EXTRAHOP

解決方案 I 簡介

透過無與倫比的網路可視性阻止勒索軟體攻擊

您的目標是在降低風險的同時推動業務。但是，當網路攻擊利用未知風險（安全盲點）時會發生什麼？透過 RevealX，您可以全面了解網絡，從而消除盲點並快速識別逃避現有安全和 IT 工具的勒索軟體指標。

如何防禦看不見的威脅？

隨著攻擊的增加，與勒索軟體相關的風險只增不減，攻擊年增 95%，勒索軟體支付額將在 2023 年首次突破 10 億美元。威脅行為者不斷尋找更聰明、更狡猾的方法來發動勒索軟體攻擊並存取（和隱藏）端點和網路。他們利用新出現的漏洞並不斷改變策略、技術和程序來逃避檢測並擴大影響。

雖然傳統的端點偵測和回應 (EDR) 解決方案對於整體網路安全策略至關重要，但它們可能會被規避和操縱，從而為網路犯罪分子留下了可乘之機。此外，EDR 工具不會偵測到濫用有效憑證的惡意行為者。一旦勒索軟體攻擊者繞過 EDR，他們就可以隱藏在網路上，執行複雜的攻擊後活動殺傷鏈，有時需要等待數天甚至數週才能完成任務。防禦者需要一種更聰明的方法來利用此視窗在造成損害之前捕獲並阻止勒索軟體。

獲得您網路的完整可見性

全面了解網路上的即時和歷史活動對於在勒索軟體攻擊成功之前阻止勒索軟體攻擊至關重要，只有網路偵測和回應 (NDR) 工具才能提供這一點。 ExtraHop Reveal(X) NDR 平台使組織能夠深入了解規避其現有安全和 IT 工具的網路威脅、漏洞和網路效能問題。

使用人工智慧驅動的行為分析和機器學習， Reveal(X) 可以追蹤並記錄勒索驅動的攻擊者破壞網路、嘗試透過基礎設施進行操作、枚舉目標、升級網域權限或透過嘈雜的 DNS 通道發送 C2 信標。它可以在加密開始之前發現資料暫存和其他可疑行為模式，這些模式可以指示勒索軟體攻擊。

憑藉完全的網路透明度，組織可以更聰明地進行調查，更快地阻止威脅，並根據風險的速度採取行動。

使用 RevealX 將威脅解決速度提高 87%

消除盲點
獲得完整的覆蓋

偵測其他工具未能偵測到的威脅
偵測威脅速度提高 83%

迅速採取行動捍衛您的企業
修復時間縮短 86%

好處

完整的網絡能見度

全面了解網路上的所有內容：從使用者、辦公室到資料中心或雲，每個使用者、應用程式、資產、交易、服務和工作負載。如果發生這種情況，即使在加密流量中，RevealX 也可以看到它。

廣譜檢測

偵測由機器學習/人工智慧驅動，由多個專有和第三方情報來源提供，並提供豐富的上下文以加速分類和緩解。我們的專家研究團隊開發的威脅簡報為新興和關鍵漏洞提供指導檢測和調查工作流程。

企業規模平台

RevealX 為資料中心、雲端和分散式環境提供單一平台，提供統一的網路智慧、交付到用戶需要的任何地方。它提供解密和分析即時流量，高達每秒 100GB，不會降低服務或增加延遲。

