Fidelis Cybersecurity

DATASHEET

Fidelis Network®

網路流量分析：您資訊安全架構的基石

網路流量分析

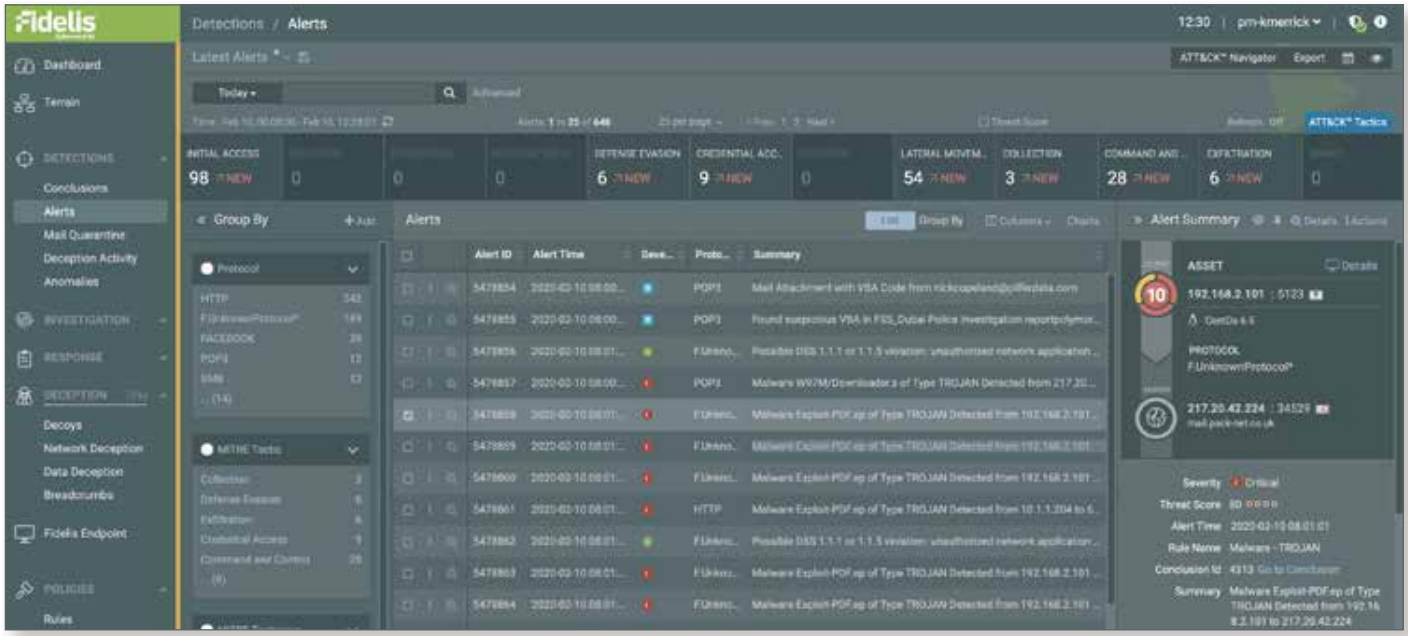
Fidelis Network 專屬的偵測器可部署在任何位置(網路閘道、內部網路、電子郵件)。即時內容分析用於 DLP 網路、電子郵件和網路流量，包括影像中的 OCR 文本。機器學習式的異常偵測建立在內容豐富的 Metadata 資料，也可透過 Fidelis Network 的資產分析和分類持續映射的網路地形中進行威脅獵捕。開放式威脅情報來源的設計，是您現代資訊安全架構的核心。

Metadata 資料如同您資安架構的 DNA

資訊安全是基於有限度的紀錄、事件及告警。機器學習及資料科學是仰賴於豐富的 Metadata 資料內容及事件歷程和根據即時的預防與偵測，以追溯分析新威脅情報的指數，Metadata 資料需要持續不斷地紀錄，而非數天或是數小時之後所產生的資料。 Fidelis Network 使用專利的 Deep Session Inspection® (DSI) 使整個 Session 階段可以重組、通訊協定及應用程式解碼，深入解碼內容，以及即時的內容、威脅和 DLP 分析。

核心優勢

- 將駭客 TTP (戰術、手法、步驟) 映射到 MITRE ATT&CK™ 框架改進告警可視性及事件處理
- 取得所有埠及通訊協定中網路流量(包括 TLS)雙向可視性
- 深入檢查多重級別內容以偵測出惡意活動及資料外洩
- 風險區分設備通信互動地圖使網路地形可視化
- 有力的機器學習模型來偵測異常行為
- 匯集告警、內容及證據，使威脅調查及分析更快速並減少處理告警的疲勞
- 自動對網路所有 IT 資產的分析及分類以瞭解您的環境
- 透過行為及歷史分析，加上資安政策及告警管理風險評等
- Fidelis Endpoint® 的整合實現事件反應自動化



