

## Fidelis Network™ 解決方案概述



### Fidelis Cybersecurity® 唯一名列美國軍隊資訊安全認證產品列表的資安解決方案。

Fidelis 高端的進階威脅偵測技術已成為整個美國軍隊將它確立為核准的技術使用資安鑑識產品，並將 Fidelis Network 添加入美國軍隊資訊安全認證產品列表 ( Army IA-APL )，Fidelis 在美國國防部、陸、海、空軍、情報機構，以及美國州/市政府部及三大科技業: APPLE、Microsoft、IBM 等客戶群，目前採用 Fidelis Network 解決方案防禦進階式威脅以及數據洩露的風險，從而保護身份數據，商業機密信息和作戰安全的敏感信息。

除了提供顯著的進階威脅防範和數據洩露預防功能，還提供了落實網絡和安全策略檢測合法授權和未經授權的使用能力。作為第一個也是唯一的新一代 ATD 主動威脅防禦解決方案 Fidelis Network 獲得通用標準安全認證( Common Criteria Security Certification )，Fidelis Network 也經歷了" Red Team "滲透測試由 Sandia 國家實驗室為空軍信息作戰之作戰實驗室 ( AFIOB )。這種測試是 AFIOB 的整體評價和選擇 Fidelis Network 作為運營安全項目外部驗證，推動進階式威脅解決方案的一部分。

### 鑑識能力和控制能力對威脅生命週期的所有階段

進階的 APT 針對性的攻擊並不是突然發生的暫態事件;而是在一段時間內發生的多個階段的複雜過程。Fidelis Network 綜合的 ATD 主動威脅防禦解決方案;包括高端的防禦技術及威脅情資，可有效發現隱匿的攻擊完整內容，以及後續可完整鑑識追蹤調查和遏制所有攻擊的進階威脅生命週期。

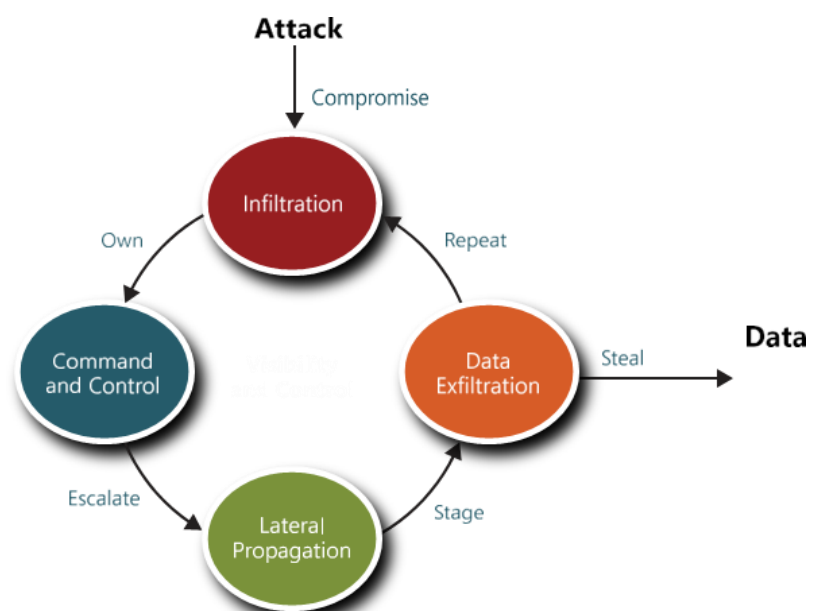
**滲透階段:** 駭客集團需要先滲透和掌控你組織中任一網路設備，透過駭客的惡意程式元件取得你的電腦與網路資產的存取權限。

#### 遠端指揮和控制通信的階段:

駭客集團一旦取得資產權限，它們會嘗試執行遠端控制你的電腦與網路設備。

**橫向傳播階段:** 成功地取得網路資產權限控制後，駭客會試著去尋找及滲透其他連在你的網路上的內部資產設備，並尋找有價值的、機敏性資料。

**資料竊取外洩階段:** 駭客集團會想辦法避開資安系統，將收集到的資料打包或以加密的方式，透過網路傳輸並成功竊取。



## 全面的進階式威脅防禦

Fidelis Network 提供先進的惡意軟體防護、資料竊取保護以及網路安全分析，集成在一個單一緊密的鑑識系統連續保護您的組織，並縮短整個攻擊威脅生命週期。



### APT 先進的惡意軟體防護

- 高級惡意軟體檢測
- Real-Time 即時威脅預防
- 自動化威脅情報
- 靈活的安全政策 (規則)
- 超高效能流量檢測
- 靜態特徵碼比對(Static analysis)
- 動態程式碼模擬執行 (Simulation)
- 豐富的惡意程式註解資料庫
- 可偵測與阻擋未知的網路通訊協定

