惡意威脅的預警系統
Network Traffi c Security Analytics

即時入侵檢測與完整的威脅能見度

Bitdefender 惡意威脅的預警系統 (NTSA) 是適合企業的資安解決方案，可即時準確檢測進階攻擊、自動執行警報分類，並提供相關資訊以利有效應變。NTSA 讓組織能藉由專門的網路防禦來彌補現有資安架構 (網路和端點) 之不足，從而快速檢測和應對複雜的威脅。

NTSA 利用網路流量作為可靠資訊來源，能在受感染的端點行為發生異常時立即偵測入侵，有效檢測已知或前所未見的一般威脅或進階持續性攻擊 (APT)。事件警報經過自動關聯和分類，可提高資安監控效率，改善事件調查和應變時間。

「Bitdefender NTSA 提供全面的網路能見度，使威脅無所遁形，讓資訊部門完全掌握網路上出現的不良情況。」

知名汽車及製造業大廠

替各種網路裝置即時檢測威脅

不受端點類型或現有資安解決方案 (公司或用戶管理裝置、網路元件、BYOD、IoT) 影響，針對威脅相關活動，為網路中所有端點提供完整的能見度。

資安事件自動分類更省時事件分類

以自動化方式關聯相關事件和產生高精確警報，自動執行資安事件分類，從而提升分析師的威脅獵捕效率。

透過精細的鑑識尋找網路威脅

對所有資安事件提供詳細說明和建議的行動方案，從而改善事件調查和回應。

網路威脅情報與人工智慧領域的領導者

NTSA 運用從全球5億個端點收集而得的高級 Bitdefender 網路威脅情報 (CTI)，將其與先進的機器學習 (ML) 和啟發式演算法結合，可即時分析網路 meta-data，並準確顯示威脅活動和可疑流量模式。藉由側重於對外流量的自動安全分析，可降低雜訊，為資安監控提供實用警報。

IntelliTriage 智慧分類 — 資安警報分類自動化

IntelliTriage 是最新推出的 NTSA 組件，可自動執行資安事件分類，以顯著改善事件調查時間，並通過高精確警報降低組織風險，並依據資安事件提供建議補救步驟的指南。

複雜的情境導向學習能夠高精確檢測進階攻擊，並且可以處理數以千計的資安警報，對每一事件瞭若指掌。IntelliTriage 針對事件嚴重性分級提供詳細說明，並顯示建議補救措施，可提升事件應變速度。

「在確定資安需求之時，我們考量到入侵網路的惡意軟體構成的潛在威脅，基於這個原因，我們專門尋找檢測這些威脅的新方式。我們認為，最佳解決方案必須能辨識由內往外傳輸的網路流量。」

知名醫療機構 ICT 管理部門主管

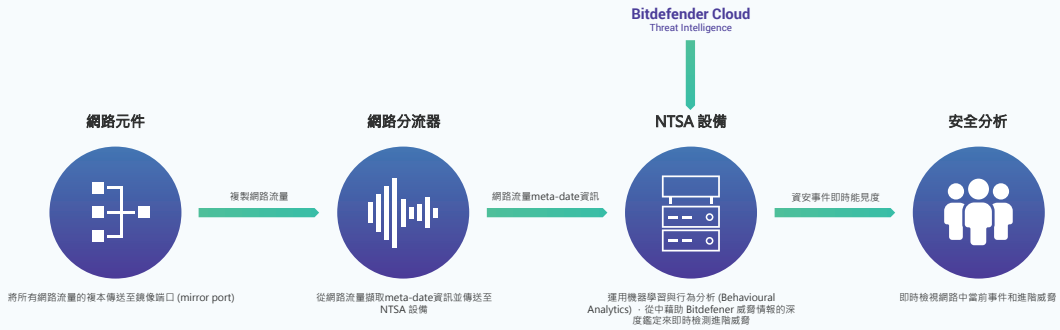
針對物聯網 (IoT) 與自攜裝置(BYOD) 提供防護

企業環境日趨由個人電腦與智慧裝置共構。儘管傳統電腦一般受到嚴密監視和多重保護，但處於灰色地帶的智慧裝置所受保護有限或不存在，網路中越來越多裝置成為下手目標，在進階攻擊發生時首當其衝。

NTSA 入侵偵測功能也擴及企業網路中的智慧裝置，著重於端點的網路行為，可保護具有有限或不具備內建資安功能的裝置，如同大多數物聯網裝置，無需在頂層執行端點安全代理程式。

員工在企業環境中使用個人筆電、手機和其他裝置時，便給了攻擊者盜取公司資訊的可趁之機。確保自攜裝置 (BYOD) 的資安可提升員工工作效率，降低公司洩資風險。 NTSA 對所有用戶和裝置行為持續進行即時監控追蹤，有效運用高級威脅情報，幫助保護組織免於竊資之災。這是一套無代理程式、非侵入式的解決方案，獨立於作業系統之外。

NTSA 運作模式



合規支援

包括歐盟個資法 GDPR 在內，許多法規要求組織如遇入侵時，迅速提供惡意活動的相關詳細資訊。 NTSA 保存長達 12 個月的網路流量記錄資訊，有助於組織滿足合規要求。其記錄內容僅有 meta-date，不包含 payload，並且僅限資料隱私專員存取，可消除敏感資訊暴露風險。

NTSA 特點

即時回溯檢測
即時被動式檢查對外流量中的所有惡意通訊，以便檢測入侵。將新型威脅情報運用於 meta-date 記錄，可回溯檢測入侵。

威脅情報雲端更新 / 地端分析
Bitdefender 雲端威脅情報結合基於人工智慧 / 機器學習和啟發式演算法的即時網路流量分析，達到更加出色的威脅檢測率和低誤判率。

防護範圍加大，完整的能見度
不受端點類型或現有資安解決方案 (公司或用戶管理裝置、網路元件、BYOD、IoT) 影響，針對威脅相關的網路活動和端點流量異常，提供完整的能見度和深度鑑定。

自動分類，高效率威脅獵捕
以自動化方式進行安全分析和降低雜訊，提升分析師的威脅獵捕效率，並且產生實用警報，在資安事件中有效應變。

加密通訊及隱私
著重於流量 meta-date 可分析加密通訊，並排除涉及非加密流量的隱私問題。

迅速配置，立即見效
憑藉簡單的混合運算架構 (實體或虛擬配置皆可) 和隨插即用 (Plug-and-Play) 元件，可立即收到成效。

GravityZone 主控台整合
與 Bitdefender GravityZone 本機部署完成單一簽入 (SSO) 整合，打造快捷的無縫管理。

Bitdefender
Cyberview 力悅資訊
力悅資訊股份有限公司
■ 台北市中山區松江路54號4F-4 ■ 02-25429758 ■ Sales@cyberview.com.tw
http://www.cyberview.com.tw/