SentinelOne™

AUTONOMOUS ENDPOINT PROTECTION

安創資訊

nuvign

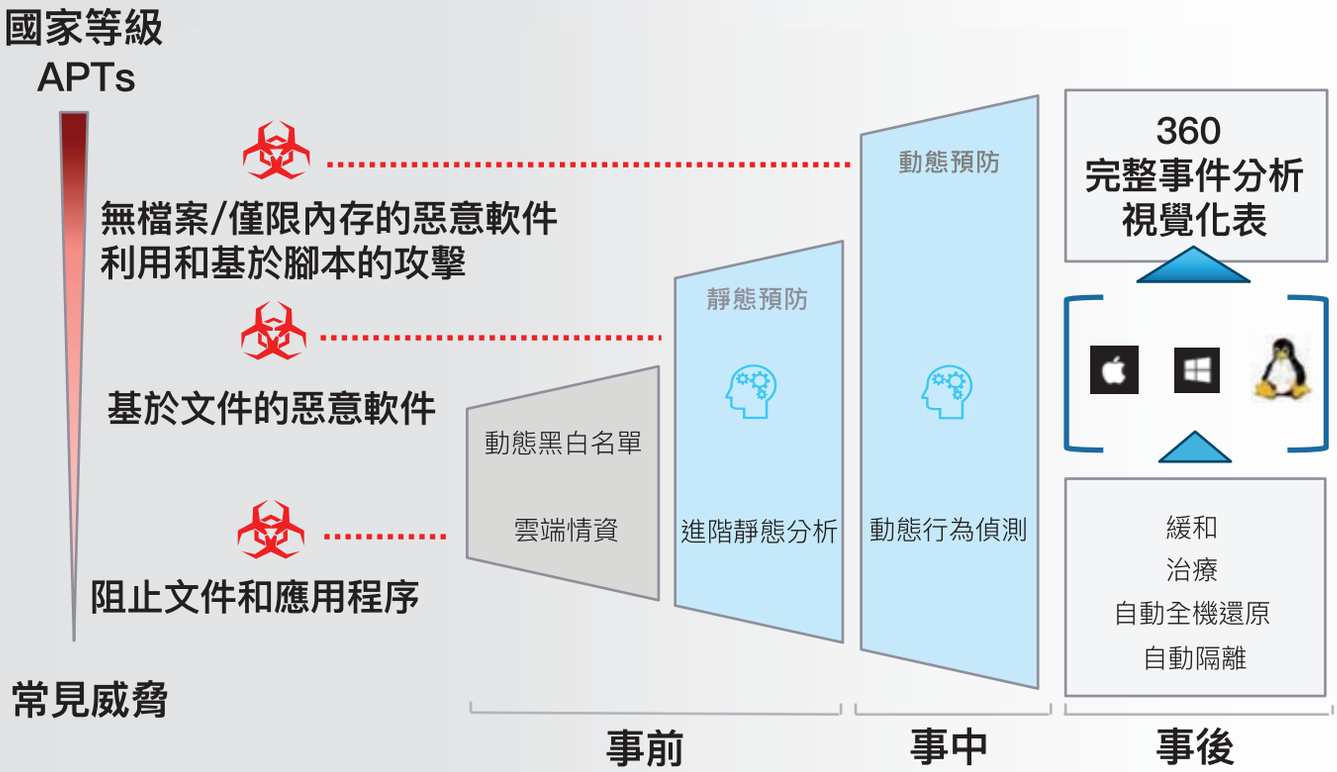
SentinelOne™

輕量級的整合新世代端點保護

SentinelOne 端末防護平台（Endpoint Protection Platform, EPP）在單一控制台管理的平台上整合了：事前預防、事中偵測、事後回應、完全阻擋。為企業提供一致化的端點防衛服務及應用管理。

