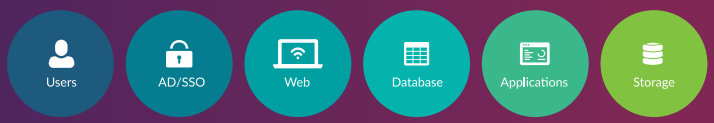
EXTRAHOP

Extrahxop Reveal(X) 解決方案

運用 Extrahop NDR 網路可視性實現零信任轉型

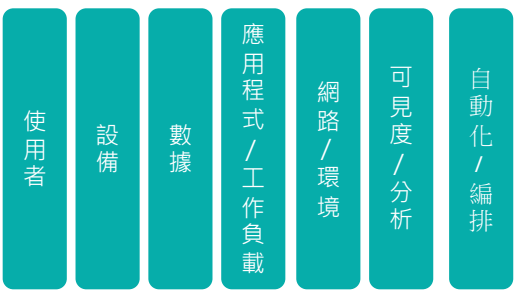


隨著雲端和行動技術的採用不斷增加，在此過程中傳統的網路邊界已經消失，網路流量的可視性變得越來越重要，尤其在東西向流量中，您將發現妥協後的行為，例如偵察、橫向移動、權限升級、命令和控制通訊等，這些行為預示著早期的攻擊。

美國國防部遵循 NIST 對零信任的定義：

零信任是一組不斷發展的網路安全範式的術語，它將防禦從靜態的、基於網路的邊界轉移到專注於使用者、資產和資源。

雖然身分驗證和其他基於身分的工具是零信任的重要組成部分，但實現零信任涉及技術、策略、流程變更和工作流程的組合。任何單一實踐或工具都無法創造零信任環境。



美國國防部零信任戰略規定了零信任安全模型的以下七個支柱或重點領域，這些支柱或重點領域被普遍認為是協同工作以實現有效的零信任實施所必需的。

1. **使用者** - 您能看到誰在使用您的網路嗎？
2. **設備** - 您能辨識網路上有哪些設備嗎？
3. **數據** - 您能看到網路中傳輸的不同類型的數據及其去向嗎？您可以評估加密資料是否有威脅嗎？
4. **應用程式/工作負載** - 您能看到正在使用哪些應用程式嗎？
5. **網路/環境** - 您對網路架構有整體了解嗎？
6. **可見度/分析** - 您能否全面監控網路上的活動？
7. **自動化/編排** - 您能否建立正常網路活動的基線，然後應用人工智慧來自動偵測與正常網路和使用者行為的可疑偏差以及策略執行？

Extrahop Reveal(x) 揭示未知並揭露攻擊

Extrahop Reveal(x) 提供整個網路（包括使用者、裝置和應用程式）的資料包級可見性。透過持續監控所有流量並建立基線，Extrahop Reveal(x) 可以即時識別可疑或惡意活動。這種可視性使您能夠 "**永不信任，始終驗證**"，而不會減慢關鍵業務流程。

使用者

特權存取管理：企業組織可將此功能描述為刪除永久管理員/提升權限，轉而採用特權帳戶管理 (PAM) 系統。進階 PAM 功能可實現自動權限升級批准並利用分析進行異常檢測。Extrahop NDR 提供最終使用者行為的可見性，使組織能夠監控和審核特權身分。

使用者活動監控： Extrahop NDR 分析東西向流量，並結合規則和進階分析來識別橫向移動等攻擊後策略。它建立行為基線來發現異常和惡意行為。此資訊增強了企業組織可基於風險的身份驗證和存取控制。

設備

設備清單：Extrahop NDR可以自動、持續地發現和分類網路上通訊的所有資產，以建立完整的設備清單。根據企業組織政策，只有清單中列出的已知授權設備才允許存取。

具有即時檢查的設備授權：Extrahop NDR被動監控網路上的資產，並即時提供使用者和裝置活動的可見性，根據觀察到的行為和對等分組建立基線，以針對可疑或惡意活動發出警報，從而實現明智的訪問決策。

應用程式和工作負載

應用程式清單：必須識別和清點所有應用程式和應用程式元件。只能使用授權的應用程式或應用程式元件。Extrahop NDR 解決方案可自動發現應用程式並對其進行分類，提供即時應用程式分析並對應應用程式相依性。

