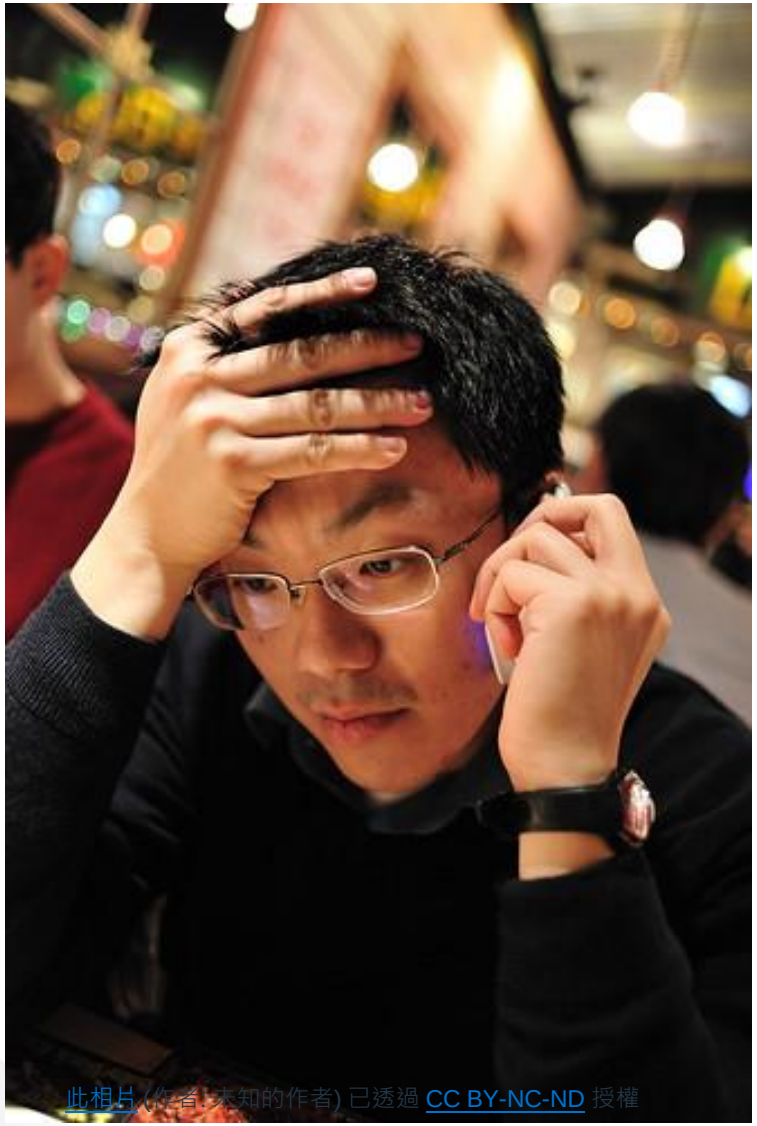
資安攻防終極戰 - 端點偵測與回應

Marty 張益盛
mchang@fortinet.com

苦 命 的 MIS



老闆的電腦又中毒了.....

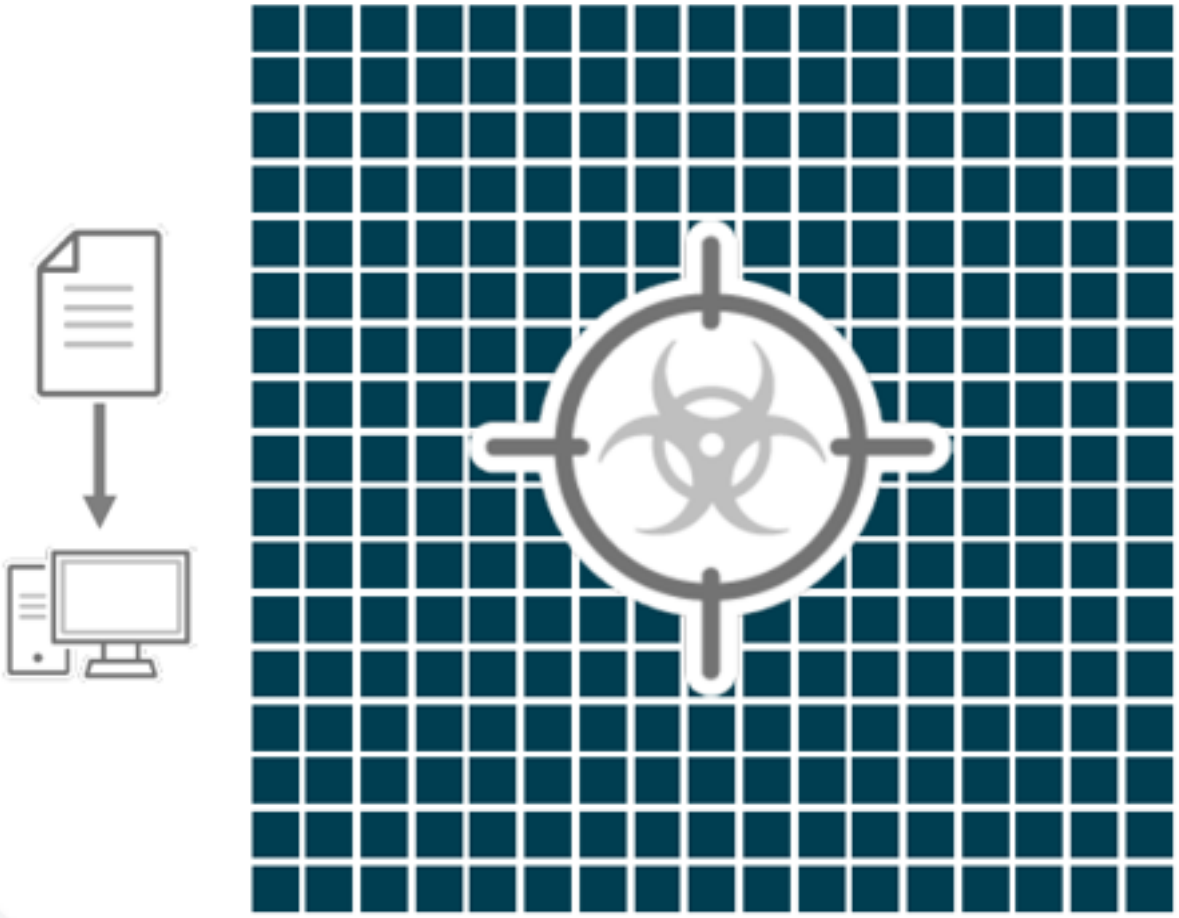
叫他不要上有的沒有的網站,就是不聽!!

這次更慘了,中了勒索病毒 !!

付 錢 < > 重 灌 ??