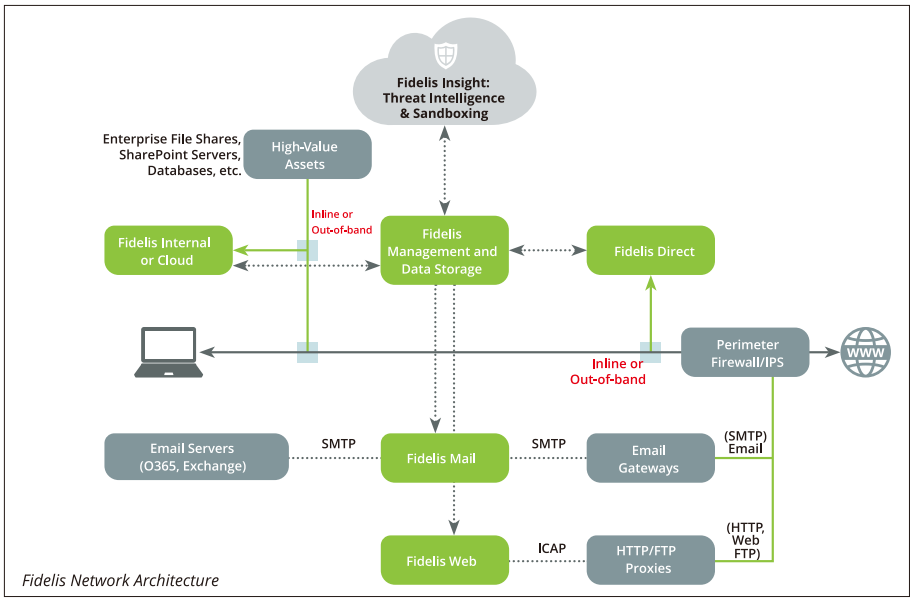
使用者取得 MITRE ATT&CK™ 的互動版本，經過已辨識的 TTP 映射該平台，以改進告警可視性及事件處理

辨識、分類、偵測、阻止及反應於一個解決方案

你無法防衛你偵測不到的攻擊。 Fidelis Network 透過分析、分類及辨識有風險的資產，提供網路地形無可比擬的可視性。 Fidelis 透過閘道、內部網路、電子郵件偵測器提供所有埠及通訊協定中的雙向即時分析，確保你的網路中沒有盲點。 Fidelis Network 也收集了超過 300 個 Metadata 資料屬性，這對即時及追溯性分析和威脅獵捕都是相當重要的。

即時可視性促進 Fidelis Network 多重防衛功能，包括：

- **威脅偵測**使用雲端式沙箱、網路行為分析、自動應用於追溯性 Metadata 資料的新威脅情報，以及機器學習異常偵測
- **威脅獵捕**以即時內容分析或是支援快速和互動式查詢追溯性索引 Metadata 資料以測試獵捕情境
- **威脅預防**使用靜態特徵碼、多維行為規則、威脅情報來源，外加模擬及啟發學習法
- **DLP** 使用網路、電子郵件偵測器預先制定策略之資料分析及分類為資安政策違規做告警
- **資料外洩**閘道及內部偵測器丟棄Session，郵件偵測器將隔離郵件丟棄Session
- **電子郵件安全**針對 URL 分析、附件及機敏資料 OCR 圖像文字分析
- **安全分析**基於事件頻率及排序分析
- **分析 TLS 加密流量**基於 Metadata 資料及憑證，決定人為瀏覽及機器流量，資料科學模型以偵測隱藏的威脅
- **威脅情報**開放來源 (Fidelis Insight、Reputation、STIX / TAXII、YARA、Suricata)，包括客製化規則及內部威脅情報



Fidelis Network Architecture

無縫整合 Fidelis Endpoint® 及 Fidelis Deception® 來建造 Fidelis Network 的基石。

使用網路、端點及誘捕科技產品以形成 Fidelis Elevate 平台，為你的組織網路地形，包括易受攻擊的表面提供了無與倫比的洞察力。 Fidelis 完全的整合、自動及組織強大的功能，包括了資產發現及分類、網路流量分析、資料外洩預防、端點偵測及事件反應和駭客誘捕科技。

FAIRLINE
Quality Service Through Team Work

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
高雄市前鎮區一心二路128號9樓之1

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cybercrime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.