中芯數據 CoreCloud Tech.

Gigamon × ExtraHop 解決方案

整合網路安全和可視化

Gigamon 網路安全交付平台與 ExtraHop NDR（網路偵測與回應）的整合結合了網路流量視覺化和深度威脅偵測能力，能夠在複雜環境中提升安全營運效率。

目前客戶在網路安全和可視化方面面臨的挑戰，包括如：

- 加密流量的威脅偵測
- 混合雲環境的複雜性
- 安全工具的效能瓶頸
- 網路盲點和威脅隱藏

Gigamon®
消除網路盲點，賦能安全工具

×

EXTRAHOP
在混合雲與加密流量成為常態的背景下，需持續強化「可視化即安全基礎設施」

整合的核心優勢

流量優化與高效率偵測

Gigamon 提供流量聚合、去重和過濾，降低網路噪音，確保 ExtraHop NDR 接收高品質流量數據，提升威脅偵測精確度。
支援加密流量解密（TLS/SSL），使 NDR 分析原本不可見的加密通信，減少盲點。

降低營運複雜度與成本

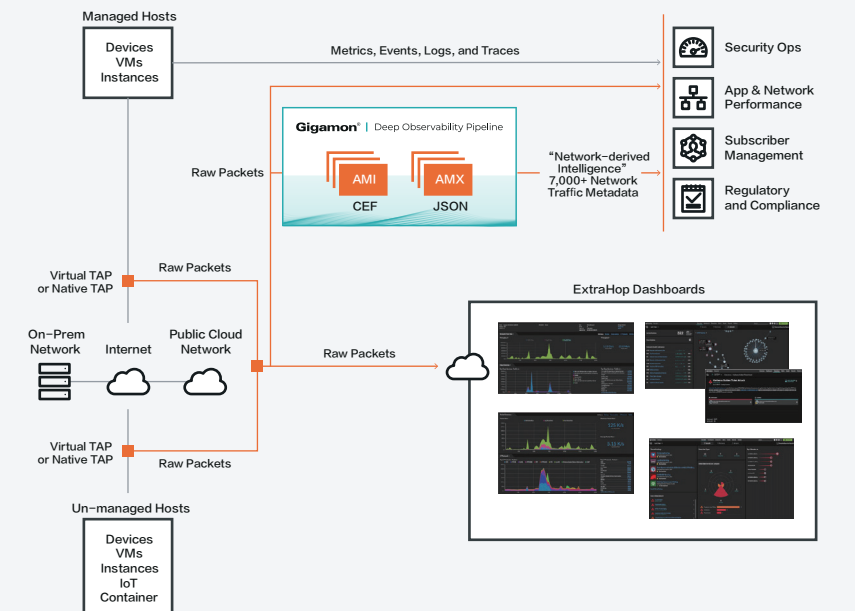
透過統一流量分發，減少安全工具重複部署，節省硬體資源及授權成本。
自動化威脅回應（如連動防火牆隔離受感染設備）縮短 MTTR（平均修復時間）。

增強上下文關聯分析

Gigamon 的元資料（Metadata）與 ExtraHop 的行為分析結合，可識別異常橫向移動、資料外洩等隱藏威脅。

合規與審計支援

提供完整的流量記錄與取證能力，滿足金融、醫療等行業的嚴格合規要求（如 GDPR、HIPAA）。



典型應用場景

1. **混合雲與多雲環境** 統一監控跨公有雲、私有雲和本地資料中心的流量，應對雲端遷移中的安全碎片化問題。
2. **零信任架構實作** 透過持續網路行為分析（如微隔離策略驗證），動態調整存取控制，支撐零信任模型落地。
3. **高級威脅狩獵 Threat Hunting** 結合歷史流量重播（PCAP）與即時分析，追溯潛伏威脅，辨識 APT 攻擊鏈。
4. **關鍵基礎設施保護** 監控 OT/ICS 網路中的異常流量，防範針對工控系統的針對性攻擊。
5. **合規性監控與稽核** 自動化產生網路活動報告，證明資料流合規性（如 PCI DSS 要求）。

中芯數據 Cyber Defense Center 作為您企業內部資安團隊的延伸，協助企業共同防禦進階威脅。
www.corecloud.com.tw

詳情內容請洽中芯數據
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 976-8909