BLOCK ALL ENDPOINT THREATS

www.cloudhood.com.tw

ENDBLOCK
BLOCK ALL ENDPOINT THREATS

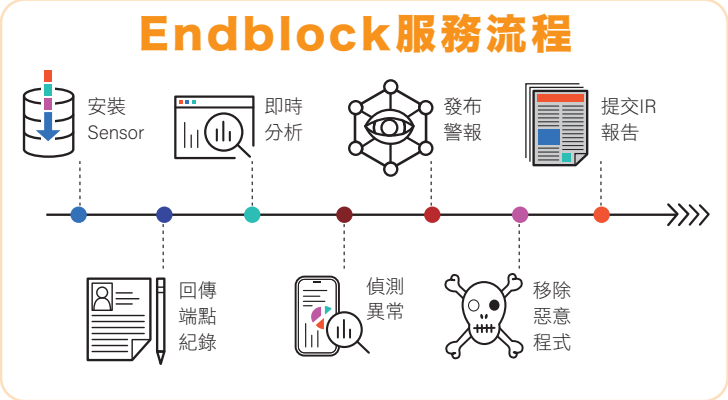
“即時反制所有威脅”

擁有一群來自國內專業產官學資安單位，熟悉資安攻防技術專業人員

主要成員擁有多年第一線的資安事件處理與鑑識實戰，累積多年處理各種進階威脅APT的經驗。鑒於傳統事件處理必須等到事件發生後才能處理，同時需要耗費大量人力，對於避免損失往往都緩不濟急。因此自主整合開發EndBlock，透過即時、自動、高精準度的端點行為分析系統，提供主動式的事件分析與處理MDR服務。讓客戶完美避開駭客的攻擊。

服務項目

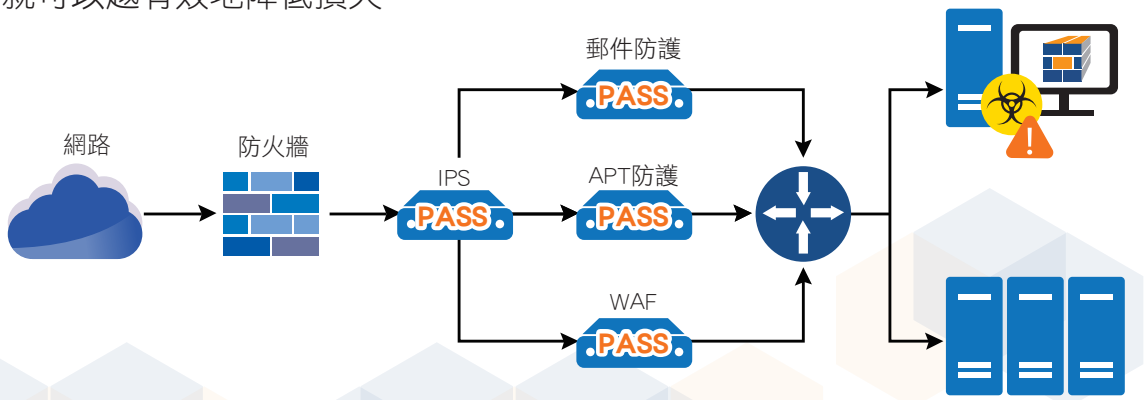
- 7x24 MDR服務
- 惡意程式偵測、處理及應變
- 網路威脅分析與獵捕服務
- 資安事件處理與諮詢服務 (不限次數)
- 資安事件鑑識與定期報告



EndBlock MDR成功關鍵

EndBlock服務提供事件處理（Incident Response ， IR），不是單純的自動化偵測設備。在傳統資安防護架構中，事件處理是所有資安防線的最後一道防線。在目前所有可知的資安事件中，事件處理是惡意程式偵測率最高的技術手段。但傳統的事件處理並不被市場歡迎 ， 因為必須要等到事件爆發 ， 損失已經造成才會處理。

EndBlock完美解決了傳統事件處理的缺點，透過主動收集端點系統活動資訊並比對MITREATT&CK的攻擊方式，完善了即時收集及鑑識的能力，更能有效地分析惡意活動、惡意檔案、惡意程序等攻擊手段。在網路攻擊的初期階段，因攻擊者擁有的資訊與權限相對稀少，故攻擊的手段相對單調、容易辨識。EndBlock更能利用其優勢讓任何疑似攻擊的系統活動在早期階段就無所遁形。越早開始進行應變、停止、隔離並移除惡意程式，就可以越有效地降低損失。



