Fidelis Elevate解決方案
端點Endpoint

Agenda

- Fidelis公司簡介
- 閘道Network
- 端點Endpoint
- 誘捕Deception
- 聯防防禦架構

Why Fidelis

- Gartner：APT防禦架構5大技術，企業至少要具備兩項以上
  - 網路流量分析
  - 網路鑑識
  - Payload分析
  - 端點行為分析
  - 端點鑑識
- Fidelis 全部具備

Fidelis公司簡介

Fidelis™ Cybersecurity

- 創立於2002年
- 總部位於美國馬里蘭州的Bethesda
- 自動化威脅偵測和事件反應所設計的ADR 資安平台
- 美國軍隊核准使用的資安解決方案
- 美國國防部資訊安全認證產品列表(DODIN APL)

Fidelis深受世界上最重要品牌的信賴

- Apple 100G流量
- 微軟全球每個分點都有Fidelis
- 美國海軍DLP、空軍每年合約超過23.6million
- Barclays(巴克萊銀行)12萬個Endpoint
- IBM mail solution
- 美國Samsung mysingle protocol

Fidelis 多項資安認證與得獎紀錄

唯一獲得通用標準(CC)安全認證

通過美國 Sandia 國家實驗室的紅隊(Red team)測試

符合美國聯邦政府單位網路的加密要求FIPS 140-2加密驗證

獲得GCN實驗室評論選擇獎

美國軍隊資訊安全保障名錄唯一建議採購的資安產品

Fidelis 在每個時間點都可以查到攻擊事件

- 除了即時檢測外，Fidelis還可以讓您看到在先前發生的攻擊

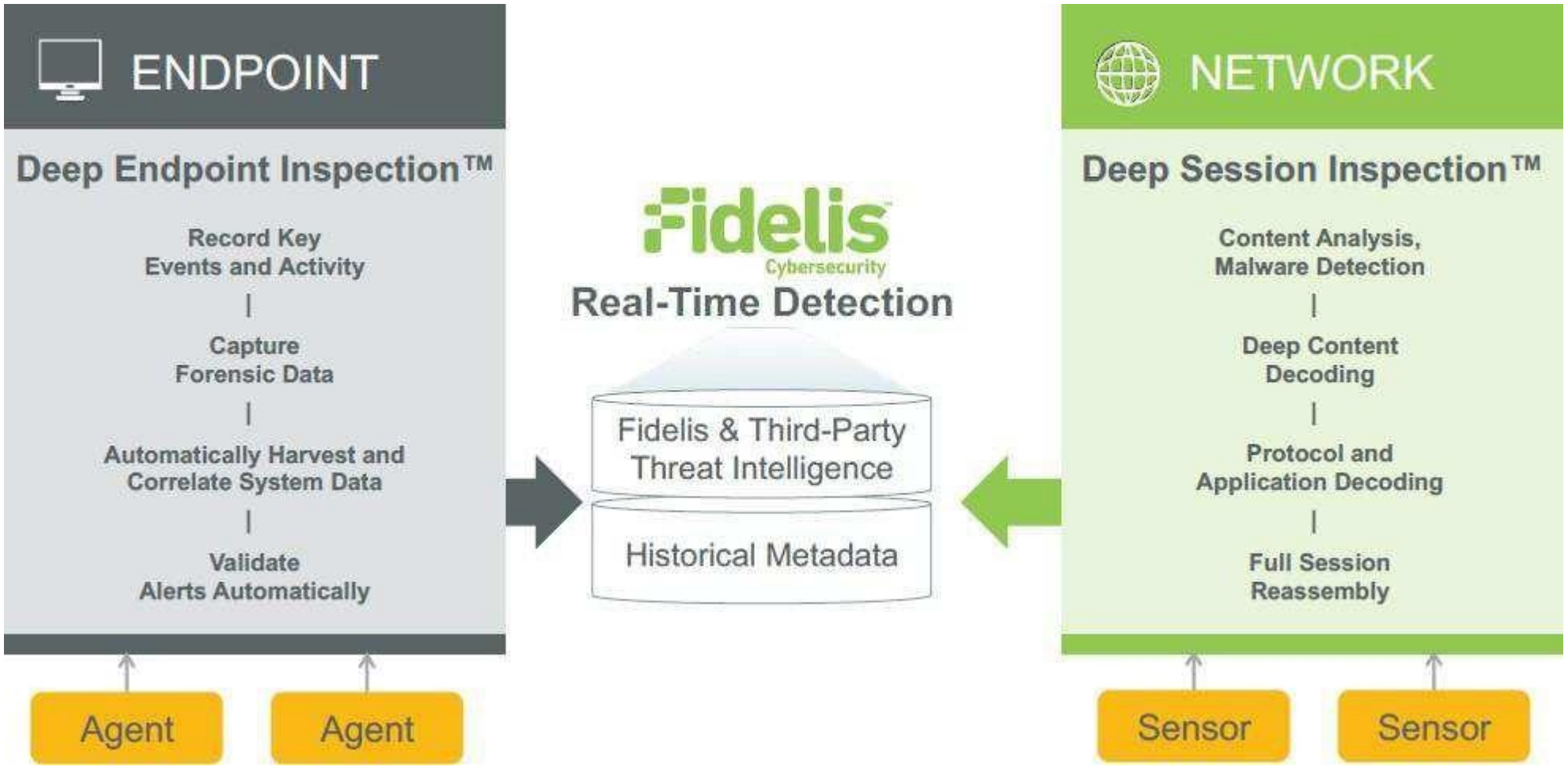
歷史資料

用情資比對歷史資料
調查告警及發生事件
偵測多維度攻擊
使用歷史資料獵殺攻擊者
看看網路上發生什麼

TODAY

確認告警
識別攻擊者活動
比對第三方威脅情資
阻擋資料外洩

Fidelis 如何偵測攻擊

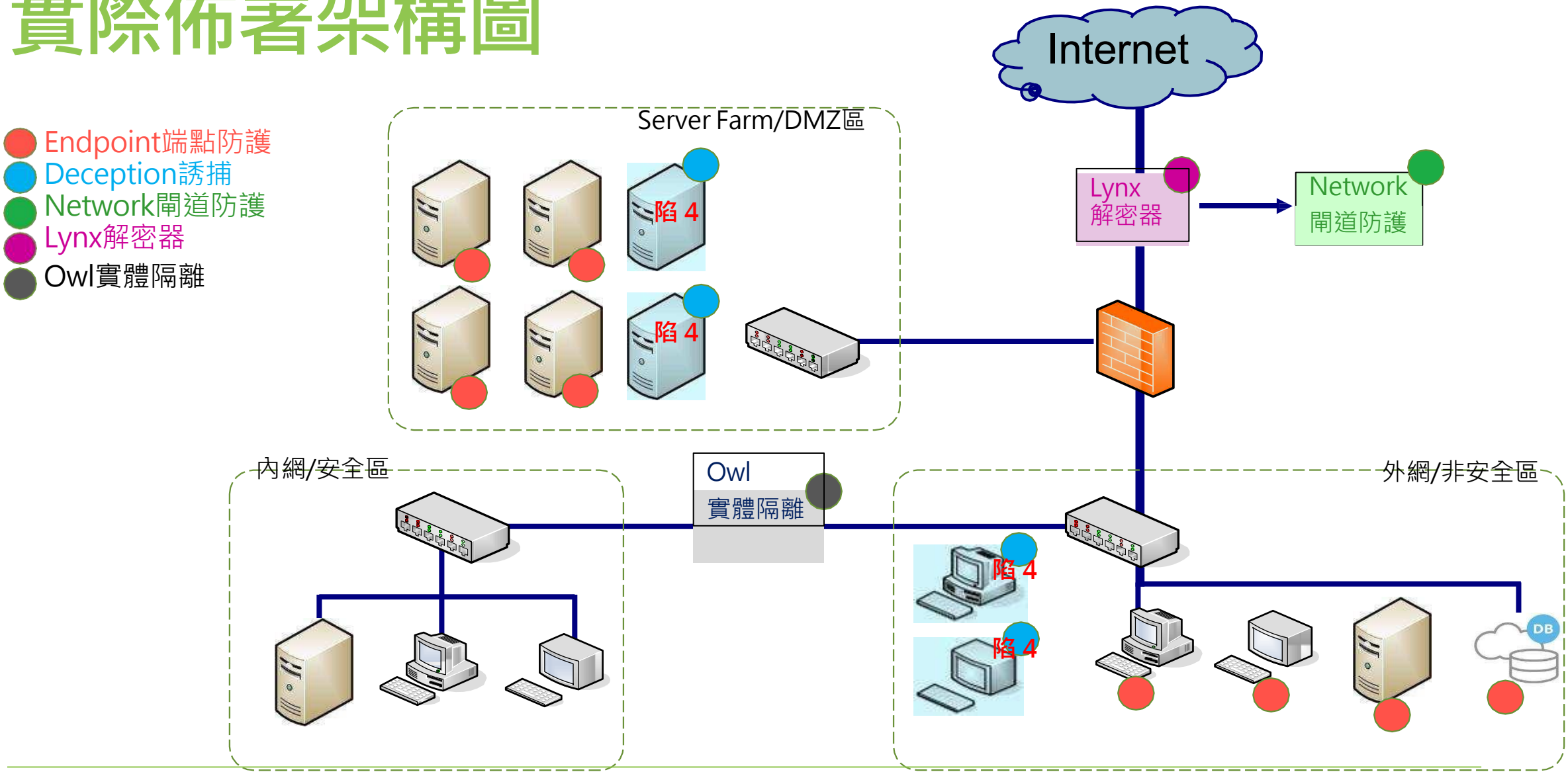


Fidelis Elevate

- 整合多個解決方案：
  - Network：網路流量監控、資料外洩防護、網路鑑識(NDR+DLP+NF)
  - Endpoint：端點防護、事件反應及端點鑑識(XDR+EF)
  - Deception：駭客誘捕科技
- 自動化的威脅偵測、獵捕和事件反應平台自
- 動驗證、關聯和事件反應
- 快速地偵測、強化獵捕駭客
- 調查歷史軌跡和瞭解事件來龍去脈

