殊環境，包括桌上型和筆記型電腦作業系統、應用程式以及瀏覽器等等來開發出客製化的惡意程式。既然惡意程式是針對系統組態而開發，因此不太可能會在通用的沙盒環境當中啟動。結論是，在一個通用而非針對您 IT 環境的沙盒當中很可能無法偵測到客製化惡意程式。

唯有客製化的沙盒才能完全模擬真實環境，並且：

- 發掘專門針對您的企業環境，如 Windows 授權、語言、應用程式以及桌上型電腦組合等等條件的客製化惡意程式。
- 防止惡意程式使用一些根據通用 Windows 授權、少數標準應用程式版本以及英文等條件來判斷的沙盒躲避技巧。
- 忽略一些不會對環境造成影響的惡意程式，例如專門針對其他 Windows

擴大您的防護策略

Deep Discovery Inspector 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，或是整合式防護。可再配合 Deep Discovery Analyzer、Deep Discovery Endpoint Sensor 或趨勢科技 Control Manager 來擴充 Inspector 的功能，且將 Inspector 的 IOC 偵測情報與其他產品分享。

Deep Discovery Analyzer 是一套開放、可擴充的客製化沙盒分析伺服器。Analyzer 可擴充 Inspector 的沙盒容量與彈性，或者將多台 Inspector 裝置的沙盒模擬分析作業集中化。Analyzer 還可補強其他趨勢科技產品以及 第三方資安產品的防護能力。

Deep Discovery Endpoint Sensor 是一套具備環境感應能力的端點安全監控方案，可詳細記錄目標端點裝置的系統層次活動並產生報表。對於調查和修正 Deep Discovery Inspector 所 發現的鎖定目標攻擊尤其有用。

Endpoint Sensor 可利用所發現的 IOC 資料來搜尋並確認端點是否遭到滲透，並且發掘攻擊的完整環境資訊、時間表、路徑及範圍。

趨勢科技 Control Manager 能為多台 Deep Discovery Inspector 裝置提供集中化的檢視、威脅調查與報表，並且集中管理所有的 Deep Discovery 與趨勢科技產品。Control Manager 還可當成最新偵測情報 (如 C&C 伺服器位址、其它 IOC 資訊等等) 的發送站，讓所有 Deep Discovery 裝置以及趨勢科技和第三方產品分享最新情報。

趨勢科技 Custom Defense 客製化防禦

Deep Discovery 平台是趨勢科技 Custom Defense 客製化防禦的基礎，讓您快速偵測、分析及回應駭客攻擊。Deep Discovery 的偵測 與 IOC 情報能與各種趨勢科技產品及第三方產品整合，將您的防護基礎架構建構成一套專為您企業量身訂做的即時防禦，對抗鎖定目標式攻擊。