病毒防範的演進與攻防

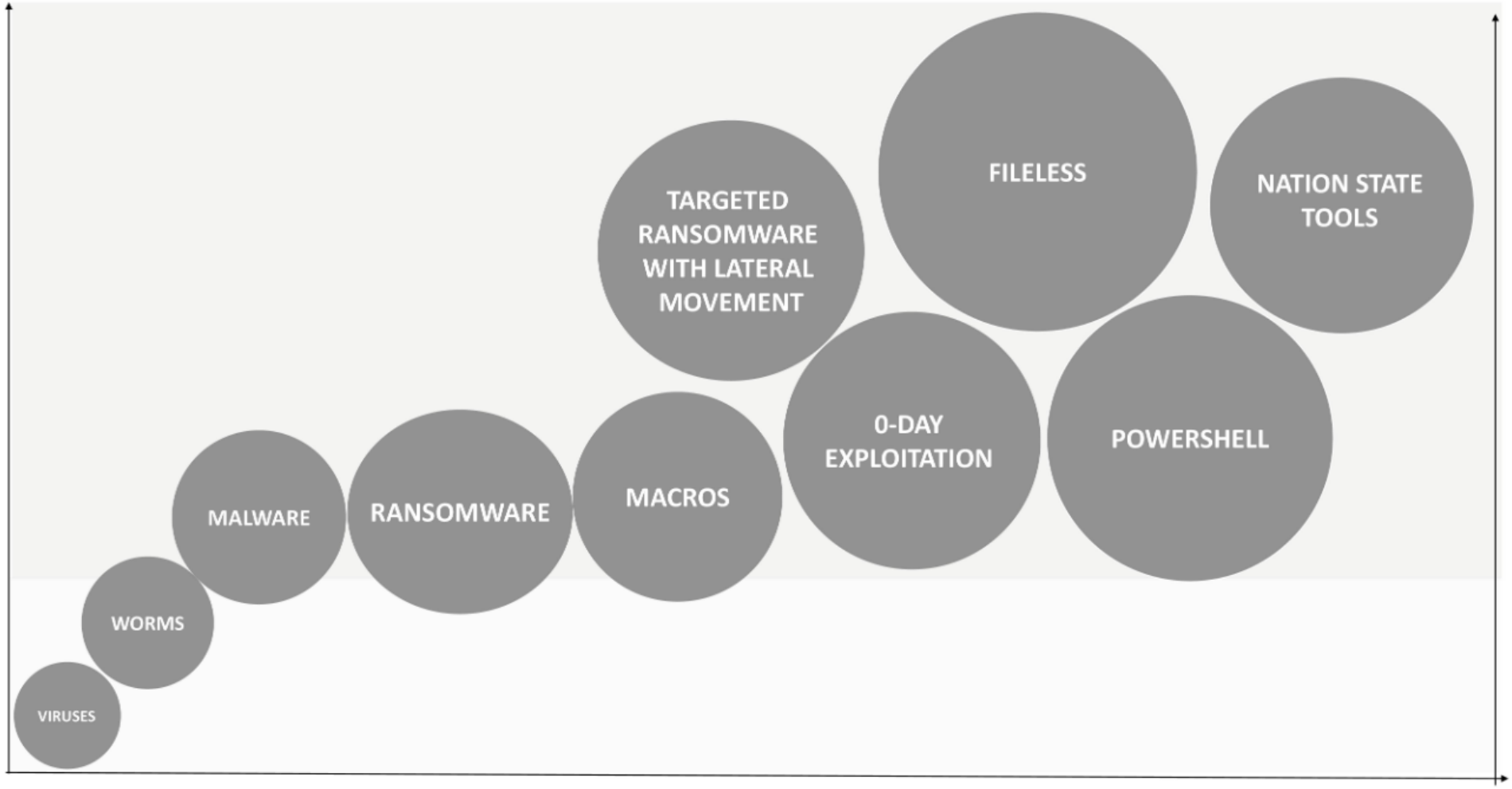
Last Decade: Rise of Machine Learning



引進機器學習防護

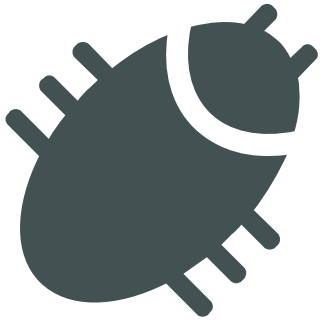
(Very) Simplified Machine Learning Model

惡意軟體的演進與資安產品的因應之道

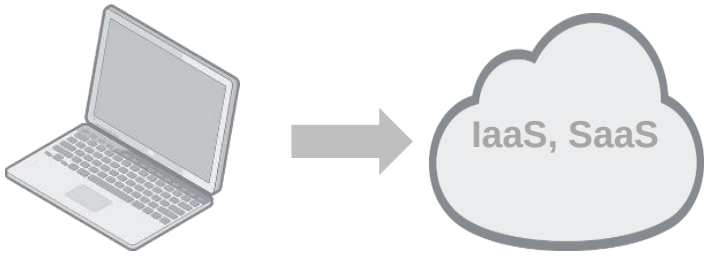


端點防護的挑戰

威脅層面
與日俱進



系統弱點
不斷暴露



雲端應用
規避檢測

Gartner®

The security mindset has shifted to acknowledge that prevention alone is not enough; security and risk management leaders must be able to more easily harden endpoints and perform more detailed incident response to resolve alerts.

Notes/Sources:

1. Gartner Magic Quadrat for Endpoint Protection Platforms, August 2019.

資安人員痛苦之處—四大難題

1. 遭受病毒感染或被加密的電腦

- 是否有100%的保護機制
- 資安威脅面向 – 勒索病毒, 資料竊取,營運中斷威脅
- 需要更好的偵測產品以及具備快速修復功能

2.資安事件的處理方式– 價位,災難復原所需的時間考量

- 想要建構一個沒有資安威脅的環境,價位是否可以負擔的起?
- 告警轟炸時,如何減少誤判
- 修復工具是否簡易使用,是否需要手動介入
- 是否有效降低公司營運中斷時間,是否需要長時間的系統回復,減少使用者抱怨

3.缺乏專業的資安人員,受限於有限的資安與網管工具

- 需要強化公司的資訊安全監控中心功能
- 需要擴建資訊安全監控中心的廣度
- 缺乏時間可以對所有設備做系統漏洞的修復或系統的更新

4.複雜的資安系統,缺乏完整的資安解決方案

- 需要一套完整的資安整合方案

端點防護需要的是:　事前防範 VS 事後保護？

- **事前防範 = EPP(防毒軟體)**

  資安工具,惡意軟體的過濾

- **事後保護 = EDR (偵測與回應)**

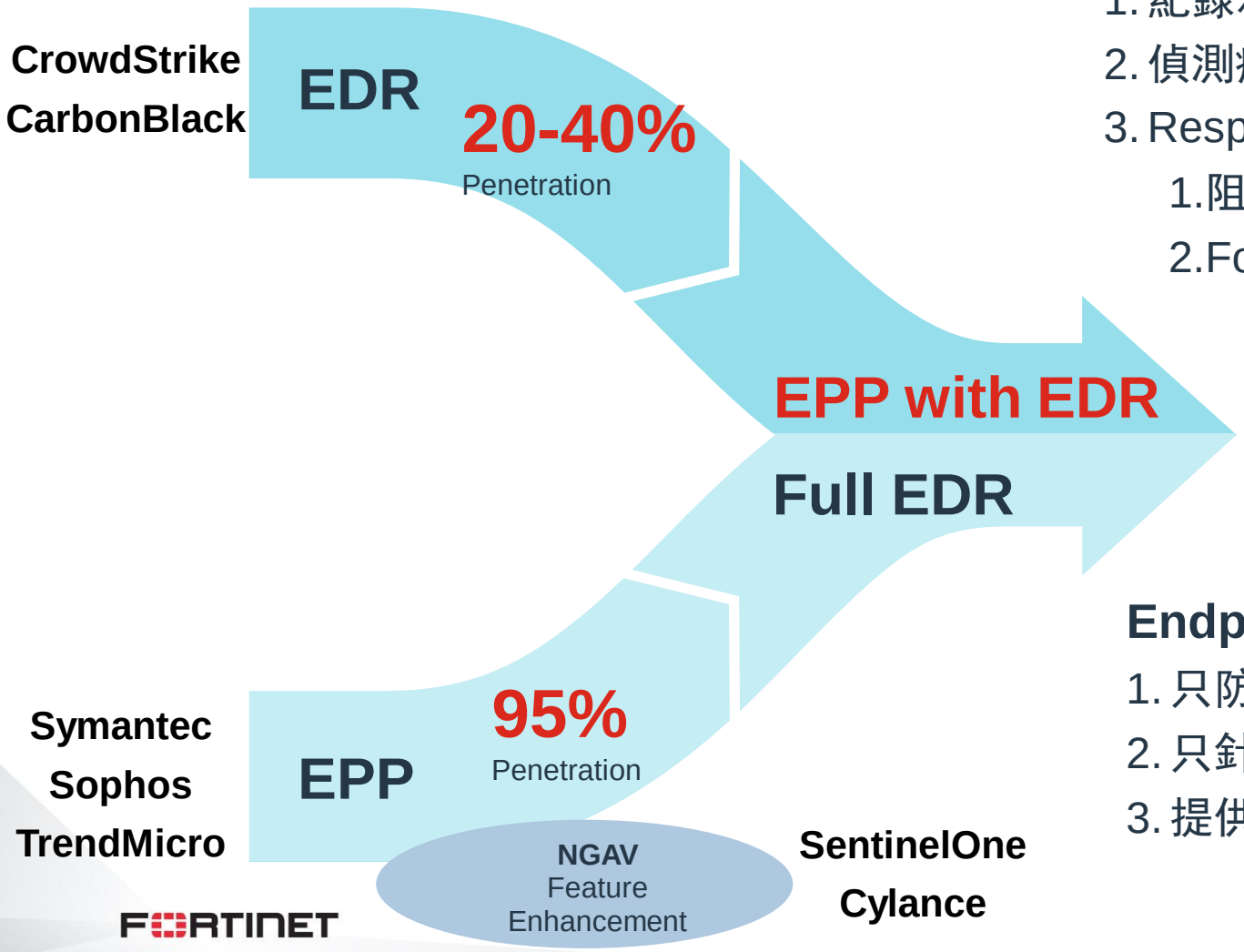
  記錄使用者的行為軌跡,偵測與回應異常行為

防 毒 軟 體
防毒引擎 (AV)
端點防火牆
應用程式控管 (伺服器)
網頁過濾
通訊埠與設備控管
弱點與補釘管理

EDR 偵 測 與 回 應 防 護
行為模型建立
惡意軟體遏制功能
使用者行為軌跡紀錄,提供日後稽核
系統回復機制

Source: Gartner. Critical Capabilities for Endpoint Protection Platforms. October 2019. and Gartner Market Definition for Endpoint Detection and Response Tools