實際佈署架構圖

- Endpoint端點防護
- Deception誘捕
- Network閘道防護
- Lynx解密器
- Owl實體隔離



端點Endpoint

Endpoint 端點防禦功能

記錄/監控

端點事件全部紀錄
行為規則偵測
內建防毒軟體
端點設備狀態管理

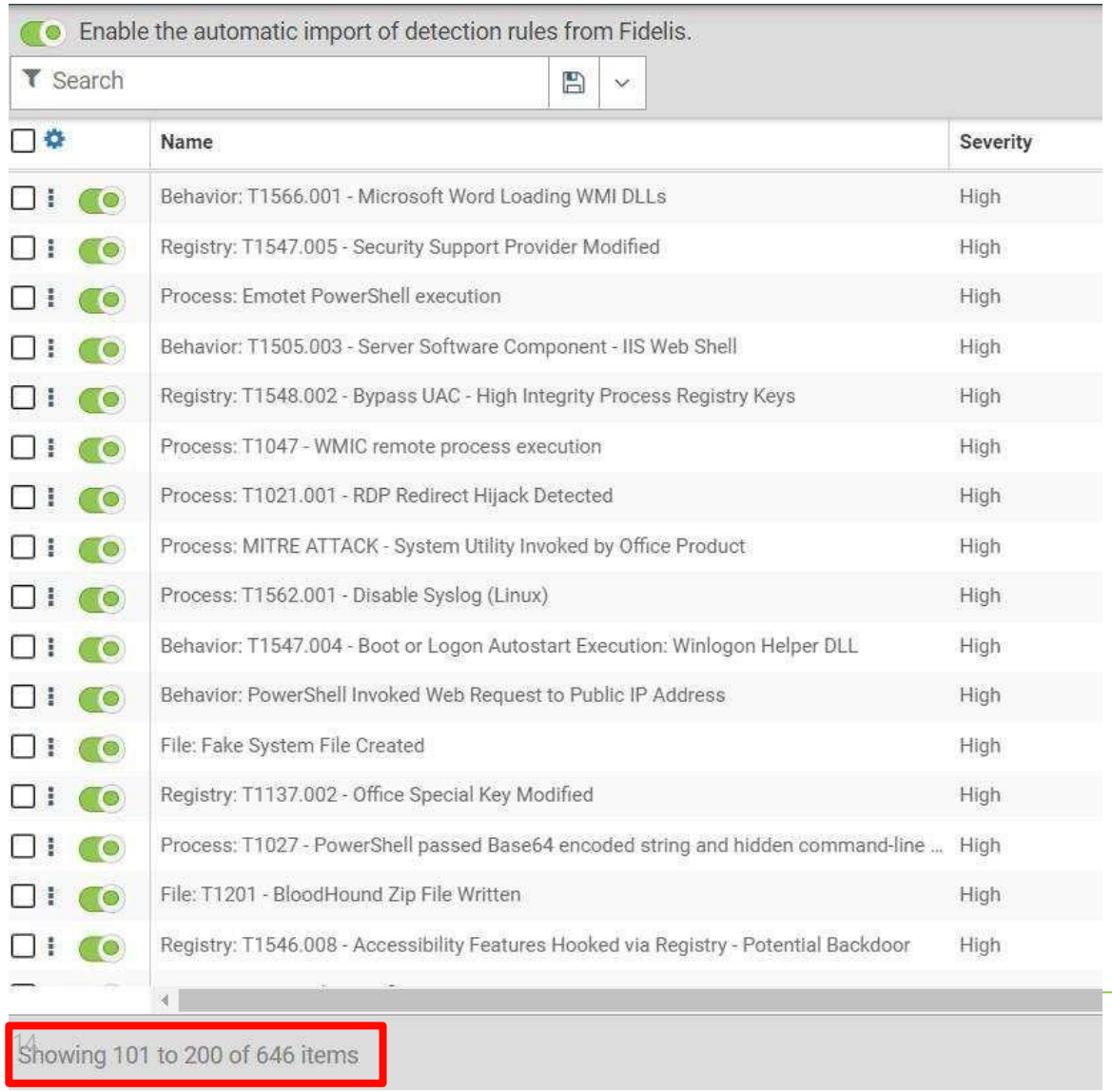
調查分析

圖像化執行緒分析
內建調查鑑識工具
襍現未知威脅的行為告警規則

處理

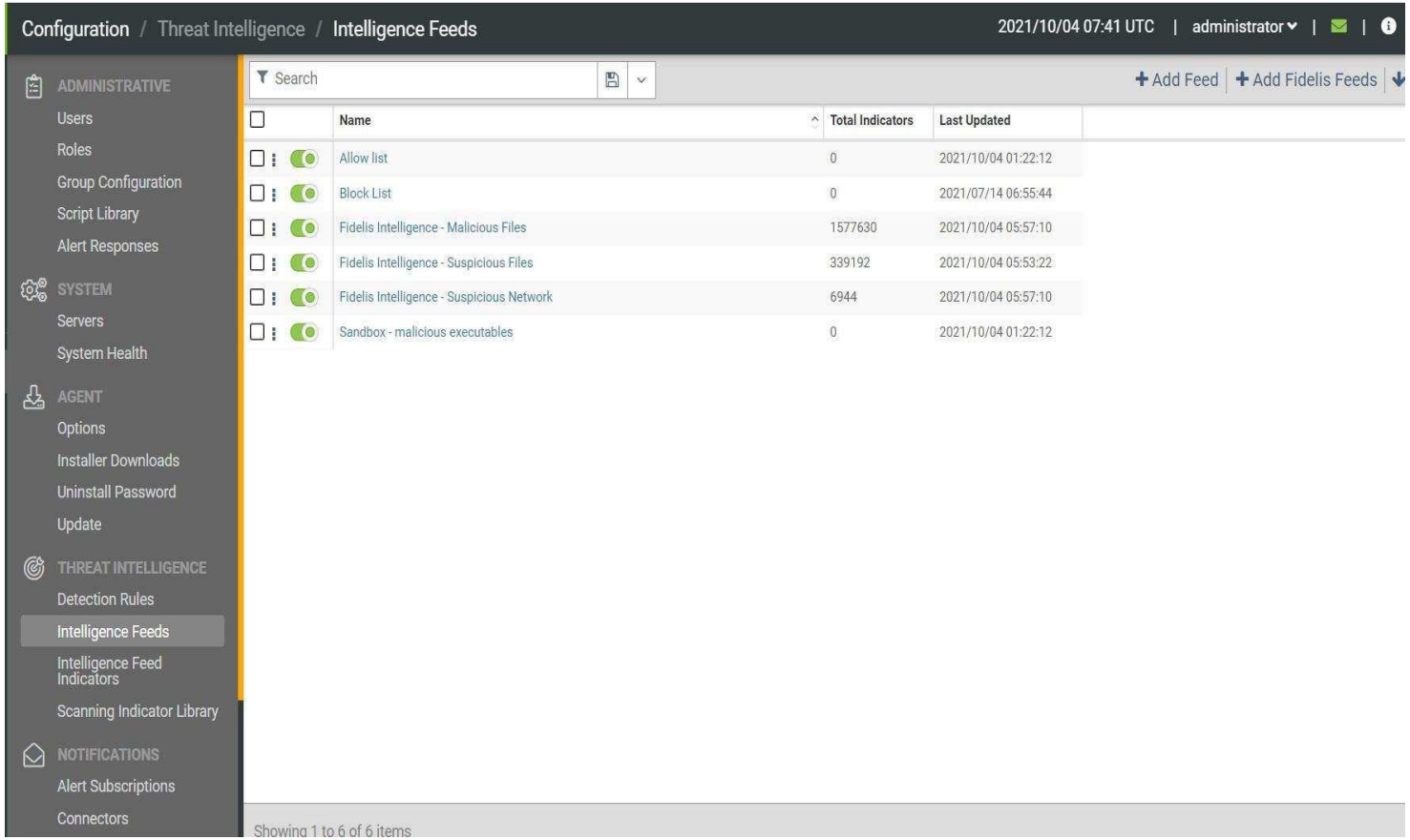
遠端收集資料檔案或上傳更新