持續監控和持續授權：根據美國國防部路線圖，企業組織應採用自動化工具和流程來持續監控應用程式並評估其操作授權。Extrahop NDR 解決方案可以擴展以持續監控每個感測器的大量網路吞吐量，並使組織能夠識別應用程式和工作負載中的可疑和惡意行為，以支援零信任計畫。

數據

資料遺失防護 (DLP) ：企業組織應確定執行點、部署經批准的 DLP 工具，並將標記的資料屬性與 DLP 整合。因此，應該檢測並減輕資料外洩或滲漏傳輸。當 DLP 工具被繞過或無法如預期運作時，Extrahop NDR 可以提供故障保護。透過持續監控和可選的資料包存儲，Extrahop NDR 使取證調查人員能夠快速過濾到相關網路流量，以發現特定的可疑資料外洩。

數據監控和感知：美國國防部零信任戰略指出，數據所有者應捕獲活動元數據，其中包括有關其數據資產的存取、共享、轉換和使用的資訊。Extrahop NDR 工具始終處於開啟狀態並被動監控網路封包以獲得最高保真度的元資料。

網路與環境

資料流映射：Extrahop NDR 工具根據觀察到的行為了解正常資料流，並在偵測到異常和/或可疑資料流時建立警報。此外，Extrahop NDR 還可以偵測惡意行為，例如用於資料外洩嘗試的 C2 通訊和東西向的橫向移動。對於企業組織來說，了解資料流至關重要，這樣他們才能為網路分段和存取控制奠定基礎。

軟體定義網路 (SDN)：SDN 的目標是透過集中式伺服器提供網路封包流的控制，以實現動態且高效的網路配置。Extrahop NDR 透過提供盤點和審計 SDN 基礎設施所需的可見性而發揮關鍵作用。

自動化和編排

策略決策點 (PDP) 和策略編排：企業組織應收集並記錄所有基於規則的策略，以便在整個安全堆疊中進行編排，以實現有效的自動化。應建立 PDP 來確定資源並根據預先定義的策略啟用、監視和終止連線。Extrahop NDR 提供的網路可見性和行為洞察可用於開發和調整這些策略並建立整體的企業安全設定檔。

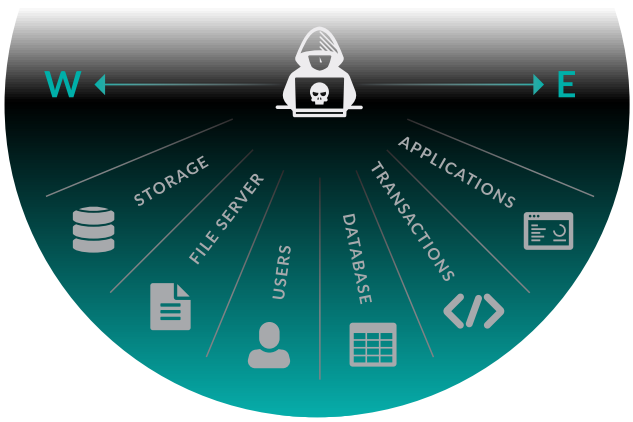
可視性與分析

記錄所有流量（網路、資料、應用程式、使用者）：企業組織應收集和處理所有日誌，包括網路、資料、應用程式、裝置和使用者日誌，並將其提供給適當的 SOC 或服務提供者。Extrahop NDR 解決方案被動收集原始資料包並將其轉換為交易、元資料、檢測、分析等，同時保持原始資料的完整性。某些日誌可以被刪除或繞過，Extrahop NDR 解決方案使用連續資料包擷取並且無法規避。

安全資訊和事件管理 (SIEM)：SOC 應監視、偵測和分析記錄到 SIEM 工具中的資料。這使得能夠對異常用戶行為進行有效的安全分析、發出警報以及對常見威脅的相關事件回應的自動化。Extrahop NDR 工具可以配置為將從即時網路資料包分析中得出的元資料饋送到 SIEM 中，以提供高保真資料、消除盲點並加速威脅偵測。

這一切都始於網路的可視性。畢竟，如果您不知道自己在保護什麼，又怎麼能有效地防禦呢？

當您掌握了保護範圍後，就可以分析網路流量與之互動的方式。這包括：使用者是誰、他們在使用哪些應用程式，以及他們如何連接。透過這些資訊，您可以評估他們之間的互動情況，從而制定一套策略，確保資料能被安全地存取。



EXTRAHOP

NetFOS 逸盈科技

詳情內容請洽代理商逸盈科技
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 976-8909