端點防護的發展 ---- 特徵值比對 VS 行為模式分析



Endpoint Detection and Response (EDR)

1. 紀錄和儲存所有 endpoint 的行為
2. 偵測病毒事件
3. Response
   1. 阻止病毒和修復
   2. Forensic—偵查資安事件，並找尋其源頭

FortiEDR整合兩種防護機制

Endpoint Protection Platform (EPP)

1. 只防範 file-based 病毒
2. 只針對不信任的應用程式偵測和阻攔惡意的行為
3. 提供偵查及修復病毒能力，並且通報和告警

FORTINET

手動方式EDR vs 自動化EDR

手動方式
第一代 EDR

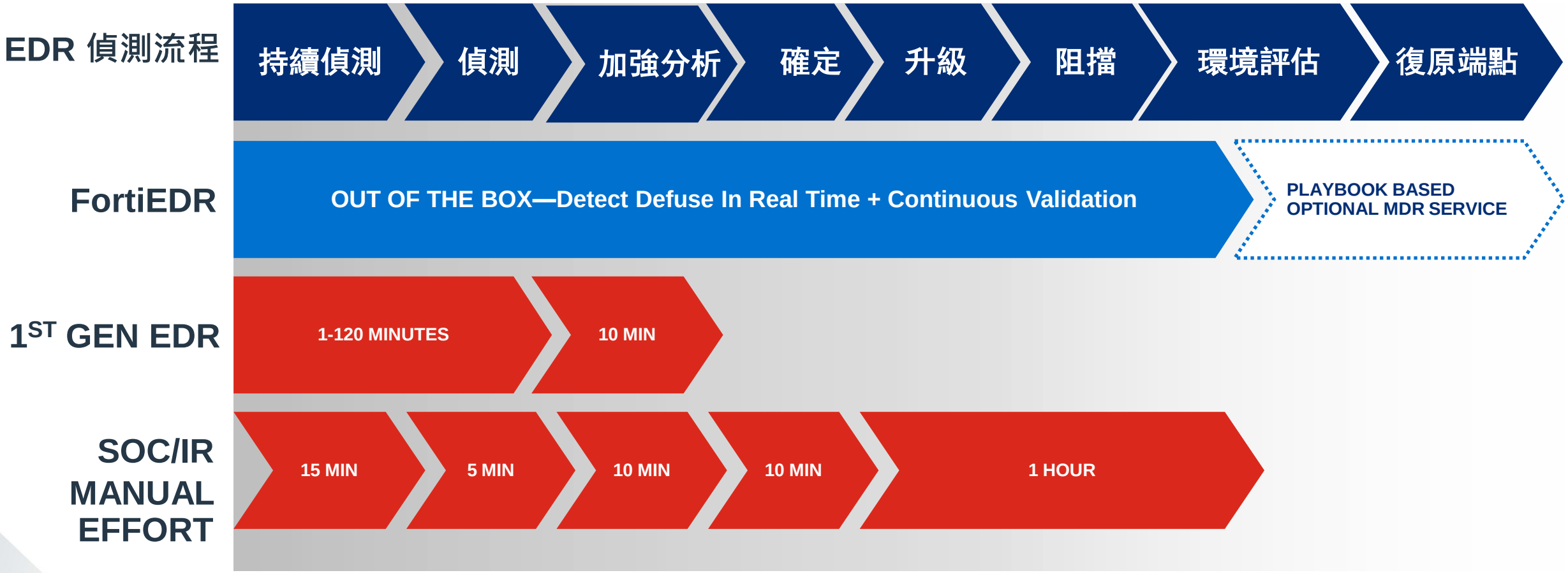
- 反應時間?
- 手動阻擋
- 系統重灌?
- 告警轟炸

vs

自動但不確實

- 誤判?
- 缺乏彈性 – 端點隔離
- 系統離線?
- 公司營運中斷

FortiEDR 自動化 vs. 手動方式 EDR



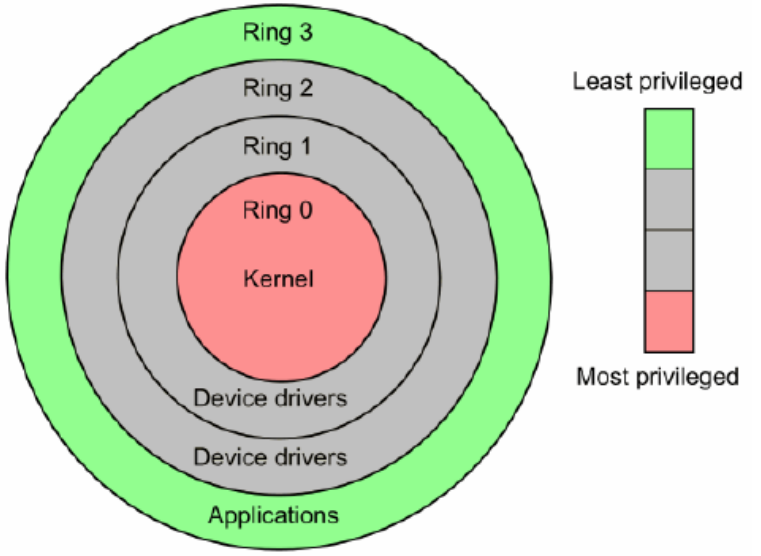
什麼是 FortiEDR—勒索病毒的終結者

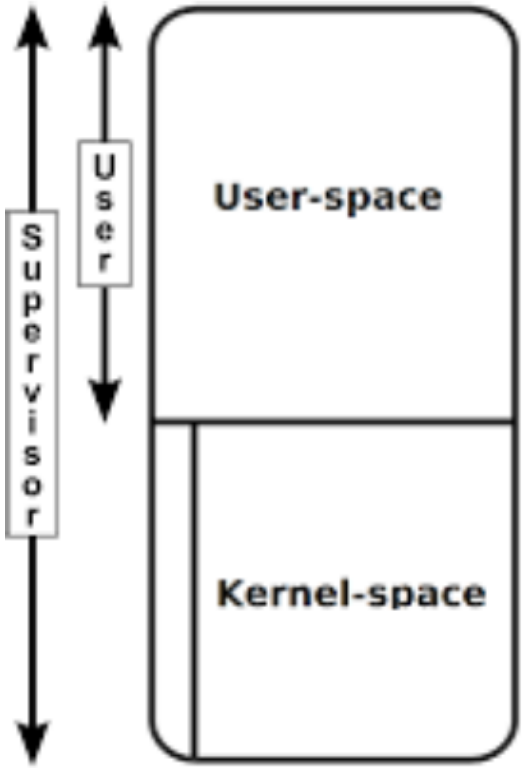
提供次世代防毒機制功能並且整合惡意軟體的偵測與回應功能.自動化腳本定義功能,整合於Fortinet安全織網中

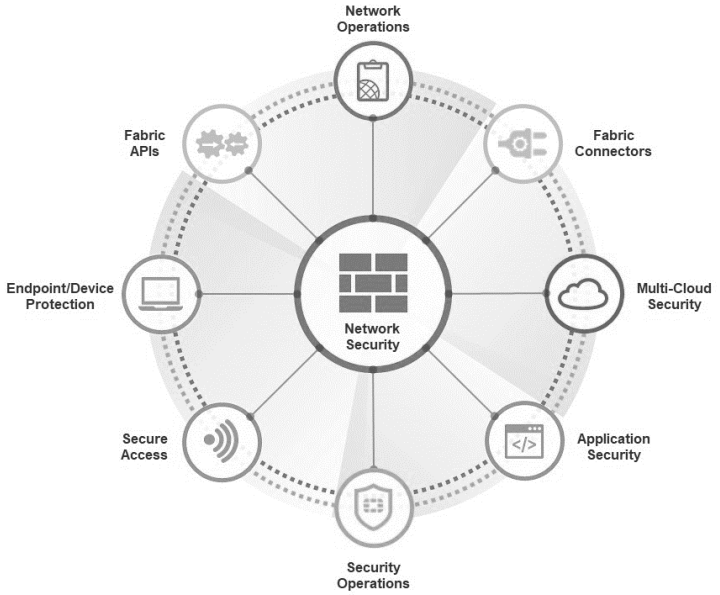
- **名列前茅的次世代端點保護產品**
  多元的機器學習引擎並獲得 NSS Labs 端點防護產品的推薦名單之中
- **以行為分析基礎為出發點的EDR產品**
  端點行為軌跡紀錄與分析,監測任何可疑的行為
- **自動化的框架建構與學習**
  以雲端應用為基礎開發出的深度學習與分析機制,提供資安事件分類與自動化腳本功能.面對資安威脅時,提供全面性的防護

與眾不同的FortiEDR !!

