

Trend Micro™ Deep Discovery™ 系列

防範針對性攻擊的進階威脅防護

簡介

針對性攻擊與進階威脅是專為躲避您的傳統資安防禦而精心設計。它們能持續躲藏在企業內部竊取您的企業資料、智慧財產、通訊記錄，或者將重要資料加密來向您勒索贖金。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。

Trend Micro™ Deep Discovery™ 包含了一系列的進階威脅防護產品，能讓您偵測、分析、回應今日隱匿的針對性攻擊。Deep Discovery 融合了特化的偵測引擎、客製化沙盒模擬分析以及趨勢科技 Smart Protection Network™ 的全球威脅情報，在面對傳統標準資安產品所看不見的攻擊時，能提供最高的偵測率。Deep Discovery 不論是獨立部署或內含在整合式方案當中，都能與趨勢科技及第三方解決方案共同運作，為您的整體企業提供進階威脅防護。



主要效益

讓您企業防範攻擊

提供獨特的威脅偵測技巧，讓您在損害造成之前預先發現攻擊。

為您資安團隊提供快速回應所需的情報

有了 Deep Discovery 再加上全球威脅情報，您就能迅速、有效回應您整個企業的威脅。

與您的防禦整合

Deep Discovery 能與您的趨勢科技或第三方資安工具整合，協助您有效防範針對性攻擊。

讓您防範整合式威脅

融合跨世代威脅偵測技巧，讓您在適當時機套用適當的技術。

與 Trend Micro™ TippingPoint™ 入侵防護系統 (IPS) 彼此配合，提供整合式偵測及防護，防範已知、未知及未公開的威脅。





Trend Micro™ Deep Discovery™ Inspector 是一個網路裝置，可監控所有連接埠與 100 多種通訊協定和應用程式的網路流量。採用特化的偵測引擎與客製化沙盒模擬分析來發掘您整個環境當中的惡意程式、幕後操縱 (C&C) 通訊，以及有潛在網路攻擊徵兆的活動。其偵測情報可協助您快速回應威脅，並自動將情報分享給其他資安產品以攔截未來的攻擊。



Trend Micro™ Deep Discovery™ Analyzer 是一套開放式客製化沙盒模擬分析伺服器，能提升您所有資安解決方案的惡意程式偵測能力。Deep Discovery Analyzer 可與多種趨勢科技解決方案開箱直接整合，支援手動送交樣本進行分析，並提供一個開放式網頁服務 (Web Service) 介面，讓任何解決方案或流程都能送交樣本以取得分析結果。此外，亦可為其他 Deep Discovery 產品提供額外的沙盒模擬分析能力，提升您資安解決方案的價值。



Trend Micro™ Deep Discovery™ Director 是一套企業內資安協調整合工具，可集中部署解決方案及沙盒模擬環境的更新，除了提供一個企業內部署架構之外，更提供聰明的威脅調查功能。這套虛擬裝置還可擔任您的進階威脅情報集散中心。您可透過產業標準的格式 (STIX 與 YARA) 與傳輸架構 (TAXII)，從眾多來源接收威脅情報，並與趨勢科技及第三方產品分享入侵指標 (IoC) 資訊。



Trend Micro™ XDR for Networks 能提供經過優先次序過濾的攻擊可視性。利用 Deep Discovery Inspector 的偵測來源與網路 Metadata 蒐集來源，藉由專家規則來交叉分析及串聯威脅偵測事件與網路存取事件之間的關係，讓威脅調查人員完整掌握攻擊的生命週期。



Trend Micro™ Deep Discovery™ Analyzer as a Service 是專為 Deep Discovery Inspector 虛擬裝置與 Trend Micro Apex One™ as a Service 設計的一項附加服務，提供進階雲端沙盒模擬分析功能。讓您的資安團隊為需要虛擬化或雲端式沙盒模擬分析功能的環境提供進階威脅與針對性攻擊防護。

託管式偵測及回應

採用 Trend Micro™ Managed XDR 服務，讓趨勢科技的資安專家和領先業界的人工智慧技術協助您監控並判斷威脅的優先次序。趨勢科技分析師將 7 天 24 小時全天候監控、調查並回應 Deep Discovery Inspector 所發現的進階威脅。Managed XDR 並不只侷限於網路層，更延伸至您的電子郵件、端點、伺服器及雲端工作負載，藉由監控並交叉關聯更多威脅管道的資料來提供您更廣泛的情境資訊，進而實現更好的偵測能力。



功能

網路內容檢查：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，協助您的資安團隊發掘針對性攻擊、進階威脅以及勒索病毒。我們的網路流量分析方法讓 Deep Discovery 能夠從您環境的內送與外送流量當中偵測針對性攻擊、進階威脅及勒索病毒，並且偵測橫向擴散、C&C 通訊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 位址與行動應用程式信譽評等，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，來偵測勒索病毒、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：採用完全符合您企業電腦系統組態、驅動程式、已安裝應用程式及語言版本的虛擬映像。如此可提高進階威脅及勒索病毒的偵測率，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。