端點網路隔離
執行矯正程序
Network、Endpoint 聯防

內建偵測規則即時監控未知攻擊



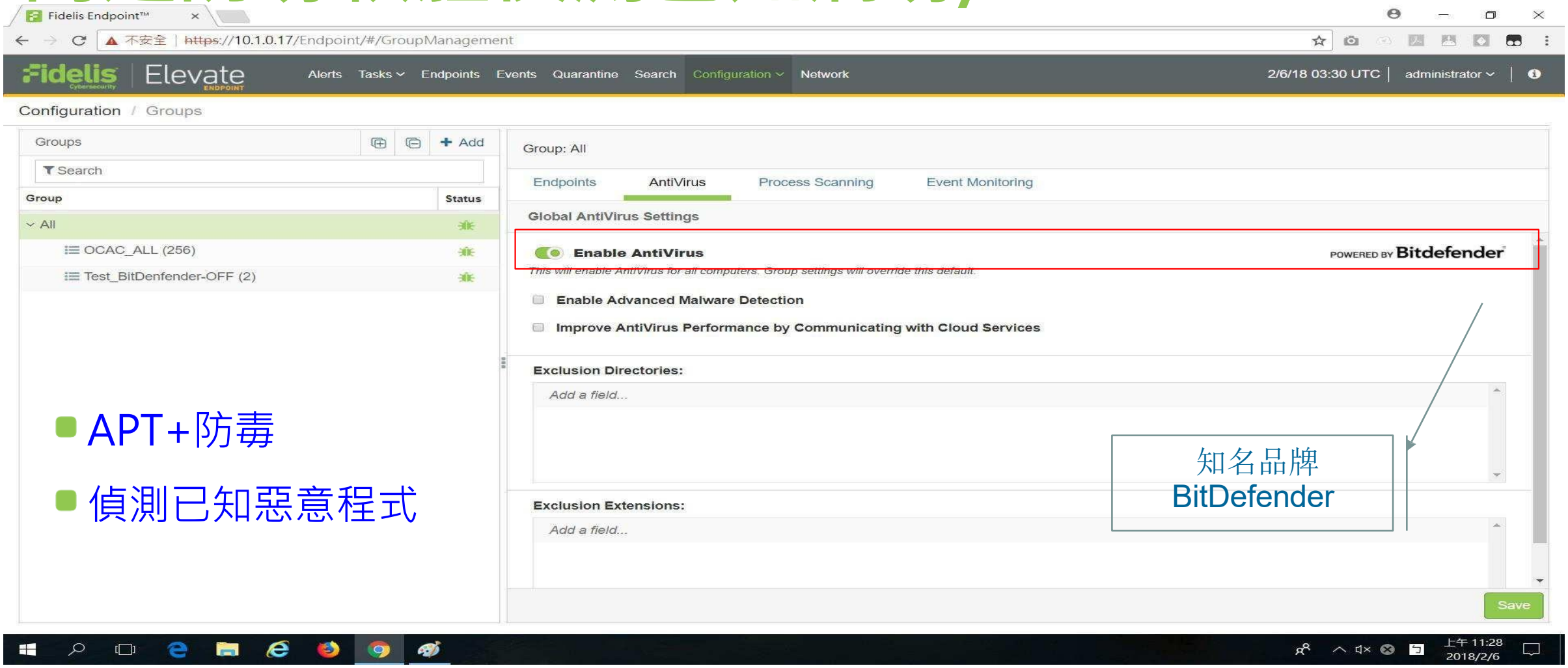
- Detection Rule內建超過600類型的規則，即時在端點進行偵測與保護
- 偵測MITRE攻擊行為類型、CVE弱點和Microsoft KB
- 針對多種駭客攻擊手法進行檢測
  - Powershell無檔案攻擊
  - Phishing等傳統滲透手法
  - 系統防火牆/目錄/檔案/機碼等異常行為
  - 已知APT攻擊手法
- 可測試未知勒索軟體行為並阻擋執行

