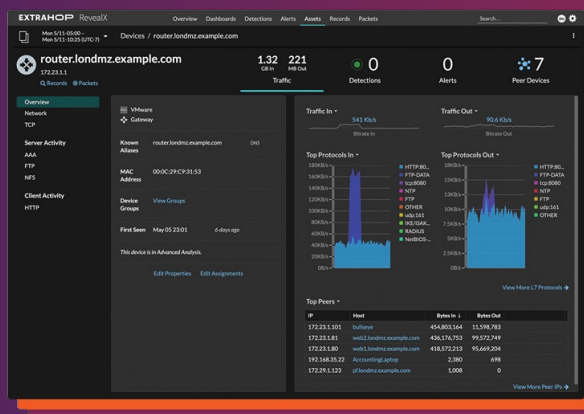


NETWORK DETECTION & RESPONSE

更快地揭示和
回應網路風險

Reveal(X) NDR

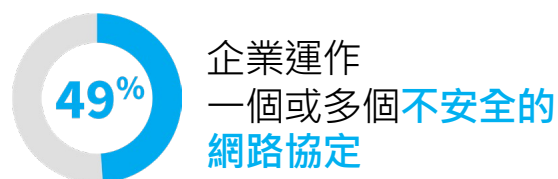
獲得所需的即時可見性，以更快地識別風險、
更聰明地進行調查並充滿信心地回應威脅。



網路可視性至關重要

用於管理網路風險和建立業務彈性

威脅行為者利用漏洞並不斷更改TTP，以逃避偵測並擴大影響。



現有工具不足

EDR 不覆蓋所有端點並且可以被攻擊者規避

SIEM 不是偵測攻擊的可靠資料來源，可以停用日誌

IDS 只捕捉已知威脅

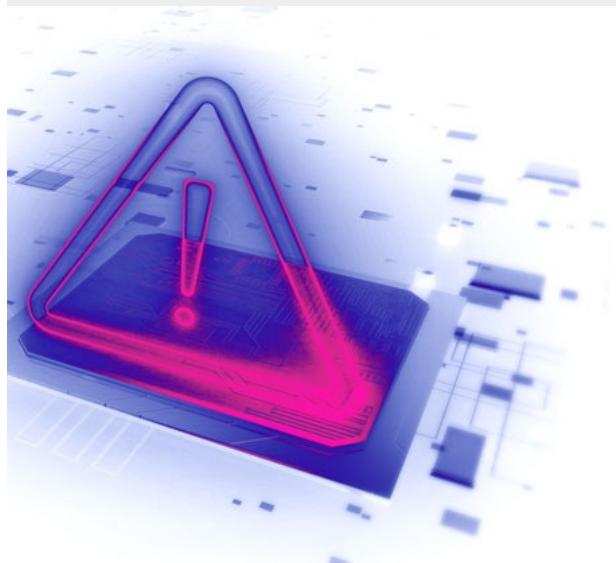
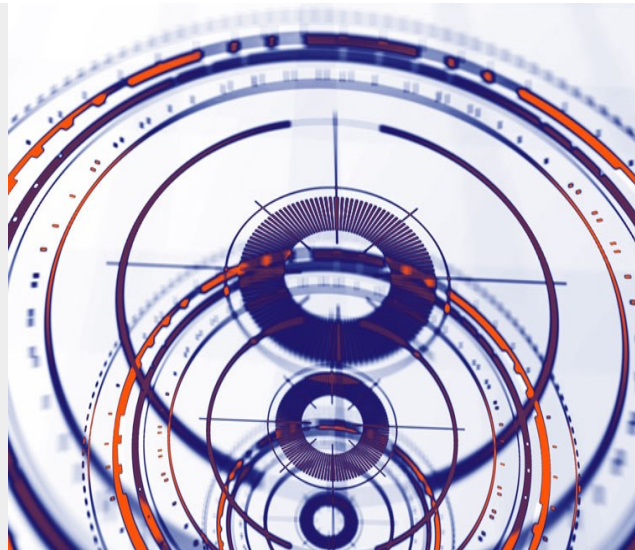
NGFW 缺乏東西向流量的可視性；將數據納入調查工作流程很麻煩

了解為何 Reveal(X) 與眾不同

完整的網路可視性

全面了解網路上的所有內容-每個使用者、應用程式、資產、交易、服務和工作負載-從使用者和辦公室到資料中心或雲端。如果發生這種情況，RevealX 可以看到它。

- **進階解密**：針對Mirror的流量進行解密，速度高達每秒100GB，包括對 TLS/SSL 1.3、SMBV3、MS-RPC 等高階標準的支援。
- **協定流暢性**：解析從資料鏈結層到應用層的每筆交易，涵蓋70多種的協定並持續增加。
- **發現和分類**：對設備、應用程式、用戶和交易進行持續、被動式的發現，並具備自動化對應和分類功能。



深度範圍偵測

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，並通過上下文、風險評分、攻擊背景和專家指導的後續步驟來豐富每個檢測，以實現自信的響應。

- **機器學習/人工智慧**：雲端規模的 ML/AI即時分析網路串流，利用5000+ L2-L7功能的機器學習和預測建模。
- **自信的響應編排**：Reveal(X) 處理檢測和調查，同時與Phantom和Palo Alto等解決方案的強大集成支持增強和自動響應工作流程。
- **回顧性智能**：網絡歷史記錄的存儲長達90天，並自動對過去活動中的問題進行回顧式偵測。