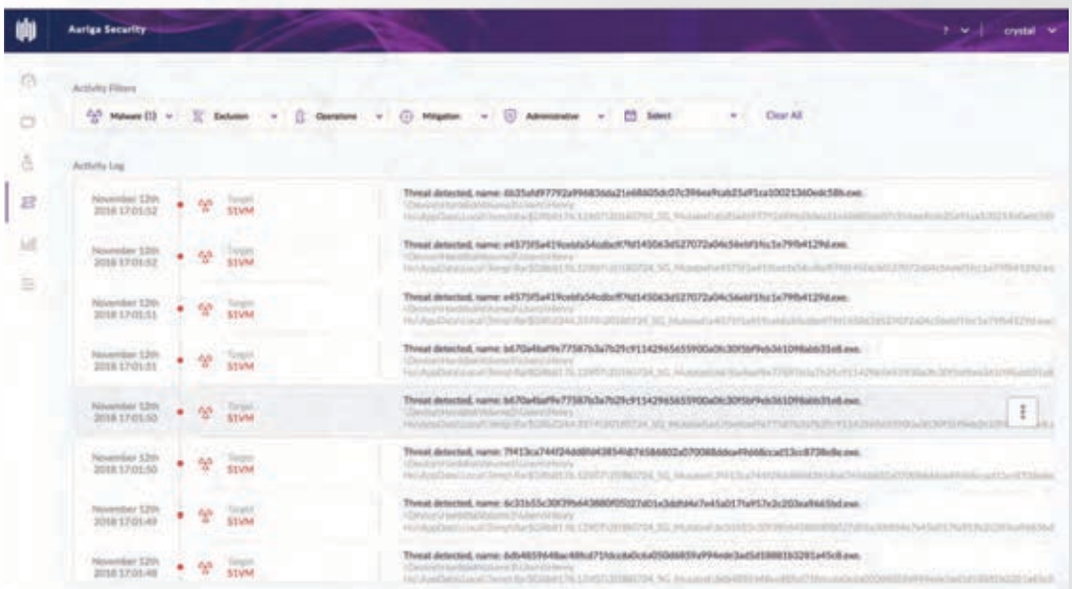
此外，SentinelOne EPP 利用先進的機器學習和「真」人工智慧來保護Windows、OS X、Linux的端點設備。

在攻擊開始之前，立即觸發，進行回應，結束攻擊。



完整的能見度 – 進入所有端點活動，且不影響任何工作效能。

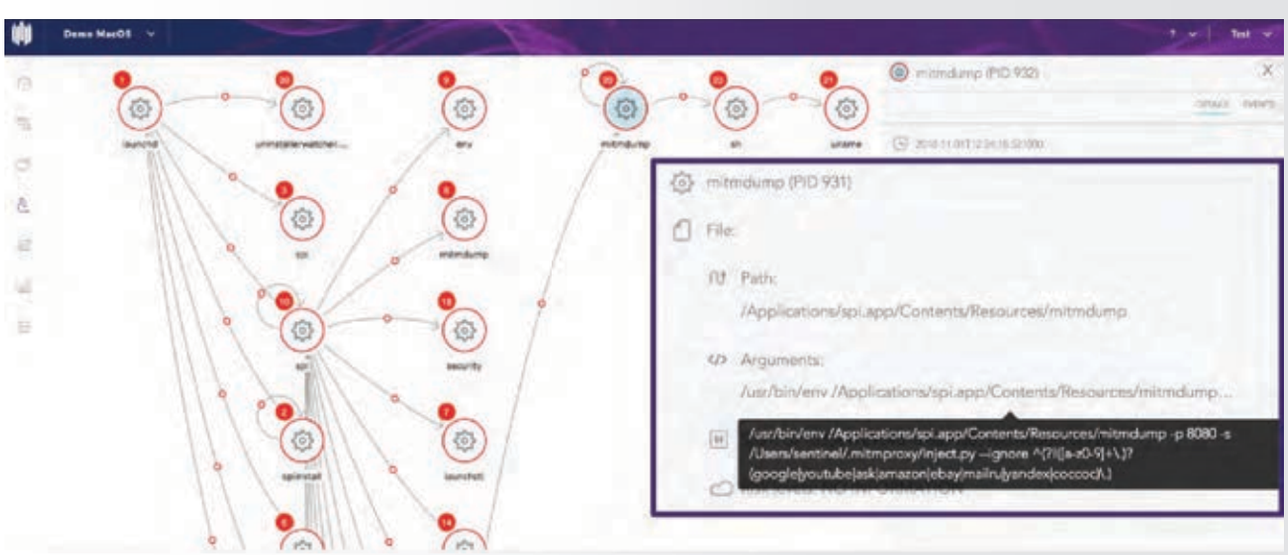
- 一個 Agent, 一個管理介面。
- 不過度使用系統資源，並支援本地或是雲端部屬模式。