加入多種情資與特徵碼偵測



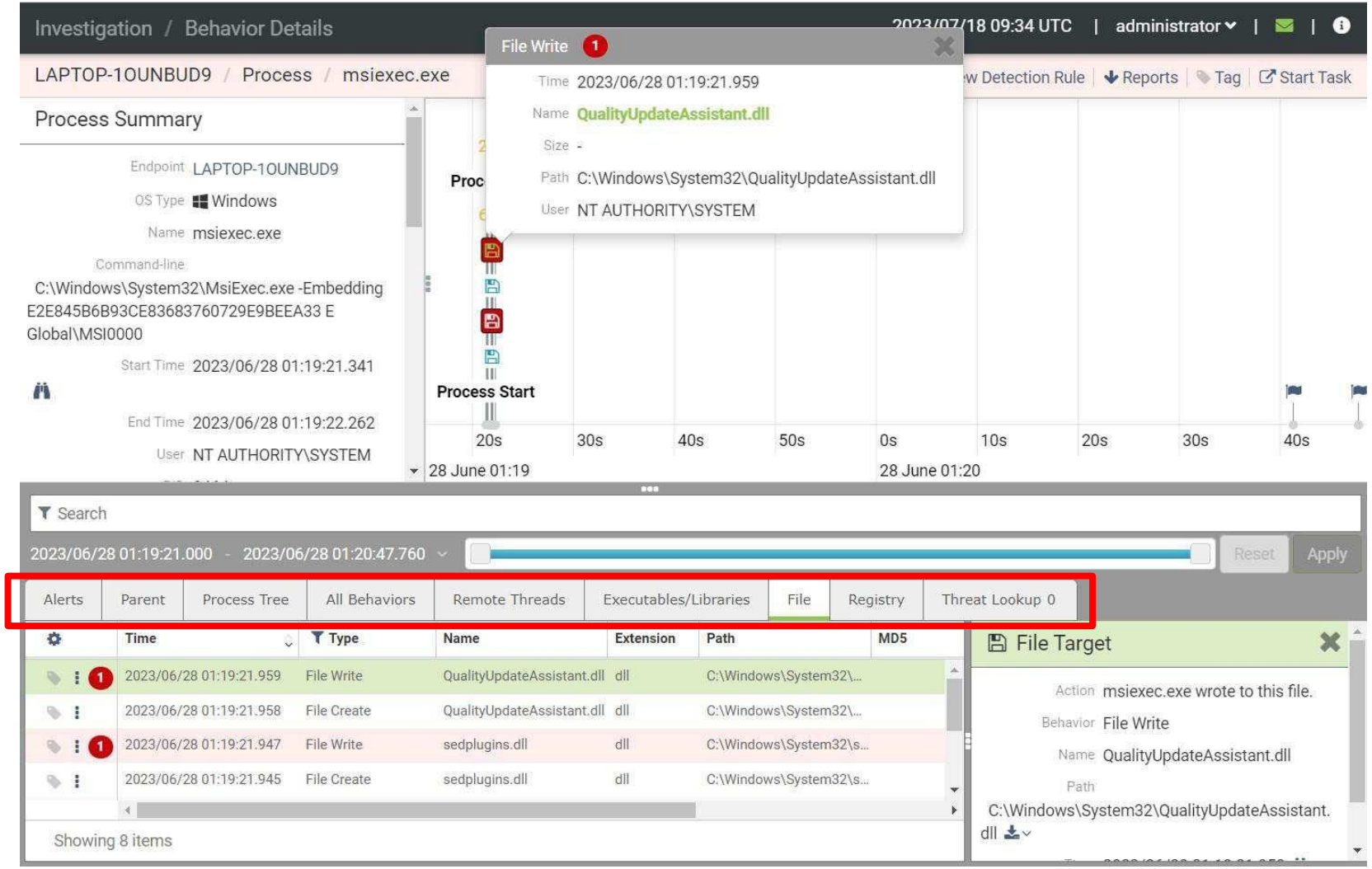
- 定期自動更新
- 包含確認Malware的資料庫
- 可疑檔案的資料庫
- 黑名單URL
- 沙箱驗證判定為惡意的可執行物件

