Kaspersky Endpoint Detection and Response

為回應進階威脅與現代的網路攻擊，企業持續改善其安全策略。對網路犯罪者而言，端點仍是主要的目標─不過現在的威脅可以避開傳統的端點安全防護措施、中斷關鍵業務流程、讓生產力降低，以及增加營運成本。

延遲導致金錢損失

相較於立即做出回應，在事件探索之後的一星期才進行復原，導致企業損失的金額會**超過200%**。

卡巴斯基實驗室企業 IT 風險調查

Kaspersky EDR 非常適合希望實現以下目標的企業組織：

- 自動威脅辨識與回應─而不會讓業務中斷
- 利用先進的技術改善端點可視性與威脅偵測，包括 ML (機器學習)、沙箱、入侵指標 (IoC) 掃描與威脅情報
- 改善安全防護─利用容易使用的企業解決方案來改善事件回應
- 建立整合且有效的威脅獵捕、事件管理及回應流程。

協助符合法務遵循：

透過內部部署的 Kaspersky Private Security Network 分享即時威脅情報。

- 透過 KPSN 整合，沒有仰賴雲端和資料外流的疑慮。
- 所有的鑑識資料都會集中儲存在企業自有環境中的 Kaspersky EDR。

主動追蹤威脅：

將全年無休的威脅獵捕服務卡巴斯基託管防護新增至 Kaspersky EDR 部署，即可讓企業存取全球威脅研究。
此外，卡巴斯基實驗室的威脅研究人員可以：

- 檢閱企業環境中所收集的資料；
- 快速通知企業的安全團隊─如果偵測到惡意活動；
- 提供回應與修復處理方式的建議。

產品特性

適性化威脅回應

Kaspersky EDR 內含多種自動回應功能，可以協助企業避免使用傳統的修復處理程序─例如抹除和重新安裝映像所導致的昂貴停機和生產力損失。

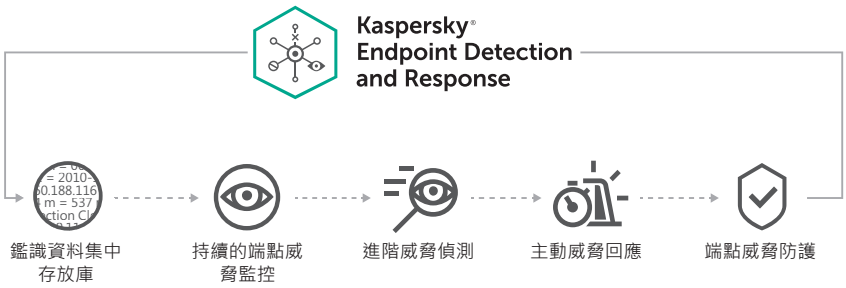
主動威脅獵捕

有了使用集中化資料庫，以及入侵指標 (IoC) 搜尋的快速搜尋功能，Kaspersky EDR 可以徹底改變安全防護工作流程。您的安全團隊可以主動狩獵威脅，而不需要等候警示─主動掃描端點找出異常訊號及安全漏洞。

直覺的網頁介面

Kaspersky EDR 的瀏覽器型介面非常容易使用，可以為安全人員提供下列各項操作的整合可視性與控制能力：偵測、調查、防止、警示與報告。

因為可以透過單一介面監測與控制多種功能，所以您的安全團隊能夠以更有效的方式和更高的效率執行安全工作─而不需要在各種工具和多個主控台間來回切換。



快速找出並遏止進階威脅

Kaspersky Endpoint Detection and Response (Kaspersky EDR) 可以協助企業進行偵測、調查與回應：

- 改善對所有端點的可視性
- 自動處理手動回應的工作
- 改善調查的功能

...而且相容於傳統的端點安全解決方案。

Kaspersky EDR 可以協助安全團隊─以及經驗較少的回應負責人─以網路回應專家的精準度，將端點分類。有了 Kaspersky EDR，貴組織即可：

- 有效「監控」威脅─超越惡意程式
- 有效「偵測」威脅─利用先進的技術
- 集中「彙總」鑑識資料
- 快速「回應」攻擊
- 透過探索的威脅「防止」惡意行動

...這些全都可以透過強大的網頁介面執行，讓調查和反應更加容易。

使用案例：

- 即時主動研究的入侵證據—包括入侵指標 (IoC) —範圍遍及整個網路
- 快速偵測與修復入侵漏洞—在入侵者造成重大破壞與業務中斷之前進行
- 整合 SIEM —協助建立警示和端點活動間的關聯
- 驗證其他安全解決方案找到的警示與潛在事件
- 以無縫的工作流程進行事件的快速調查與集中管理—範圍涵蓋數千個端點
- 將日常作業自動化—協助將手動工作減到最少、空出資源，以及減少「警示過多」的可能性。