EndBlock管理平台畫面

警報資訊

警報列表

主機資訊

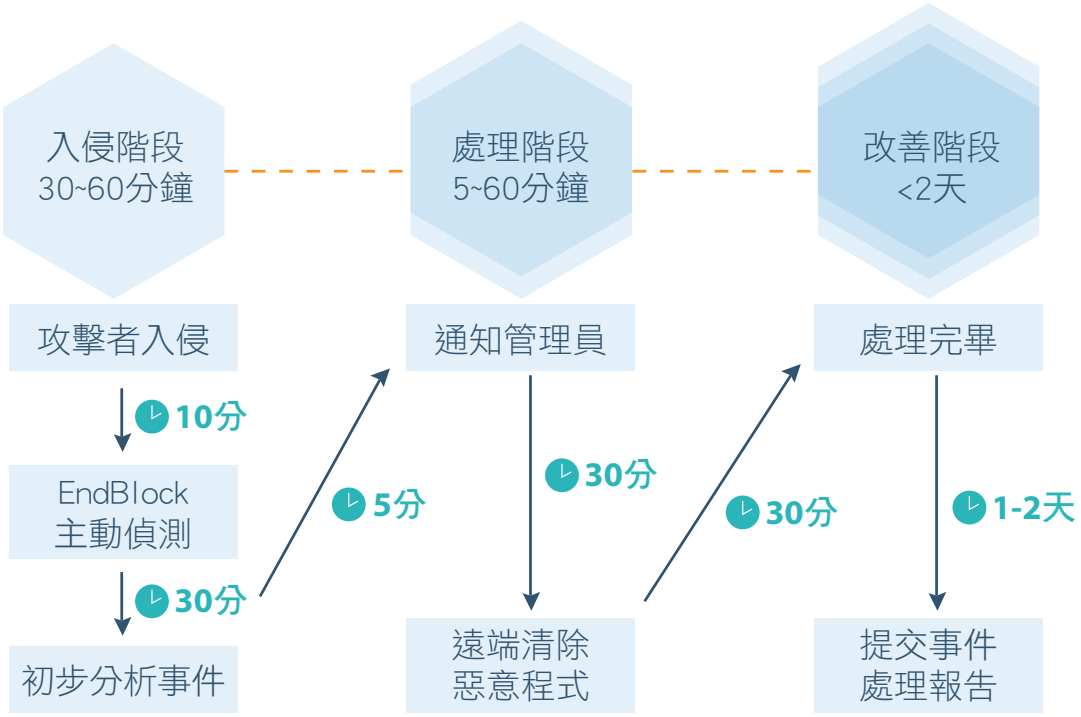
主機列表

SOC v.s MDR 優勢比較表

	MDR	傳統MSSPs
運作模式	威脅獵捕(Threat Hunting)	資安監控 Security Monitoring
驅動模式	分析整體行為導向	警報分析導向
主要核心	Big Data + EDR	SIEM
處理目標	資安事件的回復與處理	偵測到的警報
處理方式	主動發現威脅	被動等待偵測
分析範圍	異常行為整體脈絡	警報本身
服務效益	徹底瞭解、回應及處理事件過程	判斷該警報是否要關閉或通報
評量準則	資料分析對於解決資安事件的幫助	警報的數量

EndBlock處理流程-數量不受限

數分鐘內即可開始主動獵捕並處理



端點收集器基本需求

- CPU效能消耗 < 1%
- 網路平均每1000台頻寬消耗 1Mb/s
  ＊900台 PC 加上 100台 Server的平均值
- 支援作業系統
  ＊Windows 7以上
  ＊Windows Sever 2008 R2以上
  ＊CentOS7,8
  ＊Ubuntu 16.04,18.04.20.14,22.04
  ＊Debian 8,9,10,11
  ＊SUSE-SLES 12 SP3以上

耘通科技股份有限公司 Cloudhood Technology Corporation
台北市信義區松山路130號10樓之1 T：02-2712-0855 F：02-2756-5785 M：Joey@cloudhood.com.tw