- 運作於作業系統核心,全面性的保護
  - 程式啟動前的防護
  - 檔案滲透防範
  - 勒索病毒防範
- 自動化回復機制 “腳本定義功能”
- 業界系統資源使用率最低
  - 少於 30MB 硬碟安裝空間
  - 少於 120MB 記憶體使用空間
- 高效率的離線保護機制
- Fortinet--安全織網整合







FortiEDR – 即時的事前防範與事後阻擋與復原

事前防範

主動減少威脅

- 主動偵查未授權 IoT 及設備
- 應用程式評估
- 弱點分析
- 風險等級制的策略
- 虛擬補丁

Pre-攻擊防護

- 系統核心層面防護
- 機器學習--
  不依賴特徵碼
- 應用程式之間溝通防護
- 遏止檔案的外流

事後阻擋與復原

第一時間
偵測病毒

- 不亂通報病毒
- 提供惡意檔案分類
- 顯示 IOC's
- 提供完整的攻擊軌跡

防止檔案
被加密及刪除

- 事後阻擋
- 阻擋對外連線
- 避免檔案遺失
- 避免檔案被滲透及加密

完整可視性

- 客製化事件回應報表
- 減少資安處理時間
- 針對非檔案類型攻擊有記憶體快照功能
- 大幅減少駭客源頭找尋

移除感染

- 系統回復機制
- 移除惡意檔案
- 系統無須重新安裝,確保服務正常
- 支援 REST API output

進階的端點「防護」、「偵測」、「回應」與「預測」

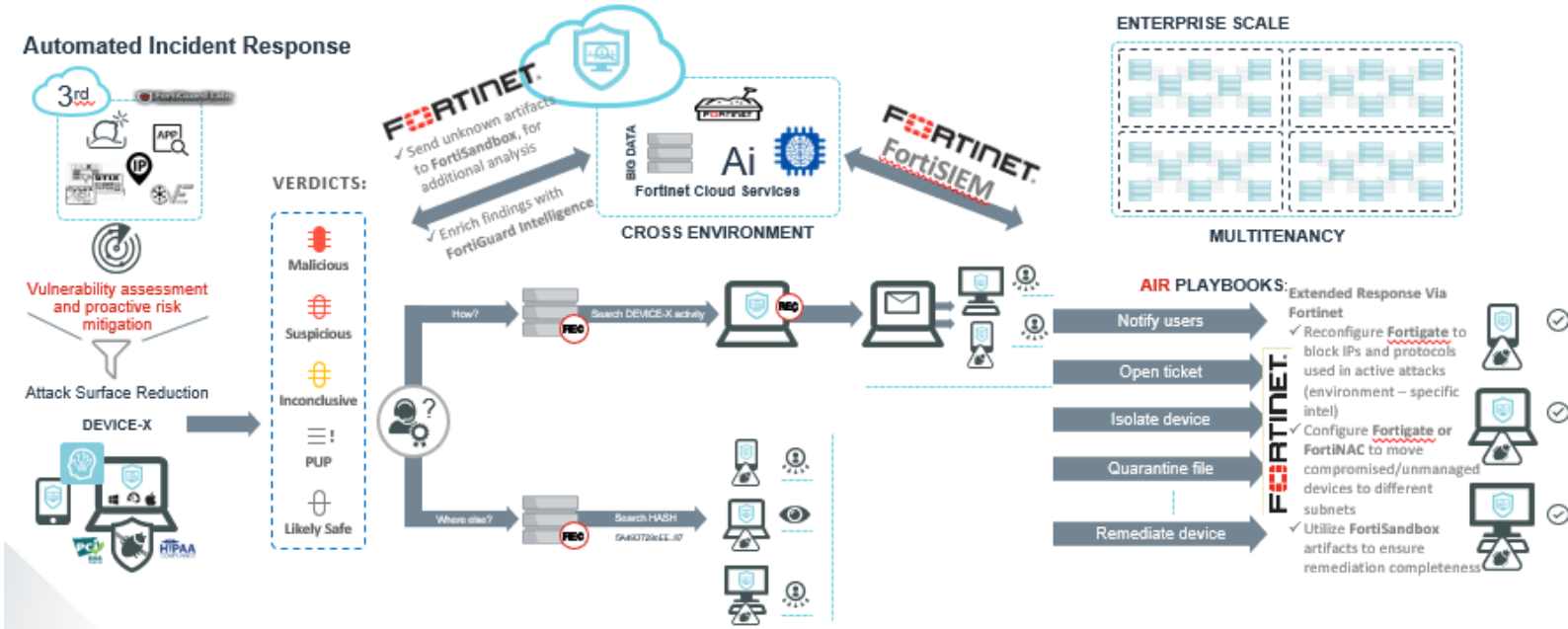
防 護	偵 測	回 應	預 測
檔案類型的病毒 沒有特徵碼的 預防惡意指令的攻擊 偵測和防禦漏洞弱點	針對檔案行為及非檔案 行為的行為模式的偵測	快速回應資安事件 遏制惡意事件 回覆機制 偵查機制 MDR 服務 [可選擇]	找出潛在的 威脅來源
完整保護 • 事前的防範與 事後的保護	*自動解除資安危脅* • 避免勒索病毒的迫害 • 持續不斷的偵測與分 析營運不中斷	*自動化回應與系統回復* • 腳本化的應對機制 • 記憶體快照功能,提供 日後稽核與調查	*避免危害的發生* • 找出非法的設備 與IoT設備的威脅 • 虛擬補釘功能