### DLP 資料防竊取保護

- 資料洩漏預防
- 智慧財產權保護
- 完整內容可見度
- 靈活的資料分析
- 可靈活操作警報
- 關鍵字/詞/檔名比對
- 正規表示式比對
- 文件特徵碼註冊/比對
- 圖片檔特徵碼註冊/比對
- 數位指紋 MD5 比對
- 加密檔案偵測阻擋
- 二進位檔正規表示式比對

### 資安鑑識網路安全分析

- 完整 Metadata 資料收集
- 多維度分析
- 進階視覺化、圖像化
- 客製化的報表
- 關聯性警報
- 以圖形化顯示行為分析結果，包含內外部 IP 通訊的關聯性分析與使用的通訊協定
- 可提供 APT 縱向與橫向全面向異常連結的時間與關連性 IP
- 客製化報表可轉成 email 或 PDF 格式自動傳送給稽核人員

## Fidelis Network 效益

- 在威脅生命週期的所有階段實現更精準的縱深威脅檢測率，增加攻擊態勢感掌握和即時預防。
- 通過強大及全譜的網路可視性，實現資安控制和預防降低企業風險。
- 以更快速的修復補救及減少事件發生來降低資安事件回應成本。
- 通過整合的縱向及橫向深度資安防禦，減少網路安全基礎設施的成本。
- 降低資安經營成本與自動化的告警規則和即時威脅情報更新。

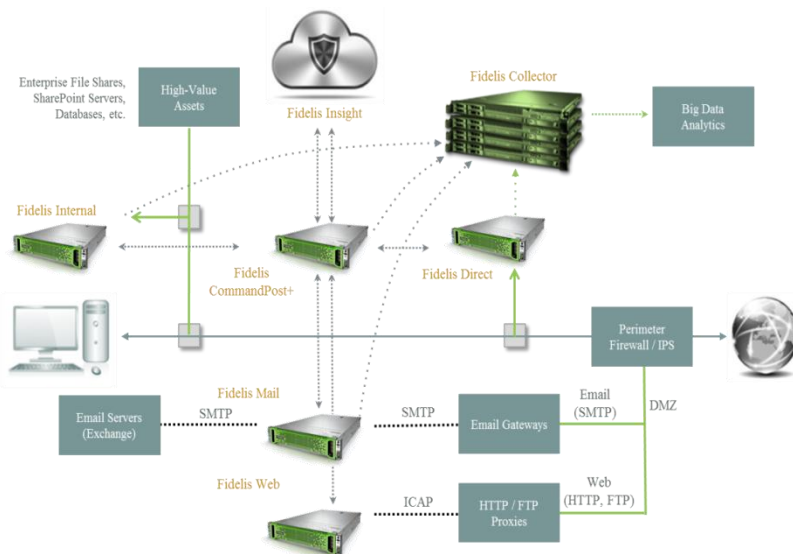
# FIDELIS NETWORK SOLUTION

Fidelis Network 是一個設計運用於快速部署的開放且靈活的平臺。提供積極主動的威脅態勢感知也提供可自由操作的威脅情報。Fidelis Network 把鑑識重點設計在通過各階段的重要攻擊數據集中事件、可快速調查所有階段允許且非法的事情和遏制攻擊的威脅生命週期。

Fidelis Network 綜合 ATD 主動威脅防禦解決方案是由四個主要元件組成：

**Fidelis INSIGHT:** 雲端服務中心，持續提供高質量的威脅情報更新，並自動部署到管理中心系統(Command Post)與內容感測器(Sensor)上運作。

**Fidelis Network COMMANDPOST:** 為 Fidelis Network 的管理系統中心提供 Web-based 的整合操作介面是用於進行創建防禦策略、政策變更、告警事件管理、感測器(Sensor)設定、報表產生及使用者管理等作業，CommandPost 可統一組合管理多點部屬之感測器。



**Fidelis Network SENSORS:** 主要為負責封包重組、解碼和分析即時網路流量的工作，運用 Fidelis 專利的 Deep Session Inspection® 技術，可即時(Real-Time)檢測/防止進階威脅/攻擊和防止資料竊取。Fidelis Network Sensor 整合了惡意軟體檢測引擎 Malware Detection Engine，以每秒數千個物件的超高速度來進行識別分析惡意程式，Fidelis Network Sensor 也從網路發生的每個網路會話中擷取每個連線的元數據(Metadata)，各種感測器可部署為透通(in-line)模式或旁接(out-of-band)模式，不同用途的感測器可在不同的實體與邏輯網路基礎結構中進行多點部署方式。