彈性部署：Deep Discovery Analyzer 可部署成獨立的沙盒模擬環境，或者搭配 Deep Discovery Inspector 一同部署以增加額外的沙盒模擬環境數量。它可經由擴充，在單一裝置內支援高達 60 個沙盒模擬環境。此外還可叢集多個裝置來提供高可用性或設定成熟備用或冷備用組態。

滿足部署目標和需求：Deep Discovery Inspector 提供了硬體裝置與虛擬裝置兩種選擇。

延伸式偵測及回應 (XDR)。XDR for Networks/Trend Micro™ Deep Discovery™ Network Analytics 採用軟體服務 (SaaS) 解決方案的方式來提供完整的延伸式偵測及回應 (XDR) 功能。企業內安裝環境則可透過虛擬伺服器或實體裝置來獲得這套解決方案的效益。

進階偵測：提供多種方法，例如：靜態分析、經驗式分析、行為分析、網站信譽評等以及檔案信譽評等，來協助您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。

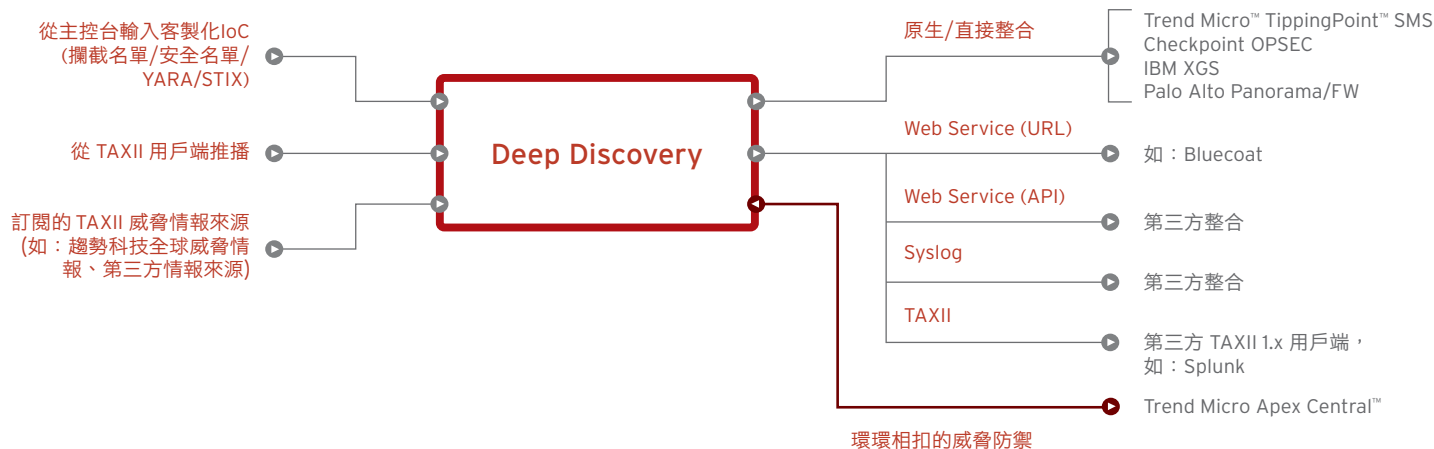
威脅情報：Deep Discovery 會交叉分析進階威脅情報並透過產業標準格式及傳輸架構 (如 STIX/TAXII 和 YARA) 分享這些情報。如此可讓企業隨時掌握可能入侵企業網路的最新未知威脅。

威脅數據分析：提供更深入的攻擊資訊，讓您判斷威脅優先次序，並發掘威脅如何入侵網路、入侵之後向何處擴散、還有哪些使用者也受到攻擊影響。透過回放來逐步查看整起攻擊的過程。我們的 15 個全球研究中心、450 名內部研究人員，以及參與我們 Zero Day Initiative™ 漏洞懸賞計畫的 1 萬多名外部資安研究人員，隨時都在鑽研全球的整體威脅情勢。

整合：Deep Discovery 是專為搭配其他趨勢科技解決方案及第三方產品一起運作而設計。Deep Discovery 提供原生整合功能以及豐富的 API，讓您將資安回應、入侵指標 (IoC) 分享以及進階威脅與針對性攻擊防範自動化。