FortiEDR

Fortinet 安全織網整合效益

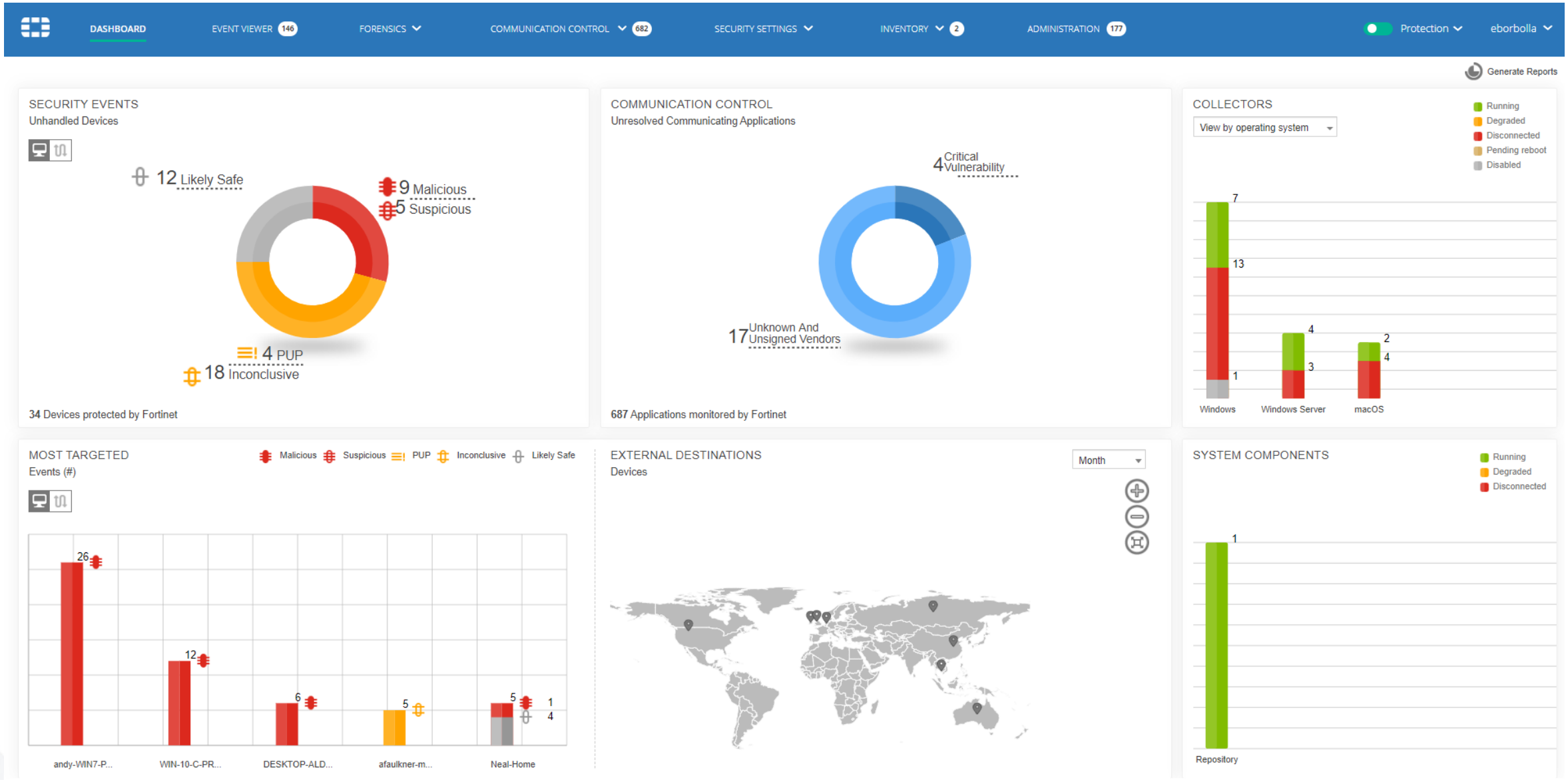
現階段整合產品及功能

- FortiGate
  - 資安威脅情資分享
    惡意檔案內容,目的IP
- FortiSIEM – 雙向整合
  - 端點告警 → FortiSIEM
    告警分流/ 事件確認
    SIEM → 訊息的傳遞與確認
- FortiSandbox
  - 可疑檔案的分析
    病毒特徵值的共享

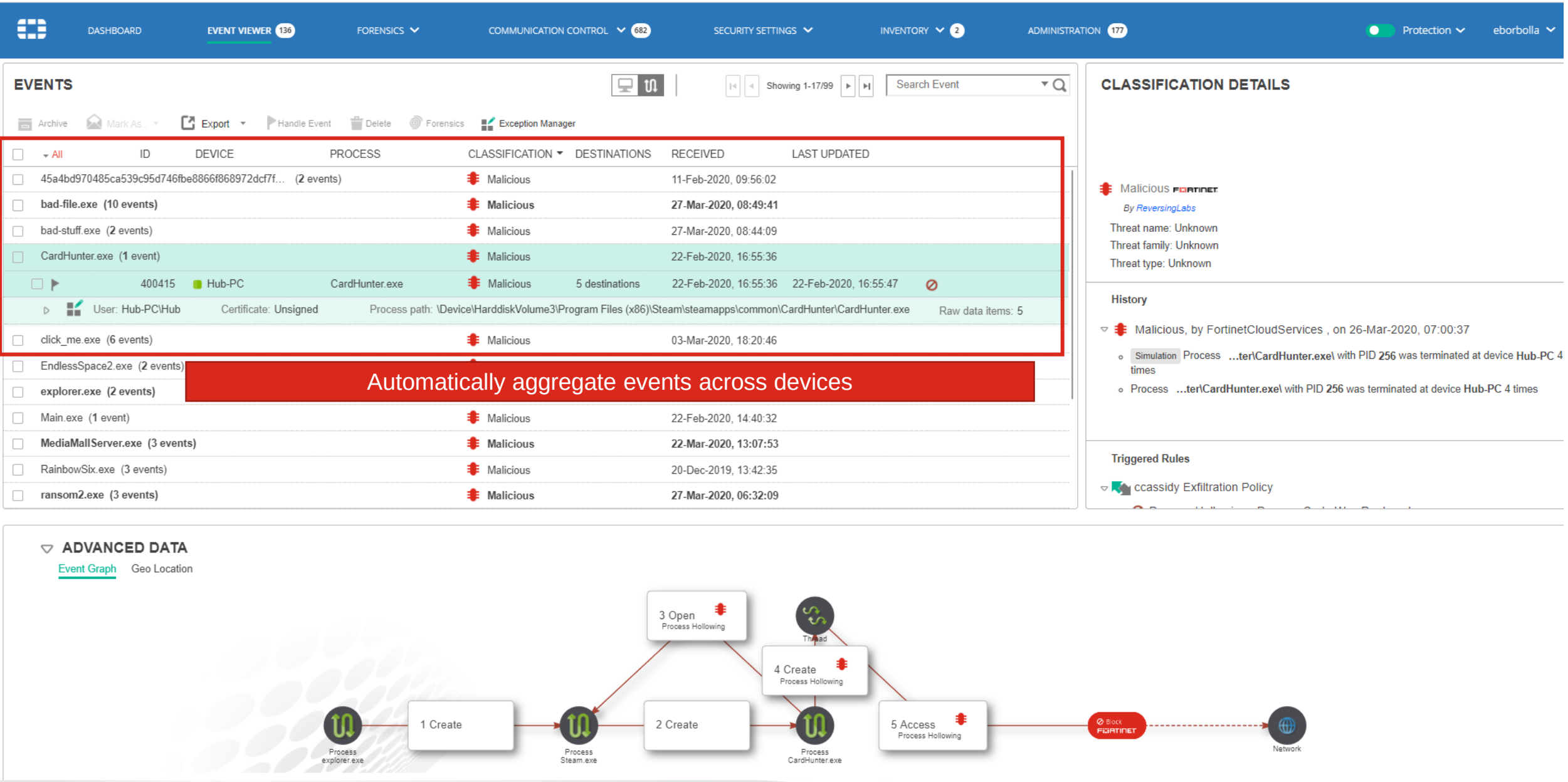


未來整合產品
- FortiNAC
- FortiInsight

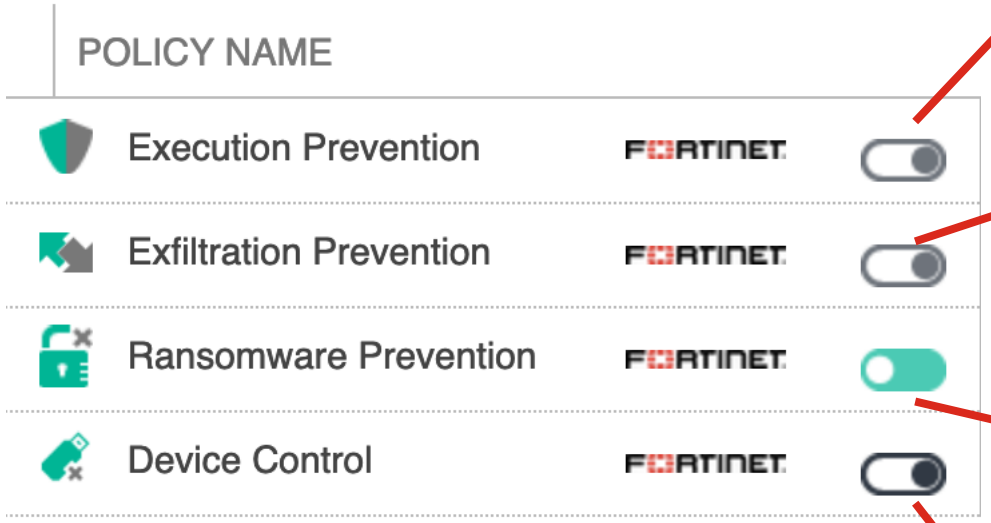
管理介面



資安事件的分類與簡化, 增加 SOC 效用



資安政策的設定與套用



Malicious File Detected	Block
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block
Sandbox Analysis - File was sent to the sandbox for analysis	Log

Access to critical system information	Block
Bruteforce Attempt Detected	Log
Debugged Process - Connection from a Debugged Process	Log

File Encryptor - Suspicious file modification	Block
Hidden Process - Connection Attempt from a Hidden Process	Block
Injected Executable - Connection Attempt from an Injected Executable	Block

USB Application Specific Device Detected	Block
USB Audio Device Detected	Block
USB Audio/Video Device Detected	Block