**市面上唯一同時監控: All port & All protocol & Unknown Protocol 的網路駭侵鑑識技術。**

**Fidelis Network Direct sensor** 執行所有政策規則並監控出入口雙向網路流量，包含已知/未知的網路流量、已知/未知的通訊協定及應用程式。

**Fidelis Network Internal sensor** 監控內部網路流量，提供了前所未有的網路可見度，並監控整個企業資訊如何使用的用與濫用。

**Fidelis Network Mail sensor** 執行郵件過濾政策，監控電子郵件通訊流量、偵測惡意/違規郵件自動導入隔離區、可執行惡意/違規郵件通知與信件轉送等動作。

**Fidelis Network COLLECTOR:** 提供鑑識調查網路連線的歷史紀錄，透過由感測器(Sensor)持續提供所有相關網路上的連線紀錄，並以 Metadata 的方式保存至資料庫，提供使用者查詢並分析有關連性的所有網路異常活動連線資料，無論是正常連線或是惡意威脅及非惡意的威脅，全都會被保存至 Metadata 資料庫中。這種保存方式比一般儲存完整封包資料的方式大幅節省儲存成本，並提供更豐富的查詢索引如通訊協定、應用程式及內容解碼等鑑識調查資訊。

# 硬體規格


	CommandPost+	Direct/Internal (2500)*	Direct/Internal (1000, 500)*	Direct/Internal (250, 100, 50)*	Mail	Collector SA
<b>Storage Capacity &amp; Configuration</b>	<ul style="list-style-type: none"> <li>Integrated 6Gbps hardware RAID</li> <li>1.6TB across 6x HDD in RAID-5</li> </ul>	Mirrored 300GB HDD for application and data storage				<ul style="list-style-type: none"> <li>Integrated 6Gbps hardware RAID</li> <li>2.4TB across 6x HDD in RAID-5</li> </ul>
<b>CPU</b>	2x 6 core 2.5Ghz Intel Xeon Processors	2x 8 core 2.9Ghz Intel Xeon Processors	2x 6 core 2.5Ghz Intel Xeon Processors	2x 6 core 2.1Ghz Intel Xeon Processors	2x 6 core 2.5Ghz Intel Xeon Processors	2x 8 core 2.9Ghz Intel Xeon Processors
<b>Memory</b>	48GB (ECC DDR3 1333Mhz)	64GB (ECC DDR3 1333Mhz)	48GB (ECC DDR3 1333Mhz)	32GB (ECC DDR3 1600Mhz)	48GB (ECC DDR3 1333Mhz)	64GB (ECC DDR3 1333Mhz)
<b>Network Adapters</b>	4x1Gb Ethernet ports (Copper)	<ul style="list-style-type: none"> <li>4x10/100/1000 (Copper)</li> <li>2x10Gb-SR, Bypass Capable</li> </ul>				4x1Gb Ethernet ports (Copper)
<b>Out of Band Management</b>	Integrated Management Module II (IMM2)					
<b>Performance Power Supply</b>	Dual hot-swap 550W/750W High Efficiency AC power supplies (80+ Platinum Certified)					
<b>Form Factor</b>	1U Rack-mount chassis					
<b>Dimensions</b>	Width: 440 mm (17.3 in)		Depth: 734 mm (28.9 in)		Height: 43 mm (1.7 in)	
<b>Weight</b>	15.6 Kg (35.5 lb)					
<b>Operating Temperature</b>	5°C to 40°C (41°F to 104°F)		Altitude: 0 to 915 m (3,000 ft)			

\*Direct/Internal sensor performance ranges from 50Mbps to 2.5Gbps

## 虛擬裝置最低要求

Fidelis Network 解決方案除專屬作為主機系統配置的硬體設備外，也提供虛擬設備的 VM 軟體版本，例如支援建置在 VMware vSphere。效能基準測試驗證使用 IBM x3550 M4 系統，Intel E5-2640 CPUs, DDR3 記憶體, Intel 1Gb 網卡, 及轉速 10k 的 SATA 硬碟。Fidelis Network 虛擬裝置性能是硬體配置規格和 VM 資源利用能力。為了優化系統性能，建議主機系統配置的數據與以下相等或更好的配置規格。

	CommandPost VM	Direct 1000 VM	Internal 1000 VM	Mail VM	Collector SA VM
<b>CPU</b>	8 vCPU	8 vCPU	8 vCPU	8 vCPU	8 vCPU
<b>Memory</b>	32GB	32GB	32GB	32GB	32GB
<b>Hard Disk</b>	100GB	100GB	100GB	100GB	500GB
<b>NICS</b>	1 vNIC	4 vNIC	4 vNIC	1 vNIC	1 vNIC

 中飛科技股份有限公司



CONTACT US TO DAY TO LEARN MORE ABOUT FIDELIS FIDELIS NETWORK.

台北總公司  
11492 台北市內湖區瑞光路 583 巷 32 號 5 樓  
Tel : +886-2-2658-1818 Fax : +886-2-2657-1589

台中辦事處  
40667 台中市北屯區文心路四段 83 號 19 樓 301 室(勤德商務中心)  
Tel : 04-2292-0855、04-2292-0856 Fax : 02-2657-1589

高雄辦事處  
80655 高雄市前鎮區一心二路 128 號 9 樓之 1(玖富商務中心 915 室)  
Tel : +886-7-331-5127 Fax : +886-2-2657-1589