趨勢科技

DEEP DISCOVERY™ EMAIL INSPECTOR

防範可能導致資料外洩或勒索病毒感染的針對性攻擊電子郵件

針對性攻擊與進階威脅已證明能夠躲避傳統資安防禦、竊取敏感資料，或者將關鍵資料加密以便勒索贖金。根據趨勢科技研究顯示，這類攻擊90%以上一開始都是利用內含惡意附件檔案或惡意連結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 採用先進的偵測技巧來偵測並攔截魚叉式網路釣魚郵件，而這些郵件經常是員工不小心遭到進階惡意程式與勒索病毒感染的途徑。Email Inspector 能搭配您現有的電子郵件閘道運作，可偵測及防範針對性攻擊精心特製的魚叉式網路釣魚郵件內隨附的惡意附件和網址，以及進階威脅和勒索病毒。Deep Discovery Email Inspector 可部署成 MTA (攔截)、BCC (監控) 或 SPAN/TAP 三種模式。

主要功能

通透式
能完美搭配現有的垃圾郵件過濾或電子郵件安全閘道來偵測魚叉式網路釣魚郵件攻擊，這類郵件通常使用惡意附件和網址來暗藏進階惡意程式，包括勒索軟體 (通常暗藏在巨集中)。

豐富完整的偵測技巧
偵測零時差漏洞攻擊、進階威脅、勒索軟體以及駭客行為。它採用檔案、IP 位址與網站信譽評等，再搭配靜態分析、經驗式分析、演算法以及沙盒模擬分析來偵測已知及未知的威脅。除此之外，也可結合本地端威脅情報與趨勢科技的分析資訊進行交叉關聯。

彈性
提供多種部署方式：in-line攔截/隔離、寫入記錄檔 (logging)、或者移除電子郵件中偵測到的威脅並通知使用者。

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、應用程式清單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「上線模式存取」(Live Mode Access) 可偵測並分析多重階段下載、網址、C&C 通訊等等。沙盒模擬分析提供硬體整合功能與可擴充獨立功能兩種型態。

防範勒索軟體攻擊
根據統計，從駭客的魚叉式網路釣魚攻擊發動開始，平均大約 1 分 40 秒就會有一個受害者開啟惡意電子郵件[1]。由於電子郵件是駭客散布勒索病毒的首要管道，因此，企業內的所有使用者都有危險。

主要效益

更好的防護

- 防範絕大多數針對性攻擊的第一階段：魚叉式網路釣魚郵件。
- 在損害造成之前預先偵測勒索軟體。
- 利用客製化沙盒模擬分析來發掘傳統電子郵件防護所無法察覺的威脅。

具體明確的投資報酬(ROI)指標

- 防範魚叉式網路釣魚和勒索病毒，省下大筆感染清除費用。
- 能完美配合現有電子郵件防護解決方案運作。
- 與網路和端點防護層共享入侵指標 (IOC) 情報。

NSS LABS RECOMMENDED
RECOMMENDED
Breach Detection System
3 YEARS IN A ROW
99.8% Detection Rate

ICSA labs CERTIFIED

Email Inspector 可偵測及攔截試圖利用員工疏失來滲透企業網路的勒索軟體：

- 已知勒索軟體：病毒碼與信譽評等分析。
- 未知勒索軟體：通訊流量特徵、腳本模擬、零時差漏洞攻擊、針對性攻擊、密碼保護的惡意程式。
- 藉由客製化沙盒模擬分析來偵測修改、加密大量檔案以及修改備份檔案的行為。

一旦偵測到勒索軟體即可將其攔截，不讓病毒到達收件者，進而防範任何資料遭到加密。可自動與網路和端點防護共享入侵指標 (IOC) 以防範後續的攻擊。

DEEP DISCOVERY EMAIL INSPECTOR 裝置硬體規格

硬體規格	7100 型	9100 型
部署選項	MTA、BCC、SPAN/TAP 模式	MTA、BCC、SPAN/TAP 模式
處理容量	每日最高 400,000 封電子郵件	每日最高 800,000 封電子郵件
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)
尺寸	43.4 (17.09) x 64.2 (25.28) x 4.28 (1.69 英吋) 公分	43.4 (17.09) x 75.58 (29.75) x 8.73 (3.43 英吋) 公分
重量	19.9 公斤 (43.87 英磅)	31.5 公斤 (69.45 英磅)
管理連接埠	10/100/1000 BASE-T RJ45 連接埠 x 1 iDRAC Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 連接埠 x 1 iDRAC Enterprise RD45 x 1
資料連接埠	10/100/1000 BASE-T RJ45 x 3	10/100/1000 BASE-T RJ45 x 3
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 600 GB 2.5吋 SAS	2 x 4 TB 3.5吋 SATA
網際網路通訊協定支援	IPv4 / IPv6	IPv4 / IPv6
RAID 組態	RAID 1	RAID 1
電源供應器	550W Redundant	750W Redundant
電力消耗 (最大)	604W	847W
發熱量	2133 BTU/hr (最大)	2891 BTU/hr (最大)
作業溫度	10 至 35°C (50-95°F)	10 至 35°C (50-95°F)
硬體保固	3 年	3 年
可選購光纖網路卡	雙埠光纖 Gigabit (SX/LX)	雙埠光纖 Gigabit (SX/LX)

Deep Discovery Email Inspector 是 **Deep Discovery** 平台很重要的一部分，能在您企業最重要的閘道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 是一台隨插即用的網路裝置，可監控所有連接埠與 107 種以上的通 訊協定來偵測針對性攻擊。其豐富完整的偵測技巧，例如內建的沙盒模擬分析，能確保迅速偵測針對性攻擊。

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、網站與電子郵件閘道防護、網路防護以及其他 Deep Discovery 產品。可疑的物件或網址可自動或手動送交 Deep Discovery Analyzer 進行分析。Deep Discovery Analyzer 可利用完整的偵測與反制躲避技巧來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、Mac 和 Android 作業系統。

1 2016 年 Verizon 資料外洩調查報告 (Data Breach Investigations Report)

採用 XGen™ 防護為基礎的 Deep Discovery Email 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
- 網路釣魚、魚叉式網路釣魚以及其他電子郵件威脅
- 零時差惡意程式與文件漏洞攻擊
- 勒索軟體攻擊

TREND MICRO™

Securing Your Journey to the Cloud