Fidelis Cybersecurity

DATASHEET

Fidelis Endpoint®

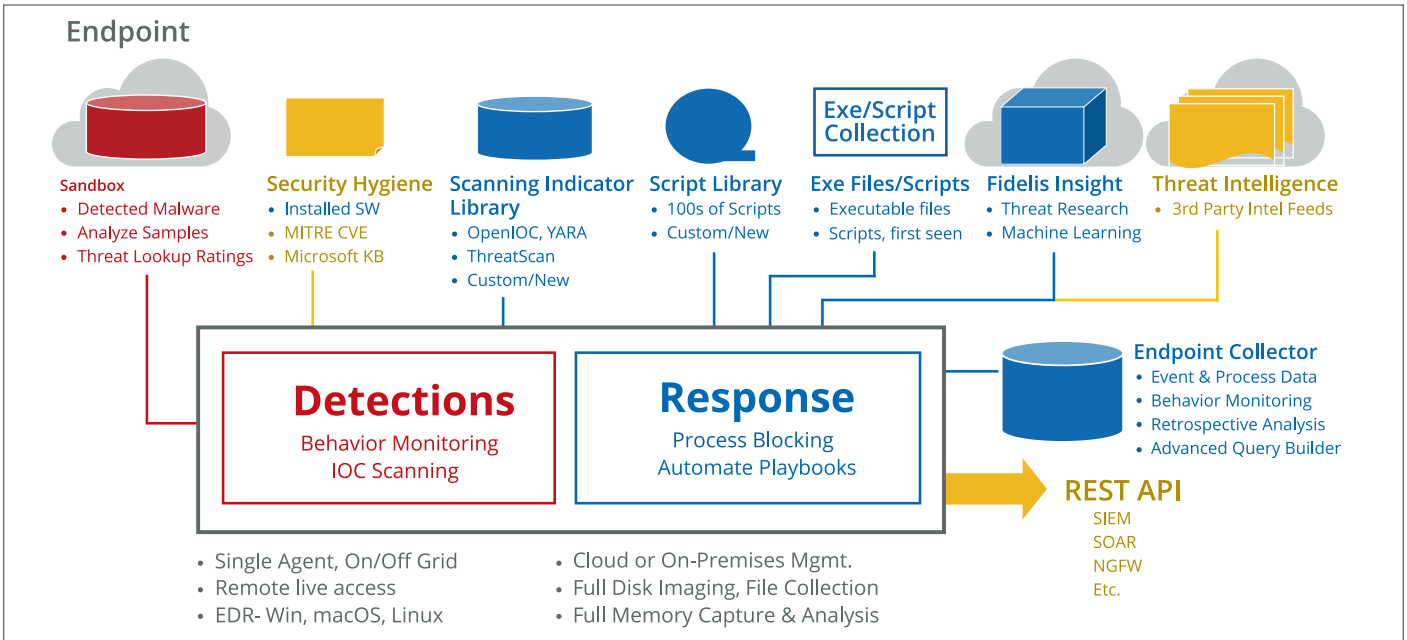
單一代理程式及中控平台以加速數位鑑識、調查及進階式威脅的事件反應

強而有力的端點偵測及反應

Fidelis端點對所有端點活動提供了深度的可視性，使得分析人員可以在幾分鐘之內對進階式威脅進行偵測、調查、獵捕及反應。Fidelis使分析師以即時且追溯性地偵測威脅、簡化威脅獵捕、透過與 AV 防毒引擎共存的解決方案達成阻擋惡意程序、進行深入的鑑識分析，以多種事件反應選項的 Advanced Scripting Engine 進行自動化反應。Fidelis端點具有單一代理程式的架構，可在本地端管理支援以連網或不連網運行，並可以擴充到 100,000 個端點。

Fidelis 端點解決方案優勢：

- **端點偵測規則映射**到 MITRE ATT&CK™ 框架以瞭解攻擊者的 TTP 並決定適當的事件反應
- **獵捕威脅**透過 IOC 及 YARA 指標的進階 EDR 功能適用 Windows、macOS 及 Linux系統中
- **分析事件及處理程序** Metadata **資料**即時或追溯性並收集所有的可疑檔案/Script
- **遠端存取**端點的磁碟、檔案及程序，以加速事件反應調查
- **開放威脅情報來源**支援來自 Fidelis Insight 開放來源及第三方內部開發情資
- **完整的軟體清單識別** 與 MITRE CVE 或 Microsoft KB 報告鏈結的漏洞
- **自動化防禦、偵測、調查及事件反應功能**，外加自定義 Script
- **選擇性 MDR 服務**進行偵測、反應與分析師溝通的全面覆蓋