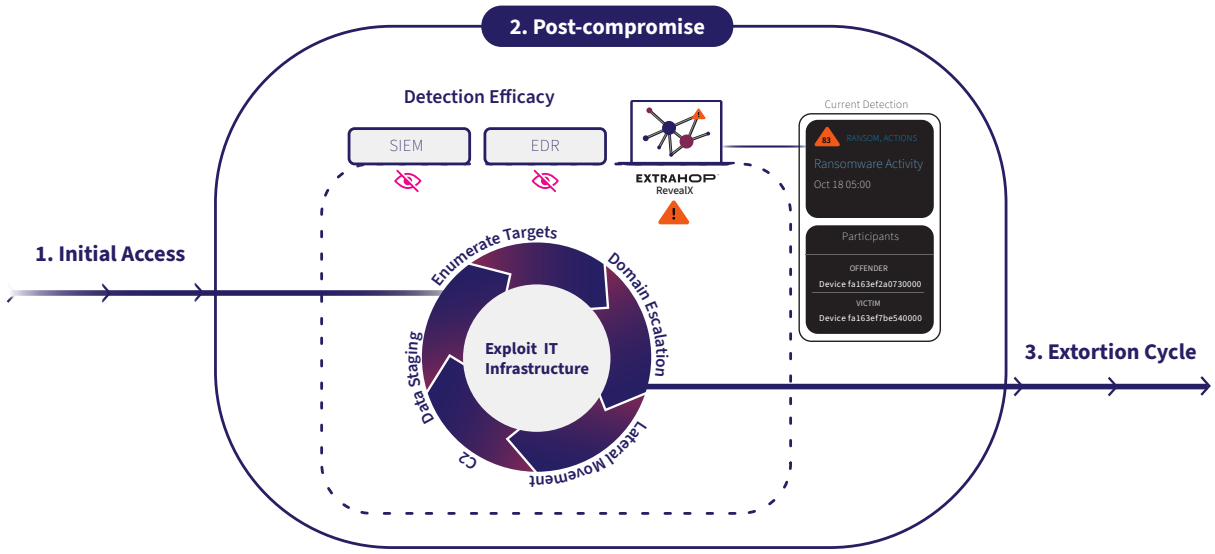
現代可擴展性和集成

公開可用的 API 和文件（包括 REST 和觸發器類型）使團隊能夠將 RevealX 與跨本地和 SaaS 部署的現有技術堆疊整合。

> “如果沒有 ExtraHop，調查將需要數天或數週的時間，使醫院面臨潛在的災難性風險。當聯邦調查局發現我們識別並遏制[勒索軟體]威脅的速度之快時，他們也留下了深刻的印象！
>
> — Joanne White，Wood County Hospital

How RevealX Works

Stop the Ransomware Kill Chain



用例

偵測受損資產	網路遙測可以更好地了解基線行為並快速檢測偏差。 RevealX 發現其他工具錯過的勒索軟體入侵者，動態調整雲端規模的機器學習以適應不斷變化的環境。
對EDR 規避應用補償控制	勒索軟體攻擊者透過應用本地技術以及利用普遍存在的非託管伺服器、Linux 主機和物聯網設備來逃避啟用 EDR 的端點。透過被動網路觀察，RevealX 對這些規避行為具有獨特的可見性。
保護敏感數據	借助 RevealX，您可以防止資料被盜，並在高價值資料庫和檔案系統被劫持之前發現資料加密的跡象。透過即時情境實現更快、更自信的行動。
追捕勒索軟體威脅	RevealX 提供直覺的威脅搜尋工作流程，以及人工智慧驅動的優先順序和建議，因此各種技能水平的分析師都可以像資深專家一樣進行威脅搜尋。分析師透過自動化、有效率的調查工作流程更快地形成和測試假設。
恢復更快網路取證準備狀態	事件回應人員立即採取行動，進行 90 天的連續流量記錄回溯和可擴展至 24 PB 的長期 PCAP 儲存庫。他們可以透過使用智慧調查功能來建立事件回應手冊，將學到的經驗教訓應用於未來的回應。

採取下一步

造訪我們的網站 了解如何為您的組織實現全面的網路可見性，以阻止勒索軟體威脅並降低業務風險。

關於 ExtraHop 網絡

ExtraHop 是企業值得信賴的網路安全合作夥伴，可揭示網路風險並增強業務彈性。用於網路偵測和回應以及網路效能管理的 ExtraHop RevealX 平台獨特地提供了無與倫比的可見性和解密功能，組織需要這些功能來更聰明地調查、更快地阻止威脅並以風險的速度採取行動。了解更多信息，請訪問www.extrahop.com 。