進階靜態預防 + AI 動態行為檢測 – 保護所有主要載體的威脅。

- 動態黑白名單動。
- AI 機器學習動態檢測; 即便病毒突變，無需依賴特徵碼，SentinelOne 仍可依照其行為模式檢測。

全面即時數位取證 – 360 完整事件分析視覺化表：從攻擊開始到結束。



產品資訊	SentinelOne	PaloAlto	Symantec	OCSE
架構	On Cloud / On-Prem	On Cloud	On Cloud / On-Prem	Server/Client
佈署	端點佈署	端點佈署	端點佈署	端點佈署
系統需求	Windows/Linux/Mac	Windowes/Mac/Linux	Windowes/Mac/Linux	Windowes/Mac
偵測機制	透過AI、深度檔案偵測、動態行為追蹤方式，阻止零日和針對性攻擊。 主控台上會詳細記錄惡意程式偵測軌跡以及惡意程式連線IP位置，以利鑑識人員查看。	運用來自Palo Alto NetworksWildFire® 雲端威脅分析服務的情報來預防已知的惡意軟體。 用於回應事件和合規性的主動式掃描，能定期掃描端點，找出休眠的惡意軟體。	整合端點安全防護(SEP),有效防堵進階式攻擊。 並運用沙箱模擬可疑檔案進行深層檔案檢測。"	透過機器學習、行為監控、整合式雲端防護伺服器、應用程式控管、漏洞攻擊防範、良性檔案檢查，再配合檔案信譽評等、網站信譽評等、(C&C)攔截。
「真」人工智慧偵測技術 *註一	✓	✗	✗	✗
是否可完全斷網使用	✓	✗	✗	✓
是否需要雲端資訊	✗	✓	✓	✗
更新頻率	六個月～一年	一個月	每日	每日
惡意程式處理行動	刪除、隔離、修復和倒回至電腦未受感染狀況(VSS)、斷網	隔離、封鎖	刪除、封鎖、修復與通知。	刪除、清除、隔離、暫不處理、重新命名。
黑白名單	動態黑白名單:阻止已知惡意程式，黑白名單經設定後並非固定不變，例如: 若白名單檔案被感染時仍會被阻擋。	靜態惡意程式阻擋名單。	阻止或允許 Symantec 黑名單和客戶自建白名單。	間諜程式/可能的資安威脅程式核可清單、信任的程式清單，以將程序排除在可疑活動監控的範圍之外。
主控台上用戶端資訊	Agent general(OS, IP, Agent Policy, Network), APP Inventory, Running Processes, I/O.	用戶端連線、運作狀態、OS版本。	Agent Policy, Platform version, last connection time, reboot request date.	登入使用者、IP、Port、用戶端連線狀態、GUID、掃瞄方法、電腦是否需重新啟動、IDLP、WRS、FRS、損害清除及復原服務、防火牆、行為監控等資訊。

註一：不需要另外依靠主機處理效能處理任何端點所需的辨識，所有防衛及偵測皆在端點完成。
註二：更新意指軟體之人工智慧數學模型組或特徵碼。

NSS Lab 『推薦』等級

第一名的TCO評價
99.8%的安全有效性等級
100%阻止惡意軟體及六大類型的攻擊

Product						Security Effectiveness[1]	
SentinelOne Endpoint Protection Platform v1.8.3#31						99.79%	
HTTP	HTTPS	Email	P2P Applications	Local Intelligence	Blended Threats	Exploits	Various Evasions
98.5%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	93.8%

ISO 27001 Certified

nurign 安創資訊
台北市大安區和平東路二段163號10樓 | +886-2822-4970 | info@aurigasec.com | www.aurigasec.com