內建防毒軟體偵測已知病毒/APT



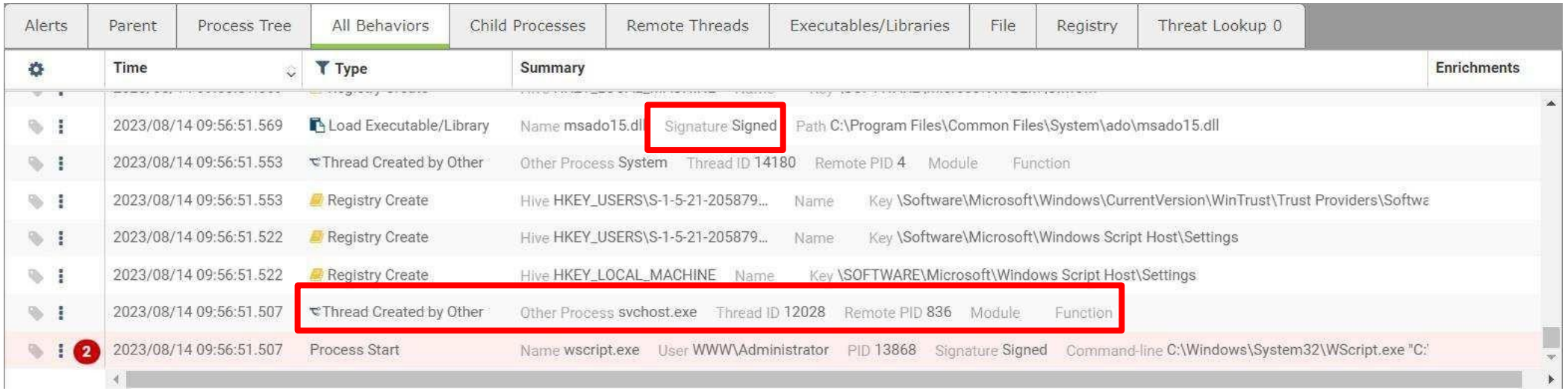
- APT+防毒
- 偵測已知惡意程式

告警自動匯整本次攻擊所有事件



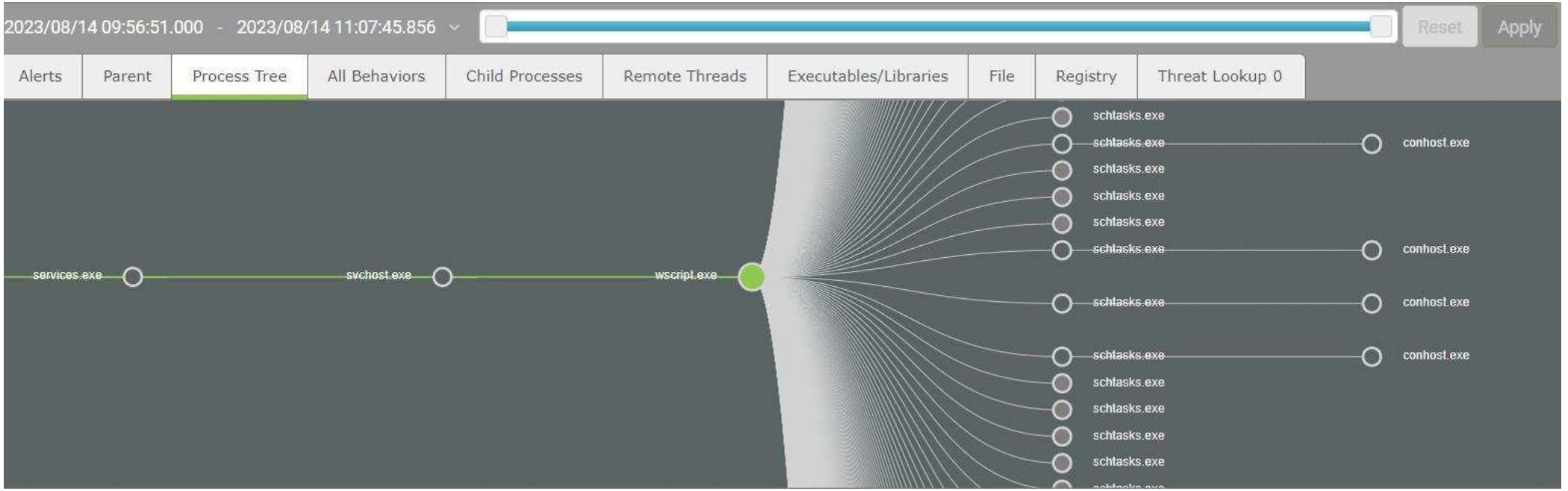
- 每個告警均自動繪出程序流程圖
- 自動收集各類型細節
  - 父程序與子程序 行
  - 為動作
  - 遠端連線
  - 使用到的檔案、機 碼
- 自動至第三方檢查雲端分數

所有的動作紀錄在All Behaviors內



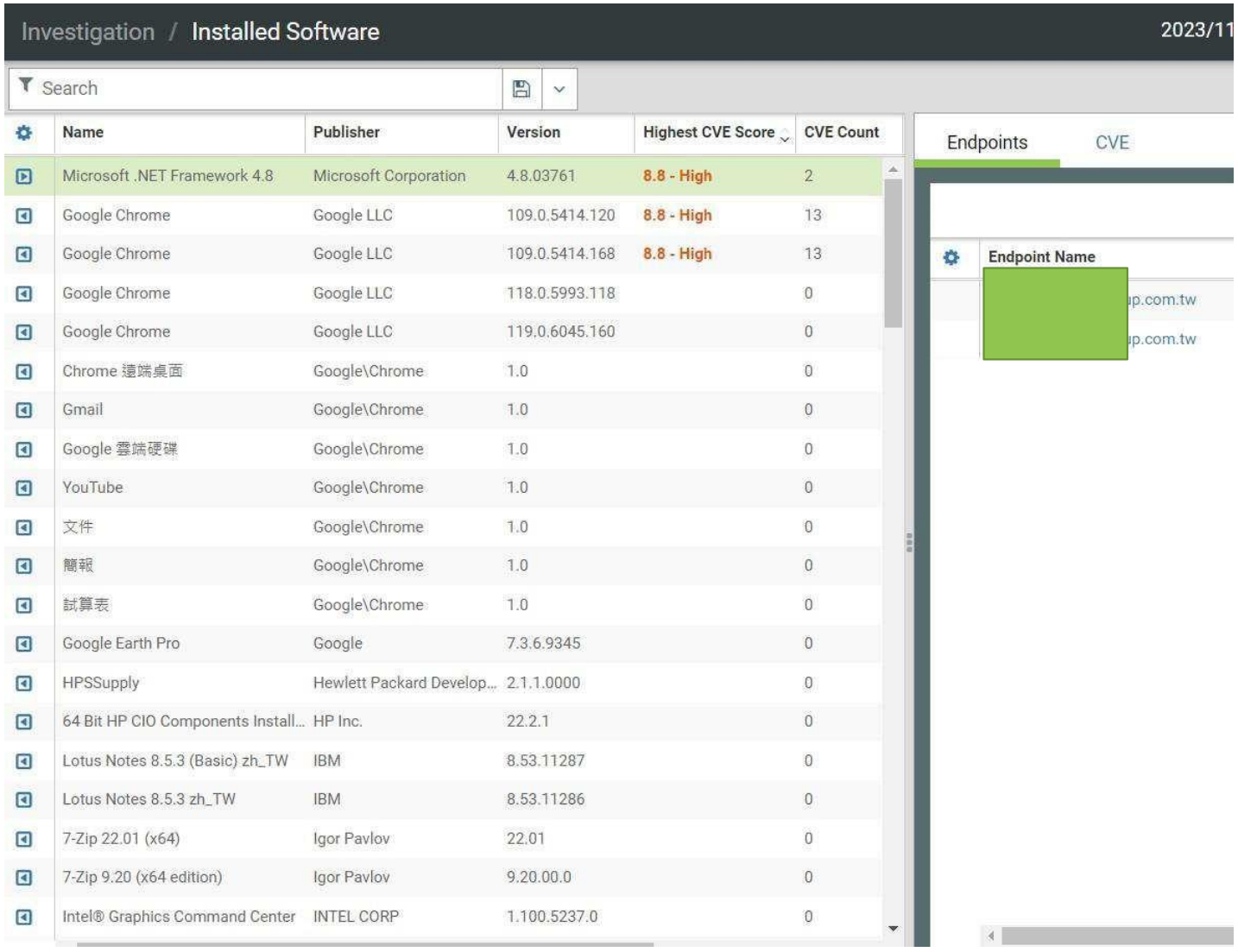
- 在All Behaviors的頁面中，依時間順序紀錄所有的惡意行為
- 被額外呼叫的程序也會進行合法憑證的檢查
- 事件紀錄的時間單位到1/1000秒，可精確分辨出每個動作的先後順序

