趨勢科技

Deep Discovery Email Inspector 1000

社交工程郵件防禦系統

防範可能導致資料外洩的鎖定目標電子郵件攻擊

鎖定目標攻擊和進階威脅已證實有能力躲過傳統的安全防禦，並且將敏感資料與智慧財產傳送至企業外部。根據趨勢科技的研究顯示，這類攻擊有 90% 以上都始於內含惡意附件檔案或 URL 網址的魚叉式網路釣魚郵件，一般標準的電子郵件或端點防護無法偵測這類郵件。

Deep Discovery Email Inspector 是專為偵測及攔截可能造成資料外洩的鎖定目標攻擊郵件而打造。它結合了先進的惡意程式偵測引擎、URL 分析，還有檔案及網站沙盒模擬分析，可發掘並立即攔截或隔離這類電子郵件。

主要效益

鎖定目標電子郵件防護 攔截絕大多數鎖定目標攻擊背後的 惡意電子郵件。

客製化沙盒模擬分析偵測 發掘傳統標準電子郵件防護無法發現 的威脅。

通透性與相容性 與現有的電子郵件防護解決方案獨立運 作，互不干擾。

主要功能

電子郵件附件分析 採用多重偵測引擎與客製化沙盒模擬分析技術 來檢查所有附件，包括：各類 Windows 執行 檔、 Microsoft Office 檔案、PDF、Zip、網站 內容以及壓縮檔案。

文件漏洞偵測 專門的偵測與沙盒模擬分析技術，可發掘惡 意程式及針對一般 Office 文件漏洞的攻擊。

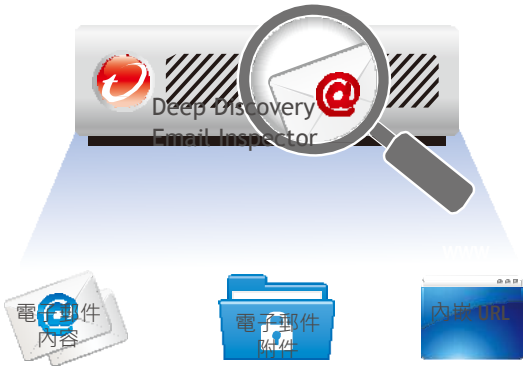
客製化沙盒分析 採用與您桌面軟體組態完全一致的沙盒模擬與 分析。

內嵌 URL分析 利用信譽評等、內容分析與沙盒模擬分析來發 掘魚叉式網路釣魚郵件內嵌的惡意 URL。

密碼情報 透過多道經驗式偵測與客戶提供的關鍵字 來解開密碼保護的檔案和 Zip 檔案。

管理與部署彈性

兩種部署模式：MTA (封鎖) 或 BCC (監控)，可搭配任何電子郵件防護解決方案。透過精細的控管輕鬆實現客製化的防護政策。



Deep Discovery Email Inspector 如何運作

URL 分析及客製化沙盒模擬
內嵌的 URL 會經過信譽檢查，必要時目標內容還會經過掃瞄與沙盒模擬，以發掘重新導向、進階惡意程式以及順道下載的漏洞攻擊。

附件分析與客製化沙盒模擬 附件會使用經驗式技巧與客戶提供的關鍵字來 展開、解壓縮與解鎖。

多重偵測引擎與客製化沙盒模擬，可偵測進階惡意程式與文件漏洞攻擊，涵蓋各種檔案類型與內容，包括：Windows 執行檔、Microsoft Office 檔案、PDF、Zip 以及 Java。

政策控管與執行
您可根據警示的嚴重程度設定各種惡意電子郵件處理方式，包括：隔離、刪除、加上標籤並轉寄等等。電子郵件沙盒模擬分析可依附件類型而自訂調整 (如：針對所有 PDF 檔執行沙盒模擬)。

威脅分析 詳細的沙盒模擬分析還可提供進一步威脅研究 之用。另外，Threat Connect 威脅情報入口網 站也能提供相關的趨勢科技全球情報來評估攻 擊的風險和來源。

規格

Deep Discovery Email Inspector1000 型	
部署方式	MTA (封鎖) 及 BCC (監控) 兩種模式
處理容量	每日 400,000 封郵件

Deep Discovery 平台

Deep Discovery Email Inspector 是 Deep Discovery 系列環環相扣的多項產品之 一，該系列提供網路、電子郵件、端點 裝置與整合式防護，讓您在企業最關鍵 的位置部署進階威脅防護。

客製化防禦

Deep Discovery 平台是趨勢科技客製化防 禦的核心，將您的防護基礎架構建構成一套專為您企業量身訂做的完整防禦，對抗鎖定目標攻擊。

Deep Discovery 的客製化偵測、情報與控管可讓您：

- 偵測及分析攻擊者。
- 立即調整防護來應付攻擊。
- 快速因應以防止資料外洩。

TREND MICRO™

Securing Your Journey to the Cloud