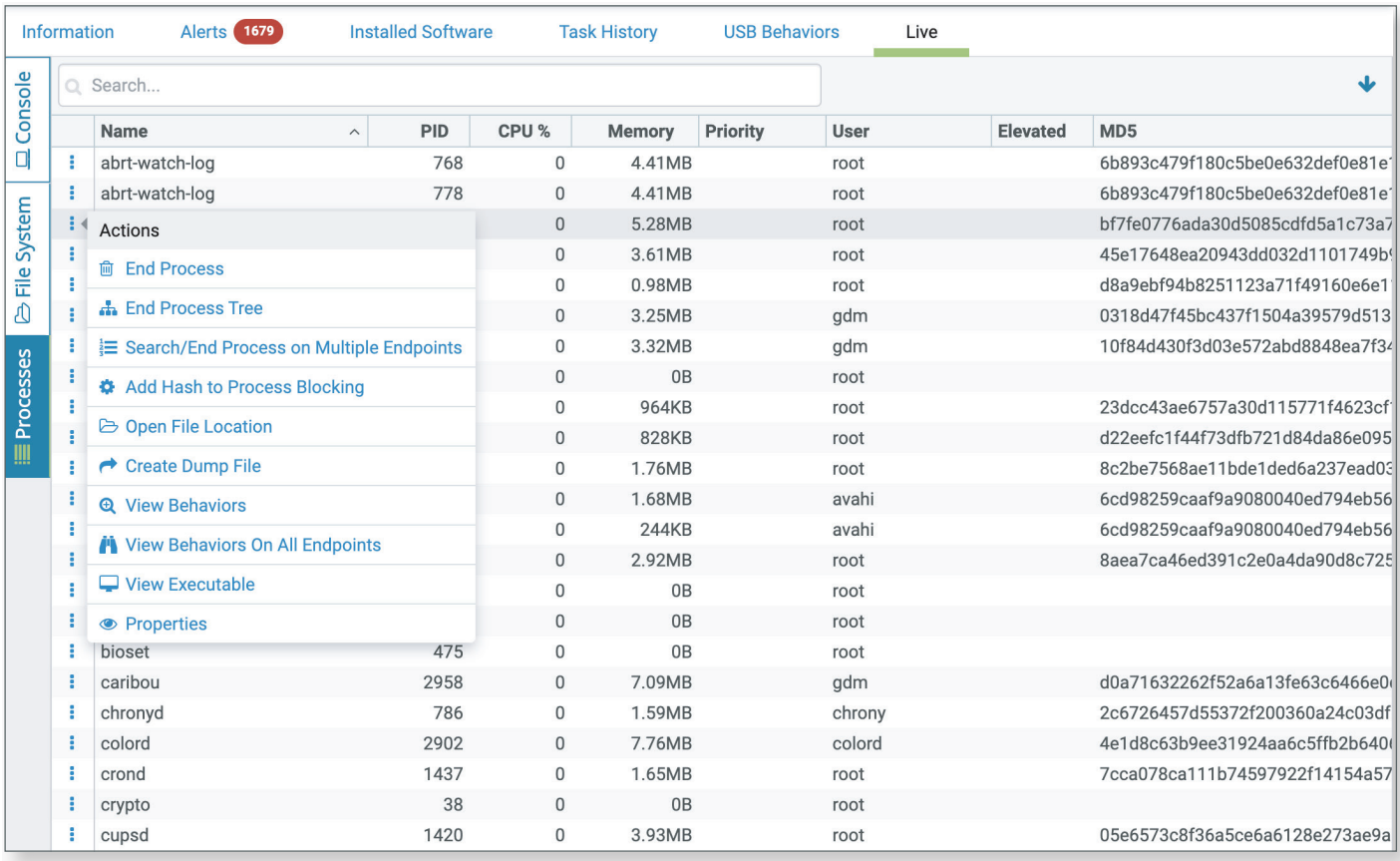
Fidelis Endpoint provides detections (red), response (blue), and third-party intelligence and integration (tan) in a single agent with on / off grid defenses.

可視性及威脅偵測

- 進階 EDR 功能支援 Windows、macOS，及 Linux 系統
- 端點偵測規格映射到 MITRE ATT&CK 框架，以瞭解攻擊者的 TTP
- 第三方資源、內部開發及 Fidelis Insight（包含沙箱、機器學習及威脅研究）存取開放威脅情報來源
- 預設自定義行為規則使反應自動化，以建立及客製化事件反應流程
- 擴充及客製化的 IOC 及 YARA 程式庫
- 30、60或90天的端點事件和即時及追溯性分析的 Metadata 程序資料 ，及最新威脅情報獵捕
- 自動應用威脅情資以偵測來自系統事件的威脅
- 關鍵事件與可疑事件的時間圖表
- 使用指標程式庫在掃描檔案系統及記憶體
- 偵測可執行檔及 Script - 獲得被刪除的檔案及隱藏攻擊者蹤跡的可視性
- 自動將不受信任的可執行檔送交雲端沙箱進行分析
- 即使離開組織網路，端點事件仍持續紀錄在本機內直到重新連線進行調查

鑑識、事件反應及預防威脅

- 客製化的 Script 及劇本資料庫採取行動及收集調查資料
- 遠端存取進入端點磁碟、檔案及程式，快事件調查及鑑識分析
- 遠端收集鑑識資料，如完整記憶體及磁碟映像檔
- 整合 SIEM、NGFW 等及執行事件反應調查
- 事件反應劇本進行自動化修補、深度分析及客製化流程
- 威脅查閱提供多重掃瞄器的雲端式偵測威脅級別
- IOC 及 YARA 規則，在企業端點中阻止惡意程序
- Fidelis 端點識別已經安裝軟體的漏洞
- 系統狀態通報漏洞修補、AV 狀態及 USB 紀錄進行資安防禦



分析師藉由 Live Console 遠端存取端點硬碟、檔案、程序資料，快速緩解資產上的威脅攻擊。

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

www.fidelissecurity.com