圖像化執行緒分析



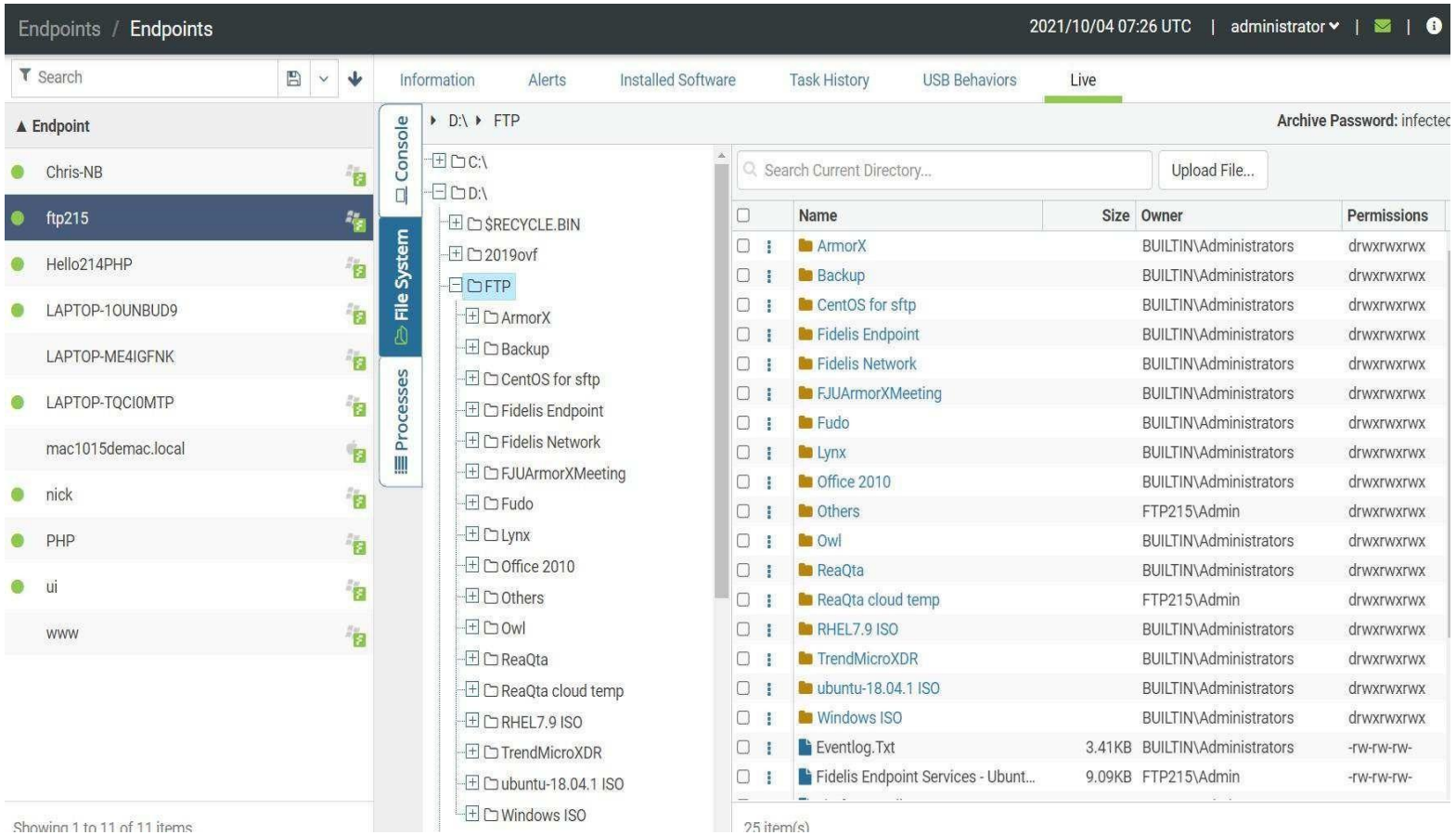
- 告警觸發的執行緒，會將該執行緒的父程序及子程序以樹狀圖表示
- 方便追踪來源

管理所有端點安裝的軟體



- 自動收集端點上所有安裝的軟體
- 比對版本並檢查是否有CVE漏洞
- 以風險值分數來區分重要性
- 匯整相關端點數量
- 可在主控台直接uninstall端點的安裝軟體

可直接端點操作

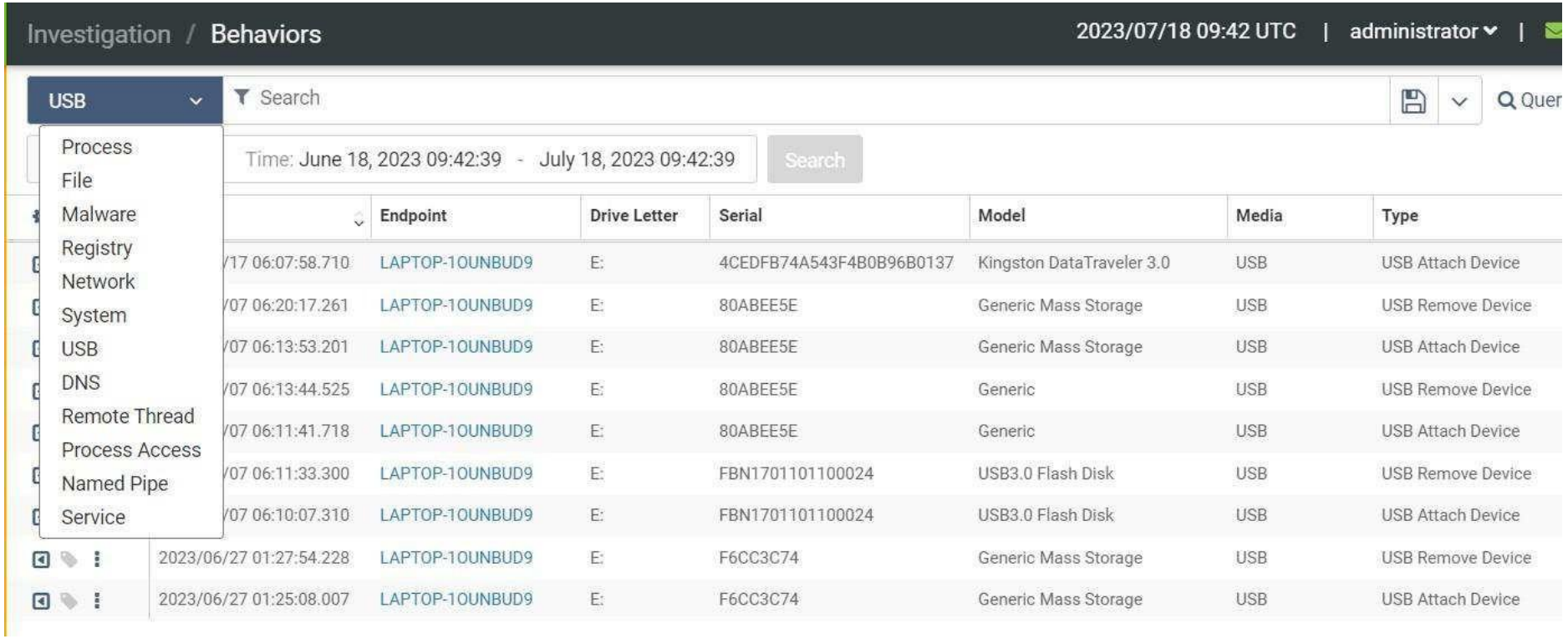


- 只要端點是上線狀態，就可以從主控台進行端點直接操作
- 可進行的操作有：
  - 檔案上傳/下載
  - 複製/剪下/貼上
  - 刪除/移動
- 可直接開啟命令列 (Windows Command Line)

