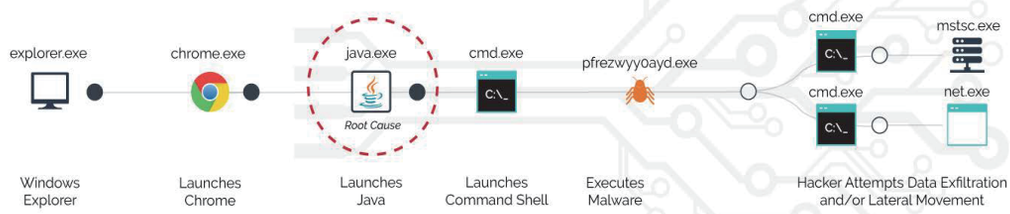
DATA SHEET

Cb RESPONSE

更快速的偵測(Detection)與回應(Response)

駭客的攻擊行為不斷創新

面對新型態惡意進階攻擊，要能夠提前知道並且預防是很困難的。93%的惡意行為能在數分鐘或更短的時間就可以使系統攻陷，偵測及回應速度就非常的重要。大部分的資安監控中心(SOCs)提供的解決方案沒有全面的可視性，無法快速做出明智的決定。在無法提供100%的事件能見度的狀況下，做任何處置都是徒勞無功。這將導致無法進行根本原因識別以及讓IR提前預防未來新型態的攻擊，其他端點偵測/回應的產品都保證搜尋的速度。但能見度仍是不足，這意味著搜尋到的資料並不完整。
只有Cb Response提供完整的可視性，快速分析和遠程修復工具，可以實現最快的端點到端點的事件回應。



威脅攻擊鏈的透視,讓用戶清楚知道根本原因以及受威脅的範圍

Cb Response 是專門為SOC以及IR團隊設計

提供人性化的操作介面，快速的搜尋速度，無限的數據保留並利用Go Back技術識別過去事件的潛在威脅。身為IR和威脅獵捕解決方案的領導者，提供SOC具備以下功能：

透過中控平台連續不中斷的事件紀錄，提供全面性的事件及威脅可視性

- 完整收錄所有端點事件，完整還原所有威脅活動
- 集中式數據儲存讓您隨時可以調閱任何紀錄
- 透視完整的威脅攻擊鏈，讓您快速找到根本原因，並查看橫向移動藉以加速調查
- 無限制的數據保留可以對任何攻擊進行全面的歷史回顧

關於Carbon Black

Carbon Black 是新一代端點安全平台的領先廠商，目的是讓企業能夠阻擋大多數攻擊、找出每一個威脅、填補安全漏洞，並且發展自己的防禦措施。

Carbon Black 擁有約3,000 名全球客戶，包括 Fortune 100 大企業中的30家，擁有超過 650 名員工。Carbon Black 被 SAN Institute 的 2015 年度最佳獎項中被安全專業人員評為最佳端點保護。

Carbon Black.

優點

- **最少的事件回應時間**：提供即時威脅回應與事件消弭，IR的平均時間少於15分鐘
- **端點全面透視**：完整記錄所有端點活動，加速事件回應，並進行主動威脅獵捕
- **無限制的歷史數據保留**：可提供無限數據保留，以滿足合規性和數據保存時間的要求
- **加速調查**：唯有全面端點透視，蒐集的數據才完整，調查事件時才不會漫無目的
- **通盤了解攻擊事件的來龍去脈**：透過攻擊鏈視覺化，深入了解攻擊者的行為及目的
- **找出既有防毒軟體未察覺的潛在威脅**：減少威脅潛伏的時間和造成的潛在傷害
- **阻止潛在威脅未來發動的攻擊**：了解根本原因，解決防禦的漏洞，消除資安盲點
- **降低IT人員的負擔**：避免端點受害後，IT人員不斷重新映像或重灌進行還原
- **內部部署優化**：最小的基礎架構要求--無須浪費額外的硬體資源，提高資源的可用性

透過Cb Response，能夠創建監視列表(watchlists)並識別其他防護機制錯過的病毒。

– 一家國際大型投資管理銀行的資安分析師

使用案例

- 預防惡意或違規行為
- 進階威脅攻擊偵測
- 告警的有效性及分類
- 即時事件回應
- 受害端點及攻擊隔離
- 威脅獵捕
- 修補既有安全不足
- 防止威脅橫向擴散
- 優先程式修補管理

即時事件回應(Response)

每次事件回應時間從原本平均78小時，大幅降至15分以內。
支援以隔離被感染的系統、中止程序、阻擋指定Hash雜湊等方法來阻斷攻擊行為。
「Live Response」功能協助您針對受感染的電能，進行遠程修復，並可以隨時採取各種動作。例如：蒐集進一步的鑑識資料或從任何地點執行自訂Scripts語法。利用根本原因分析，找出並填補防護漏洞缺口，阻止未來新型態的惡意攻擊。

主動威脅獵捕(Threat Hunting)

要避免讓貴組織因遭受入侵而上新聞頭條。您需要更快的將入侵的先進持續性攻擊挖掘出來。2016年有53%的惡意行為都未使用惡意軟體，使得威脅獵捕更為重要。

主動發現最新的潛在進階威脅，不再只是被動防禦。
利用開放式API機制與既有資安廠商整合，提高防護進階攻擊的安全係數。

適用於各種企業規模

最少的資源和基礎設施投資 - 所有企業中有99%可以部署在單個服務器叢集中。

一站式架構整合與開放式API可確保即使在最複雜的環境中也可以無縫地融合。

透過與IBM BigFix的完美整合，實現優先程式修補管理(patch management)。

經過市場驗證的企業級解決方案

Carbon Black 在 Forrester 端點防禦評比中排名第一。
檢測結果高達5/5最高評分、SOC必須具備完整可視性、強化主動威脅獵捕、是一個適合各種企業規模的解決方案。目前全球超過 3,000 個組織，包括 Fortune 100 大企業中的 30 家，都使用 Carbon Black 來保護系統。Carbon Black 銷售超過 9 百萬個授權，並有 75 個以上的專業 MSSP 將 Carbon Black 當成自己的安全服務來銷售。Carbon Black 領先市場的解決方案是免除風險、最大化運作時間並達成監管控制要求的首選。

技術特色

- 適用各規模的企業
- 無限歷史數據保留
- CPU使用率小於1%
- RAM使用量小於20MB
- 網路頻寬平均每秒50bytes
- 中央管理，控制及數據保存
- 整合IBM BigFix啟用優先程式修補管理
- 100%與Open API的完美整合
- 進行雙向SSL身份驗證與服務器進行中間人保護
- 根本原因識別速度提高75%
- 讓您端點重灌次數降低 90%

SUPPORTED PLATFORMS

申請 DEMO:

立即聯繫我們安排Demo

contact@docutek.com.tw

Carbon Black.

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

Carbon Black.

欲瞭解更多資訊，請造訪 www.carbonblack.com

臺灣官方指定代理商

docutek 達友科技

官方網站 : www.docutek.com.tw
聯絡電話 : 02-2658-8970
Email : contact@docutek.com.tw
聯絡地址 : 台北市內湖區基湖路35巷11號4樓之1