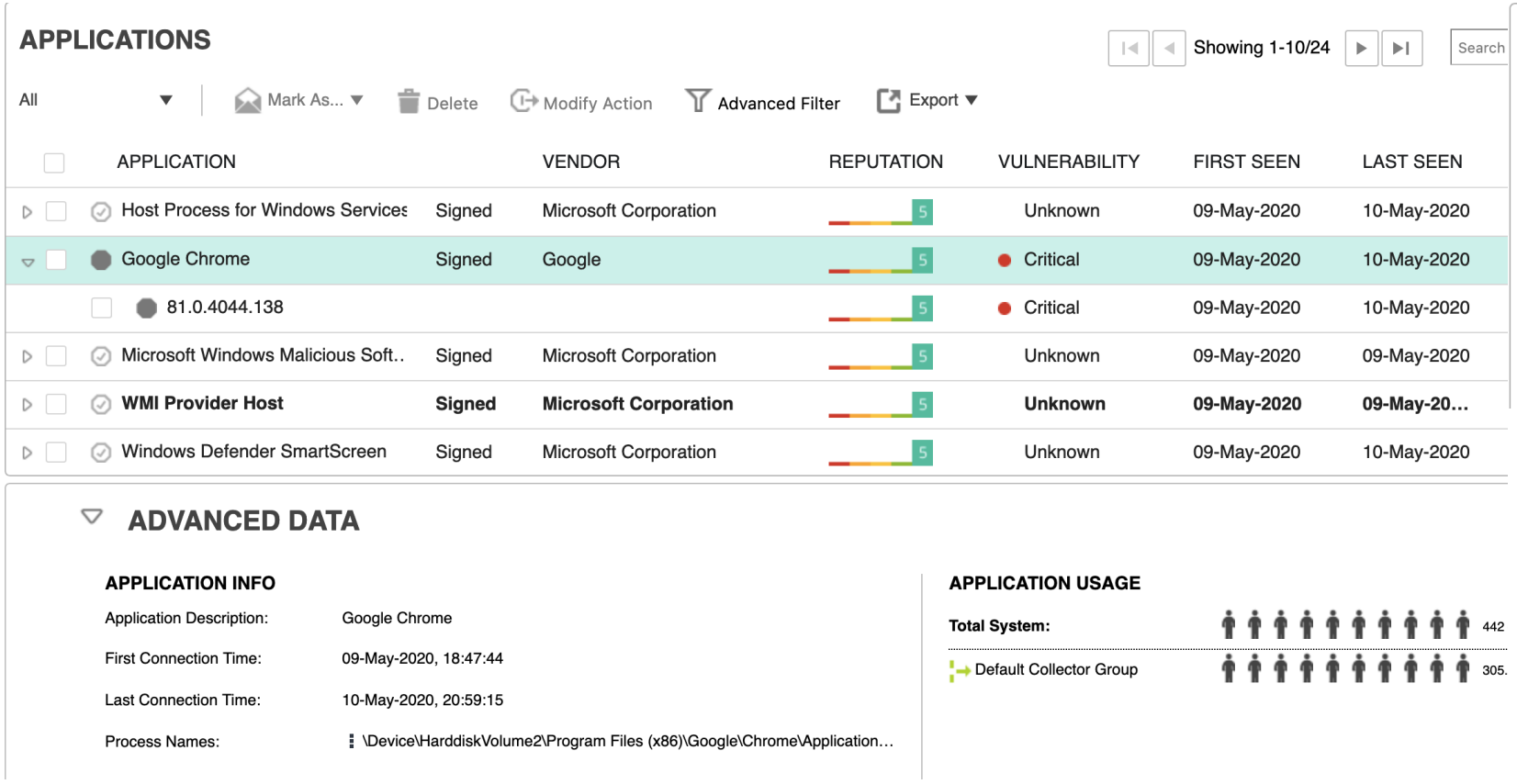
資安事件 —> 腳本化的設定,彈性的處理方式

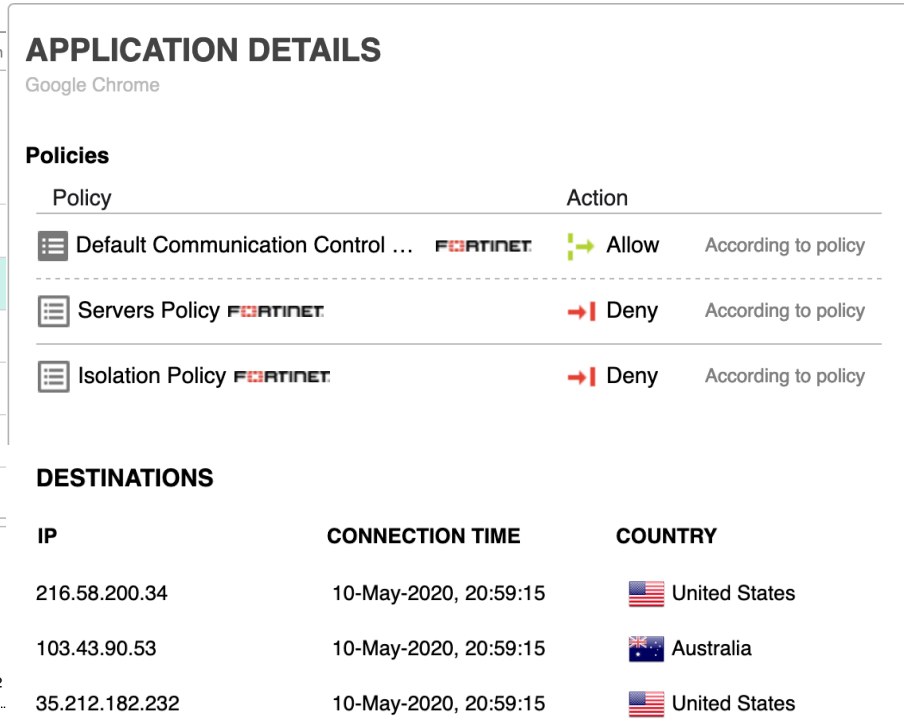
AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook | Set Mode | Assign Collector Group | Delete

NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✔	✔	✔	✔	✔
	Send syslog notification		*Syslog must be defined. Please contact Administrator.*			
	Open ticket		*Open ticket must be defined. Please contact Administrator.*			
INVESTIGATION						
	Isolate device	☐	☐	☐	☐	☐
	Move device to the High Security group	☐	☐	☐	☐	☐
REMEDIATION						
	Terminate process	✔	☐	☐	☐	☐
	Delete file	☐	☐	☐	☐	☐
	Clean persistent data	✔	☐	☐	☐	☐