系統管理功能可執行更複雜的作業

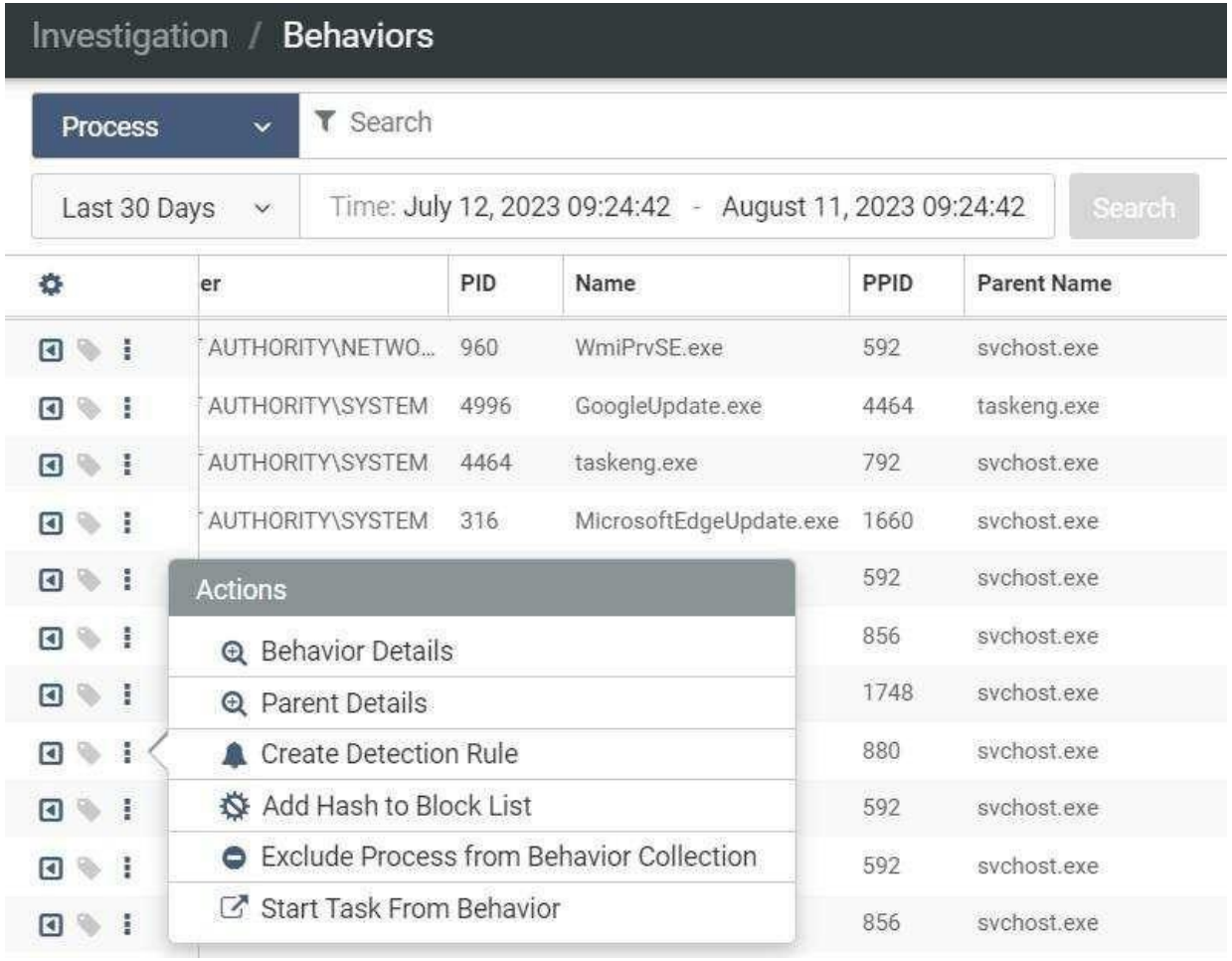
- 取回指定檔案
- 搜尋特定檔案
- 清除指定檔案
- 目前執行中程序列表
- 清除指定程序
- 防毒軟體狀態端
- 端點防火牆規則
- 端點所有帳號
- 目前網路連線
- 目前service狀態
- 還原Windows restore point
- CPU loading
- 硬體資訊
- USB drive狀態
- 登入成功/失敗紀錄
- 瀏覽器歷史紀錄
- 無線網路連線紀錄
- 記憶體分析
- 搜尋指定機碼
- CVE弱點報告
- IOC掃瞄
- .....

鑑識工具



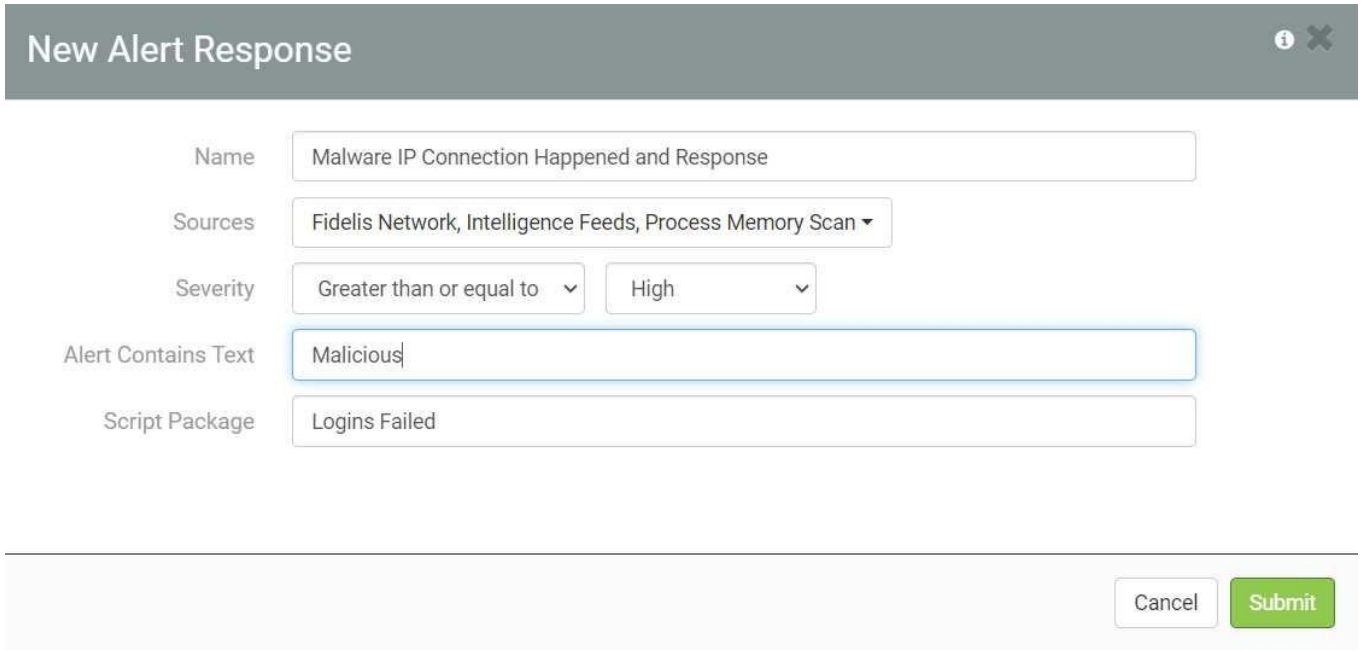
- 端點行為包含：程序動作、檔案開啟或修改或刪除、惡意程式、機碼變更、 網路連線、作業系統事 件 、 USB插 拔 、 DNS查詢等十餘種類別
- 可查詢到所有端點上發生的事件

查詢到事件後續處理



- 建立自定義Detection Rule，未來發生相同事件就會產生告警
- 直接加黑名單，阻擋下次執行
- 直接加白名單，下次相同事件不再紀錄
- 設定自動反應，當發生特定狀況時指定進行特定工作