進階端點安全防護

卡巴斯基實驗室在端點防護方面展現出持續領先的地位，原因在於我們將以下五個重要元素結合至單一解決方案：

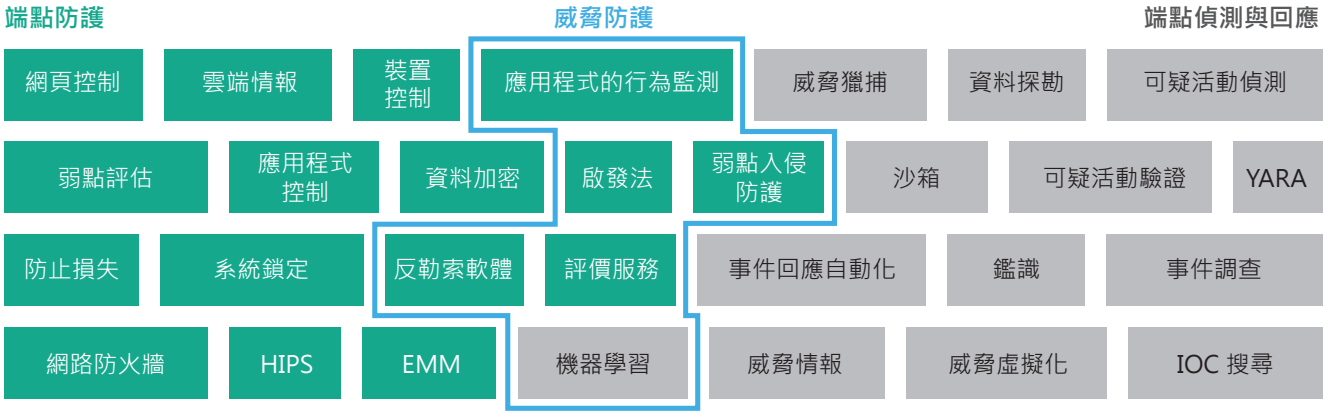
- 強大的新世代防惡意程式引擎—內含機器學習
- 端點偵測與回應 (Kaspersky EDR)
- 全年無休的威脅獵捕服務—卡巴斯基託管防護服務
- 即時威脅情報的存取權—透過 Kaspersky Security Network
- 先進的端點控制 (裝置 / 網頁 / 應用程式、加密等)。

為傳統端點提供安全防護

因為 Kaspersky EDR 相容於來自各種不同供應商的多種傳統安全防護產品，而且也可以配合企業現有的端點安全防護運作，協助增加：

- 新世代功能—用於進階偵測與防護；
- 集中式偵測與回應流程。

...企業不需要更換現有的安全解決方案。



在隔離的虛擬環境中進行物件分析

Kaspersky EDR 內含內部部署的進階沙箱，可以自動擷取任何端點中的任何檔案進行深度分析。Kaspersky EDR 有效為企業提供內部病毒實驗室—而不會將任何資料傳送到網路外部。

進階偵測—包含機器學習

Kaspersky EDR 的機器學習引擎—針對性攻擊分析器 (TAA)，可以建立端點行為的基準狀態。這可以提供用來探索入侵如何發生的歷程記錄。此外，建立鑑識資料、威脅情報和安全引擎分析結果的關聯性，將有助於偵測異常訊號。

企業整體的商業優勢：

降低成本

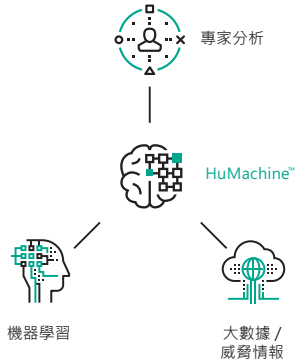
- 將手動工作自動化—在威脅偵測與回應期間
- 協助加快威脅遏止的速度—可節省金錢與資源
- 讓 IT 與安全人員有時間處理其他工作
- 協助將調查期間的業務中斷次數減到最少

提升投資報酬率

- 實現高效率的工作流程
- 縮短威脅辨識與回應的時間
- 強制建立端點記錄、警示檢閱和調查結果的文件，協助符合法務遵循—(PCI DSS 等)

緩解攻擊風險

- 協助排除安全防護缺口，並減少攻擊的「暫留時間」
- 簡化威脅分析與事件回應
- 為現有的安全防護提供威脅驗證



卡巴斯基實驗室
企業網路安全：www.kaspersky.com/enterprise
網路威脅新聞：www.securelist.com
IT 安全新聞：business.kaspersky.com/

真正的網路安全
#HuMachine

www.kaspersky.com

© 2018 AO 卡巴斯基實驗室。保留所有權利。註冊商標及服務標誌均為其各自擁有者的財產。
台灣聯繫人：台灣銷售總監 黃茂勳 eden.huang@kaspersky.com