

Fidelis Elevate®

想像您的對手如何思考，做好一切準備

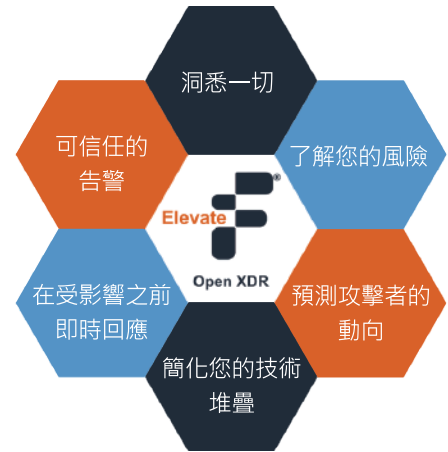
現代的計算環境變得越來越龐大，大型的數位轉型計畫也在不斷地擴展，使得被攻擊面越來越廣泛，同時數據也無所不在，攻擊者變得越來越密集且活躍。這個等式中唯一保持不變或縮小的部分，是組織為應對網路攻擊而配備的人員和資源。因此自動化、無縫整合的安全營運以及對抗網路攻擊的能力至關重要，而這正是 **Fidelis Elevate** 發揮作用的地方。

Fidelis Elevate 的運作原理

Fidelis Elevate 是您維護資安環境安全的核心，建立公開且主動的擴展偵測與響應平台 (XDR) 是為了積極地做好防禦，**Fidelis Elevate** 提供可視性與整合誘捕，即時對整個環境的威脅偵測、搜尋和響應，**Fidelis Elevate** 將 IT、物聯網、數據中心和雲系統的資安情報集中到單一視圖中，資安團隊可以快速偵測和封鎖攻擊，對潛在的威脅進行深入檢查和分析，提升業務能力，並盡快將受影響的系統恢復到可正常地營運。

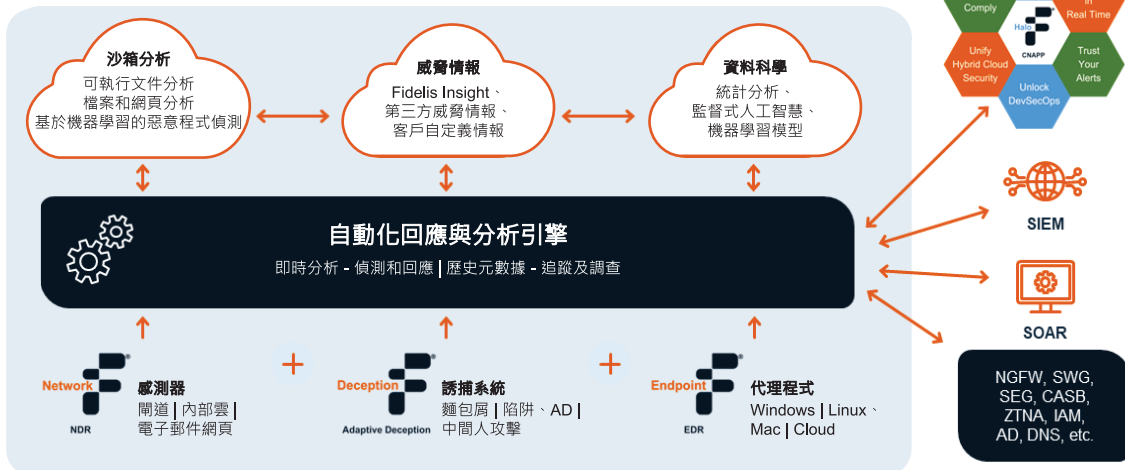
Fidelis Elevate 的優勢

- 全面的資產和風險控管
- 擁有專利的深度檢查技術
- 主動威脅偵測
- 整合式誘捕技術
- 即時分析和響應自動化
- 內建與其他資安產品的界接



Fidelis Elevate®

由分析師建立，為分析師而設定的開放式 XDR



Fidelis Elevate

Fidelis Elevate 包含深度可見性

Fidelis Elevate 提供即時風險分析和響應，透過對所有端口和協議的流量，進行深度專利對話檢查，Fidelis Elevate 利用快速的 20GB 1U 感測器，檢測其他工具可能會遺漏的風險，且在更少的機架空間中，更快速地進行檢測，包含嵌套文件中的威脅、加密流量和瞬息萬變的容器化工作負載。

- 確認及分類所有管理和非管理的資產，包含本地、雲端和端點
- 將整個安全堆疊中的數據和風險整合為一個來源，包含 NDR、EDR、IT / OT、漏洞掃描、CNAPP、CASB、活動目錄等
- 通過深度專利對話檢查和即時解密流量，在嵌套和加密流量中深入查看威脅

主動檢測威脅

透過基於 MITRE ATT&CK 框架的自動化分析模型，Fidelis Elevate 將與威脅相關的活動串聯在一起，主動檢測威脅提供事件詳細的內容與時間軸，有助於進行快速地調查和響應。

- 使用相同或者更少的資源提高偵測和響應速度
- 通過具高真實度的結論排除警報疲勞
- 自動將弱信號整合並設置告警閾值

自動化誘捕

憑藉整合雲端和 AD 的誘捕技術，Fidelis Elevate 在安全堆疊中建立了彈性，通過動態可變地形，增加攻擊者的成本和風險，同時提供資安團隊可視性和時間的優勢。

- 自動部署動態誘捕層使攻擊者分心，同時也讓資安團隊研究攻擊者的行動
- 仰賴即時性和回顧分析確定活動與過去的威脅，不斷地改進資安風險，提升彈性
- 主動防禦策略保持業務連續性、提升彈性

無縫整合

作為一個公開且可擴展的 XDR 平台，Fidelis Elevate 與許多第三方解決方案無縫整合，進一步增強和改善您的整體資安環境，開箱即用的整合和全面的 API，用於自定義整合，展現 Fidelis Elevate 現有解決方案的價值。

- 自動部署動態誘捕層使攻擊者分心，同時也讓資安團隊研究攻擊者的行動
- 仰賴即時性和回顧分析確定活動與過去的威脅，不斷地改進資安風險
- 主動防禦策略保持業務連續性、提升彈性



台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室
高雄辦事處
高雄市三民區民族一路80號27樓之2 A08室



關於 Fidelis Security®

Fidelis Security® 是積極資安防禦領域的產業創新者，透過積極的 XDR 和 CNAPP 平台，保護全球企業的現代資訊技術，Fidelis Security 整合 IT 資安營運，縮小攻擊面，自動化威脅偵測、加速分析、鑑識和回應，使企業在資安攻擊中保持彈性，變得更強大且更安全。Fidelis Security 受到全球頂尖企業和政府機構的信任。