企業級平台

適用於資料中心、雲端和分散式環境的單一平台可提供統一的網路智能，並可依用戶需求提供。

- **高吞吐量**：即時解密和分析全球流量，高達每秒100 gigabits，不會降低服務或增加延遲。
- **高階整合**：針對業界領先平台提供的整合，包括EDR、SD-WAN、SOAR/SIEM、防火牆、工單系統和事件管理等。
- **現代可擴展性**：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與其跨本地和SaaS 部署的現有技術堆疊整合。



網路可視性降低網路風險

Reveal(X) 看到了其他安全工具看不到的東西



ExtraHop 提供給企業全面的風險可視性
涵蓋其整個攻擊面，這樣您就可以：

更聰明地調查

透過即時網路洞察和高保真機器學習檢測來提高效率
和業務彈性。

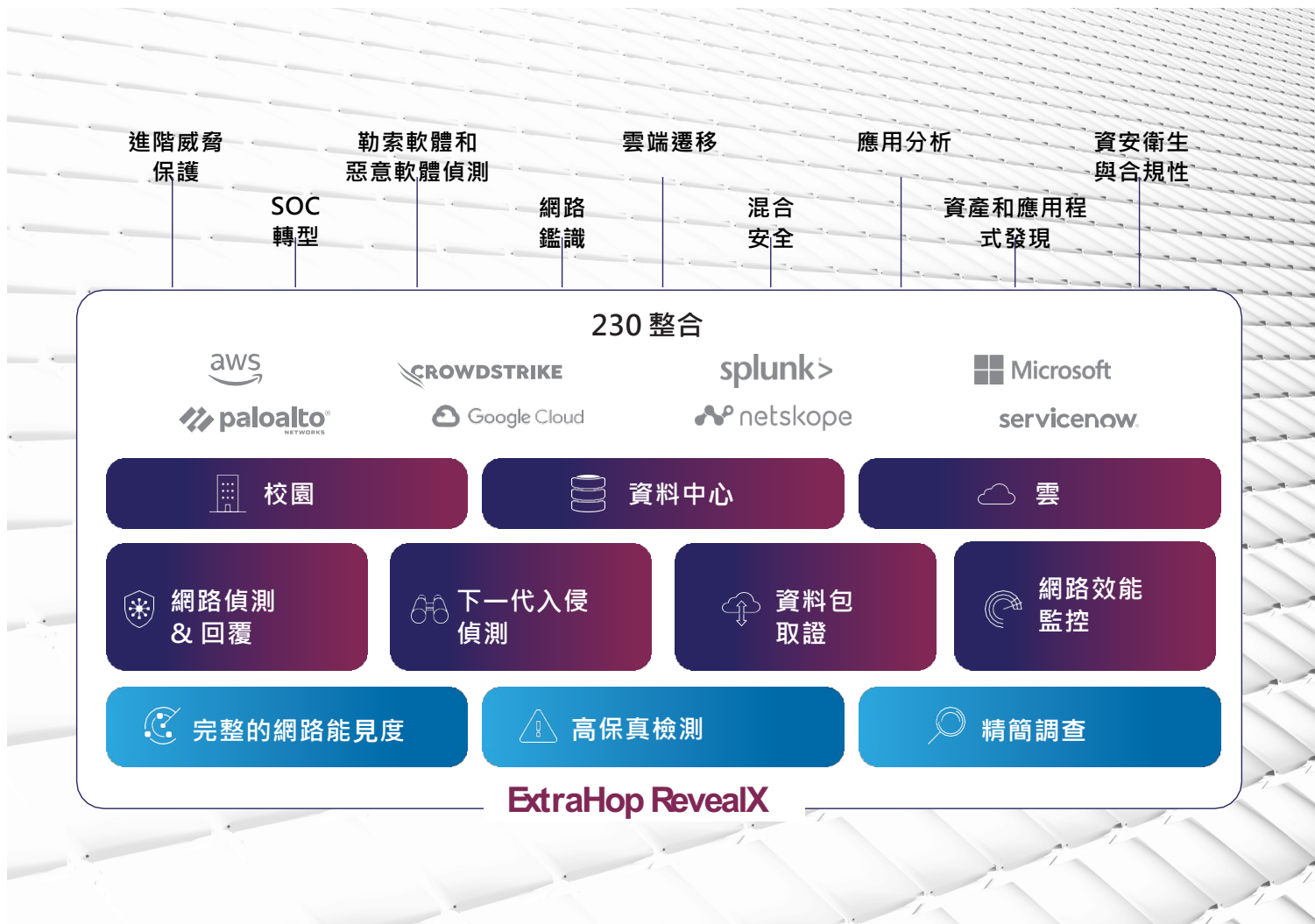
更快地阻止威脅

消除盲點並儘早回應威脅，
以防止業務中斷並最大程度地減少財務影響。

以風險的速度行動

透過揭示整個組織中隱藏的風險
並實施補償控制來支援業務
並保持營運運作。

雲端原生網路安全與效能平台



ExtraHop 支援 DoD(美國國防部) 的零信任能力