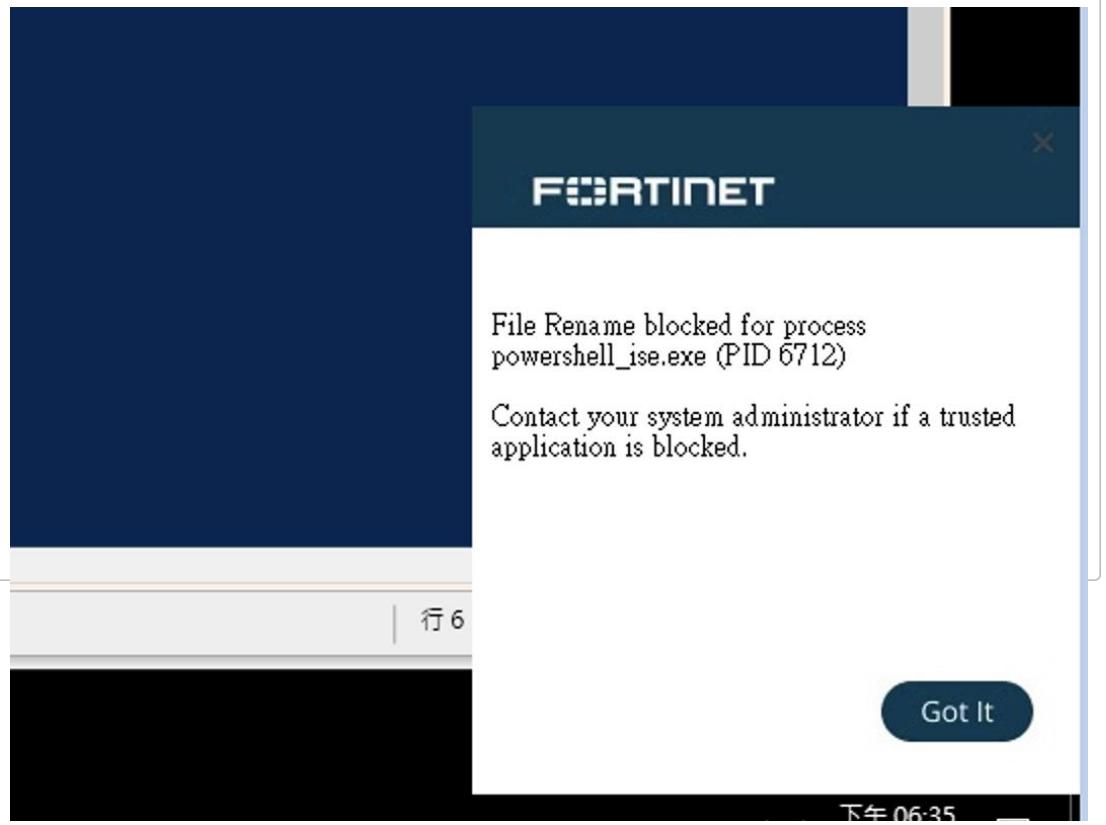
應用程式控管





勒索病毒的偵測與防護

powershell_ise.exe (1 event)			Inconclusive		10-May-2020, 12:35:45		
	882442	DESKTOP-Q3SOD26	powershell_ise.exe	Inconclusive	2 destinations	10-May-2020, 12:35:45	10-May-2020, 12:36:41
User: DESKTOP-Q3SOD26\user		Certificate: Signed	Process path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe		Raw data items: 2		
LE.dll (1 event)			Malicious		10-May-2020, 10:01:19		



Inconclusive FORTINET

By ReversingLabs

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

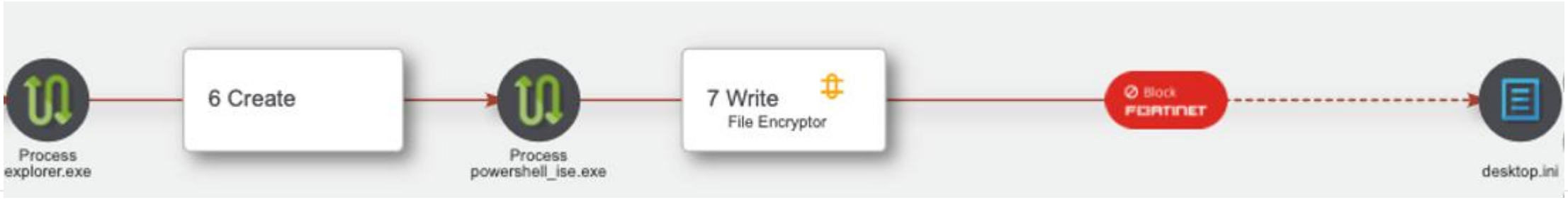
Inconclusive, by Fortinet , on 10-May-2

Triggered Rules

Ransomware Prevention

File Encryptor - Suspicious file modi

勒索病毒的軌跡追蹤



Add Exception | Retrieve | Remediate | Isolate | Export

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAS
DESKTOP-Q3SOD26	Windows 10 Pro	powershell_ise.exe	Suspicious	File Write Access	10-May-2020, 12:35:51	10-M

RAW ID: 152444687 | Process Type: 64 bit | Certificate: Signed | Process Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe | User: DESK

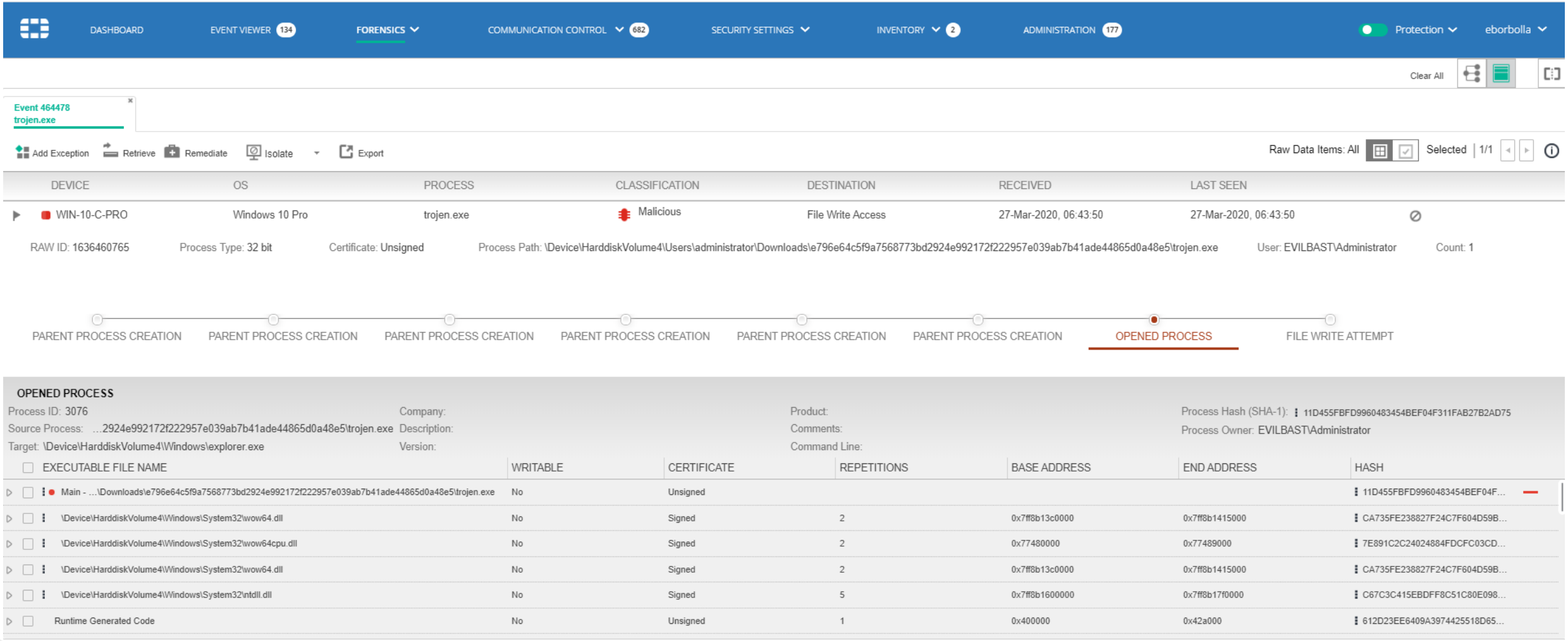
PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION

PARENT PROCESS CREATION

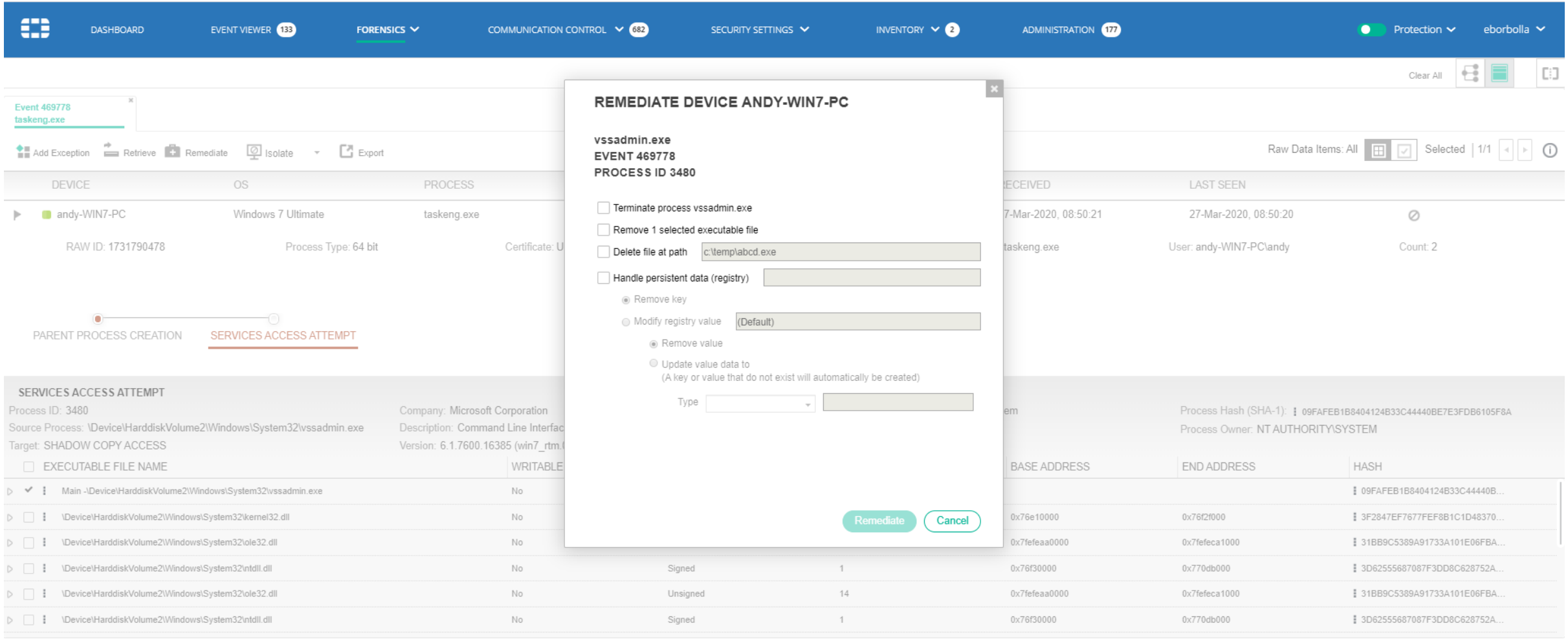
rocess ID: 4156 | Company: Microsoft Corporation | Product: | Proces
ource Process: \Device\HarddiskVolume2\Windows\explorer.exe | Description: | Comments: | Proces
arget: ...Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe | Version: | Command Line:

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END
Main -\Device\HarddiskVolume2\Windows\explorer.exe	No	Signed			

資安事件後續的追蹤與處置

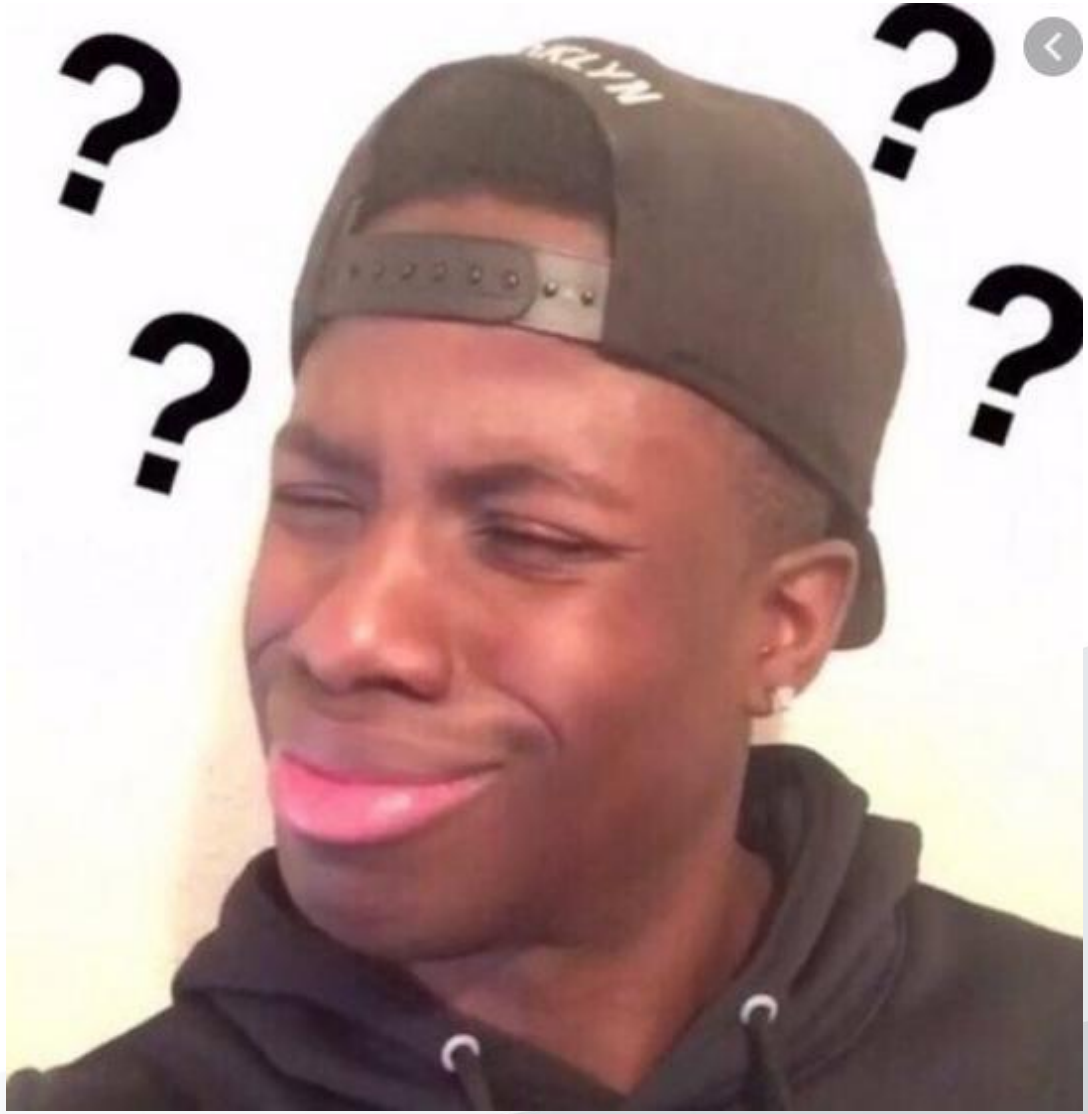


資安事件災害復原



FortiReponse (MDR)

EPP
EDR
勒索病毒
應用程式控管
手動 自動
?????



FortiResponder 團隊

Fortinet 團隊專精於以下：

- 惡意軟件找尋/逆向工程
- 專精多種Script 語言
- 資安事件的調查
- 資安事件的處理
- 中文諮詢服務

FortiResponder 事件分析

Per Incident

Forensics and Incident Response

SOW-based remote forensic analysis and incident response

Ideal for customers running FortiEDR who do not already have continuous monitoring subscriptions

協助客戶針對資安事件：

1. 分　　析
2. 回　　應
3. 遏　　制
4. 回　　復

目標在於大量減少客戶在資安反應時的時間

FortiResponder 服務

FortiResponder 優勢

7 X 24小時 365日
資安事件監控

提高資安事件處理效率

減少分析時間

市面上EDR的進階功能比較

功　能　項　目	Fortinet	CrowdStrike	CarbonBlack	SentinelOne	Symantec and other traditional EPP
機器學習病毒行為 (事前防範/ 程式執行過程中保護機制)	Yes	Yes	Yes	Yes	Yes
完整離線保護	Yes	Yes*(僅特徵值比對)	Yes*(僅特徵值比對)	Yes	Yes
支援離線保護	Yes	No	No	No	Yes
偵測	Yes	Yes	Yes	Yes	Yes
資料保存期限	6 month	7 days	30 days	3 month	??
即時的　系統化政策與自動化回覆機制	Yes	No (manual)	No (manual)	No (manual)	No
受感染電腦不須離線也可修復	Yes	No	No	No	No
弱點掃描	Yes	Yes	No	Yes	No
虛擬補丁機制	Yes	No	No	No	No
雲端架構	Yes	Yes	Yes	Yes	Cloud/ Hybrid
本地端佈建機制	Yes	No	Yes* (legacy)	Yes (limited)	Yes* (no feature parity)
支援舊的視窗作業系統(XP, 2003)	Yes	No	White-listing only	No	Yes (SEP only)

FortiClient 與 FortiEDR 差異化比較

FortiClient

- 安全織網架構成員
  - 端點保護機制Endpoint telemetry
  - 應用程式資產管理
  - 動態存取管控
- 安全的遠端存取功能
  - VPN 連線功能 – 支援SSL-VPN, IPsec
  - SSO
- 端點防護功能
  - 弱點掃描 / 弱點補丁
  - CPRL – 防毒
  - 系統漏洞防禦
  - 網頁過濾
  - 應用程式控管 (SaaS Control)

FortiEDR

- 端點防護與勒索病毒阻擋
  - 機器學習-病毒防護 + 行為分析
  - 阻擋非檔案類型的攻擊與防護
  - 應用程式資產管理
  - 弱點掃描 / 弱點補丁
  - 資料保護
- 端點偵測與回應
  - 減少潛在的攻擊來源 – 虛擬補丁
  - 程式執行偵測與保護 (行為模式分析)
  - **系統化與自動化的資安事件處理與系統回復**
- 資安事件的的調查與協助
- 威脅防範
- 提供FortiResponder MDR 服務

Q & A


FORTINET