設定自動反應作業



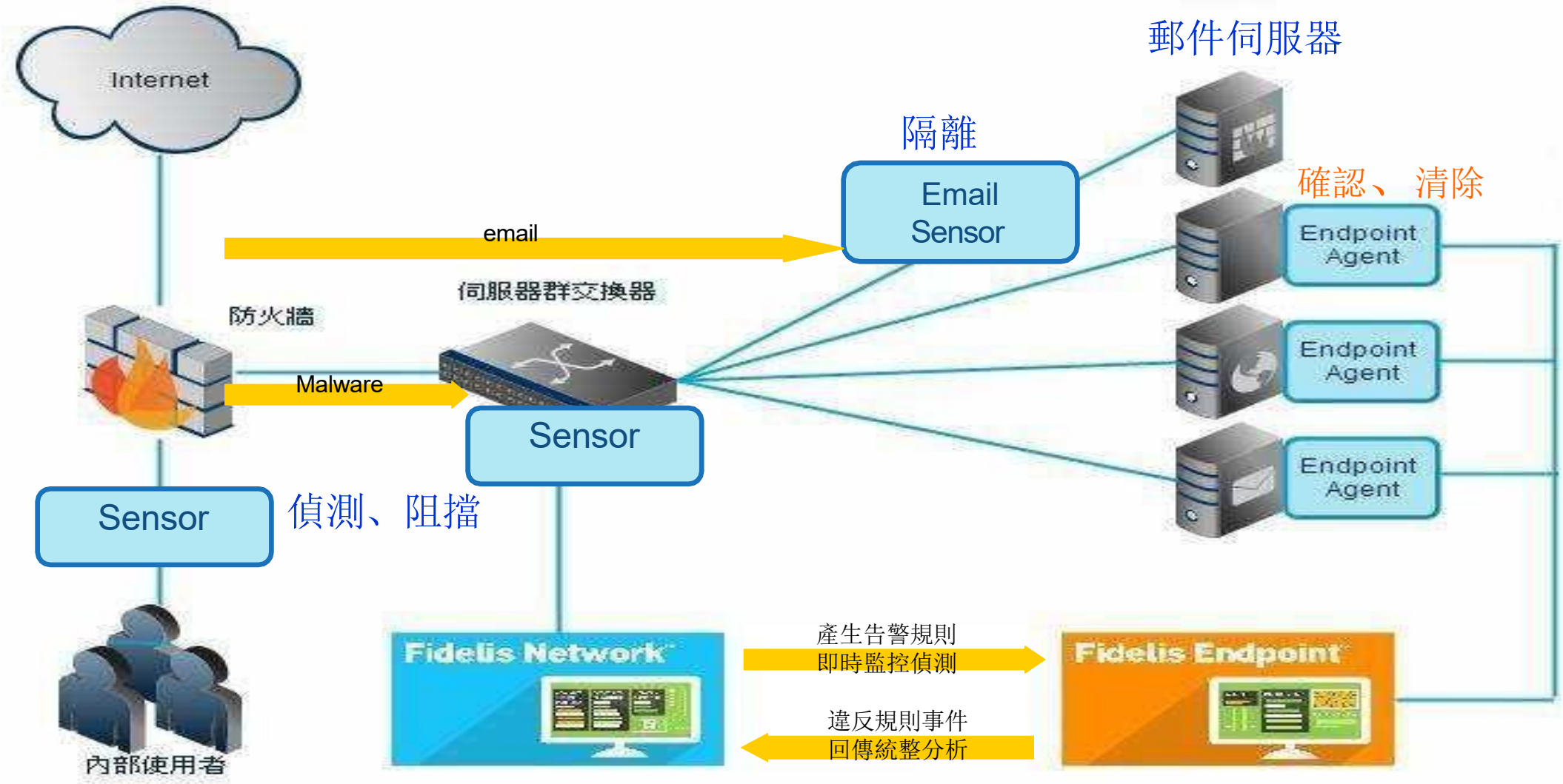
- 依據告警的類型以及所含的文字敘述，自動執行指定的工作
- 例如：
  - 當發生與惡意IP連線的行為，就自動搜尋登入失敗紀錄，查詢是否被猜密碼
- 預設工作(Task)有150+含各種平台，可自行建立新工作

可支援Windows Linux Mac等不同OS平台

OS	Version	Information	
Windows	Windows Server 2016、2019 Windows 10 Windows 11	Supports 64-bit Supports Behavior Monitoring Supports Antivirus	
Linux	Kernel 3 + CentOS 6, 7 Red Hat Enterprise Linux 6, 7, 8 Ubuntu 14.04, 16.04,18.04, 20.04, 22.04 SUSE Linux Enterprise Desktop 15 Amazon Linux 2017.03 and 2017.09, 2018.03, 2	Supports 64-bit Supports Behavior Monitoring Supports Antivirus (scheduled scan only)	
MacOS	macOS X 10.15 Catalina macOS 11 Big Sur macOS 12 Monterey	Supports Antivirus (scheduled scan only)	

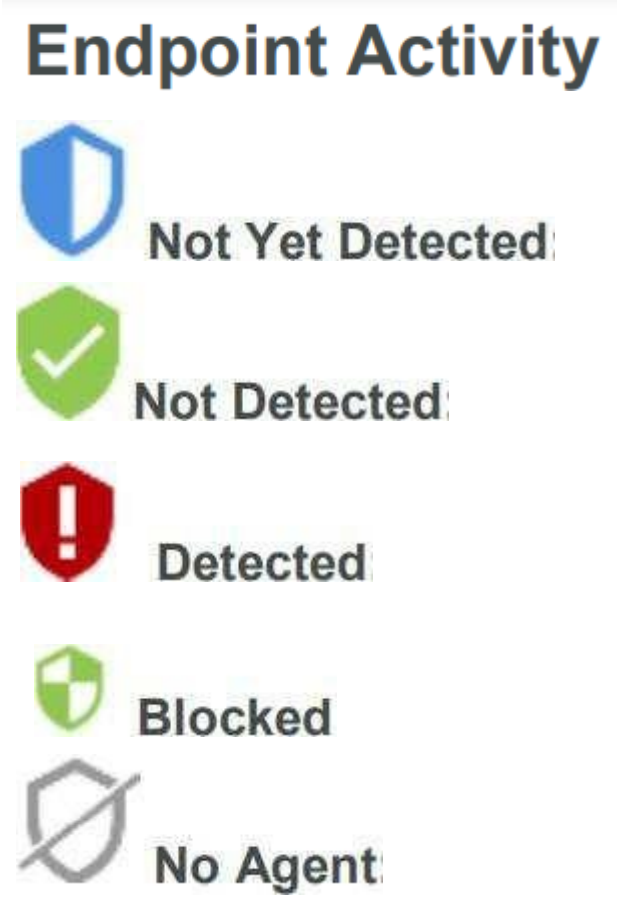
聯防防禦架構

Fidelis聯防系統架構



Network與Endpoint協防

- 增加防禦縱深
- 事件綜合匯整
- 自動建立檢查規則
- 自動回報攻擊確認
- 威脅情資共享
- 單一操作介面



Deception與Endpoint/Network的聯防

- Deception誘捕系統運作原理
  - Network收集網內的網段架構
  - 端點/伺服器的服務
  - 自動佈署相同的誘餌端點來引誘駭客入侵
- Deception資料均匯整於Network介面，單一平台統合
- Endpoint/Network發現疑端點被入侵，Deception提供確認是否被compromise
- 改善告警正確率

總結

結語

- Endpoint-最強端點管理能力清除
  - 能力最強
  - CP值最佳(內建防毒軟體)
  - 支援最多種平台(Win、Linux、Mac)
  - 調查速度最快(事件集中式管理)
  - 防禦縱深最長(整合Network協同作業)
  - 可阻止勒索軟體

Thank you