成為資安營運中心 (SOC) 的支柱

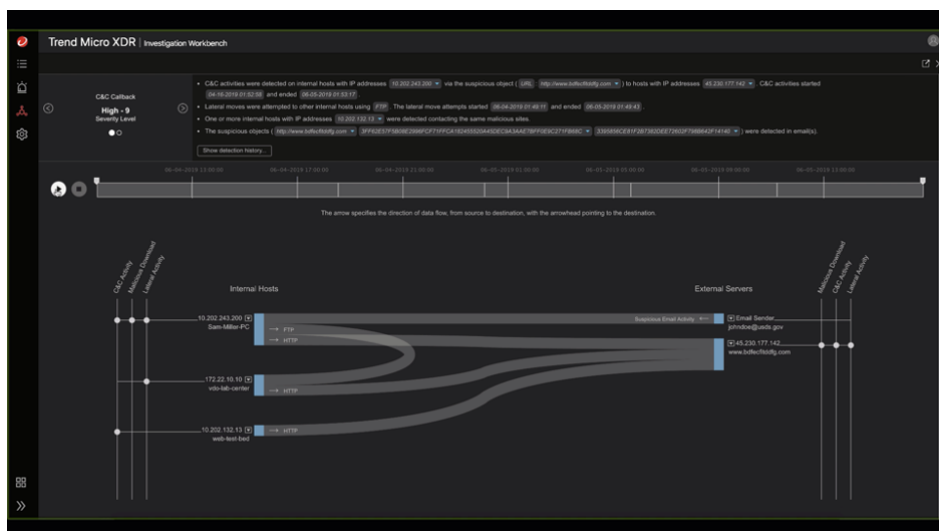
身為資安人員，您需要完全掌握威脅情勢，包括何時有威脅正在爆發以及如何加以阻止。為了協助您的資安營運中心 (SOC) 以及其他資安人員隨時掌握最新威脅，Deep Discovery 會隨時經由產業標準的格式和傳輸架構 (STIX/TAXII 及 YARA) 從各種威脅情報來源以及客製化輸入汲取最新的進階威脅情報，也就是入侵指標 (IoC)。這些 IoC 會分享給網路內的趨勢科技及第三方解決方案，讓您加快偵測進階威脅的速度。這些環環相扣的產品能讓您的團隊偵測及攔截原本未知的威脅。



Deep Discovery Analyzer 通常只是純粹提供一個沙盒模擬分析環境，可自動接收來自其他資安產品的 IoC，然後觸發並且分析威脅的行為，同時自動傳回分析結果，以便採取進一步行動。您的資安分析師或威脅追蹤人員也可以手動送交潛在威脅來加以分析。如此可簡化分析程序，針對潛在的威脅或可疑的物件，為分析師提供確切的答案。

簡化優先次序的判斷

資安產品擅長偵測、警示及攔截嘗試攻擊企業的威脅。但缺點是會產生大量的資料，有些相關、有些則不然。所以，您企業的資安人員必須每天過濾數以千計的潛在警報通知與事件記錄，來判斷是否為威脅，或者是否需要進一步處理。



XDR for Networks 可提供以下攻擊相關資訊來簡化優先次序的判斷：

攻擊的第一個入侵點在哪裡？

還有哪些內部員工受到影響？

威脅對外連線的位址為何？

(C&C 通訊)

易讀易懂的 Sankey 圖 (如附圖)，可讓您清楚看到攻擊的每一步驟，最遠可追溯至 6 個月前。XDR for Networks 能提供您即時的可視性，從網路流量資料當中持續擷取 Metadata 並且在一個圖形中顯示事件的交互關聯。如此一來，您只需更少的人力就能更快解決問題，並且更完整掌握攻擊的樣貌。有些時候，您或許以為攻擊是今天才發生，但事實上，早在數星期前您就已經遭到駭客入侵。XDR for Networks 讓您更了解該如何防範未來的攻擊。

Trend Vision One™ 的重要一環

Trend Micro™ XDR 打破了您企業電子郵件、端點、伺服器、雲端工作負載以及網路之間的藩籬。藉由涵蓋範圍更廣的可視性與專家資安數據分析，提供量少質精的警報與準度更高的偵測能力，進而更早、更快回應威脅。

更有效、且更有效率地偵測及回應威脅，減輕攻擊對企業的嚴重性並縮小其範圍。Deep Discovery Inspector 與 XDR for Networks 都是趨勢科技 Trend Vision One 平台的重要一環，能為不受管理的系統，如：外包商/第三方系統、物聯網 (IoT) 與工業物聯網 (IIoT) 裝置、印表機、個人自備裝置 (BYOD) 提供關鍵的記錄檔及可視性。

©2023 年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro、Deep Discovery、Smart Protection Network、TippinPoint、Trend Micro Apex One、Trend Vision One、Trend Micro Apex Central 以及 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。[SB05_DD_Family_Solution_Brief_230719TW]

如需有關我們蒐集哪些個人資料的詳細內容和理由，請參閱我們的網站上的「隱私權聲明」，trendmicro.com/privacy