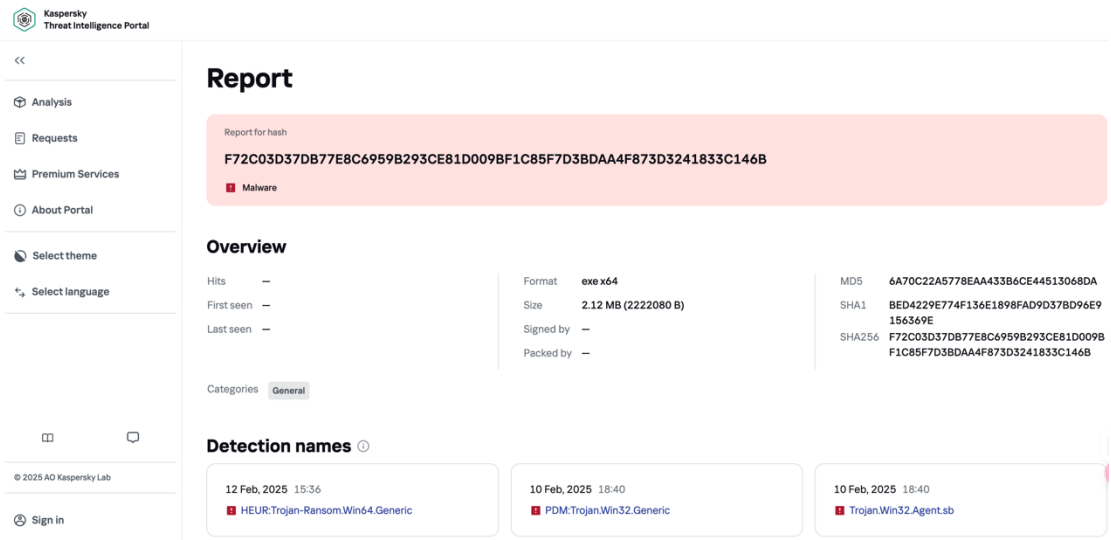
關於近期詢問關於醫療機構遭遇勒索病毒攻擊事件，卡巴斯基能否偵測及阻擋相關威脅。以下為相關說明：

卡巴斯基相關產品於 2025/2/10，就已可透過多層次防護偵測機制包含：**行為偵測**、**啟發式引擎**和**雲端沙箱模擬**等技術偵測及阻擋相關勒索病毒的攻擊。更可利用 NEXT 產品中的 **IoC 掃描**功能，清查內部電腦中是否有被感染的相關聯檔案足跡。

相關偵測到的威脅名稱如下：

HEUR:Trojan-Ransom.Win64.Generic，HEUR:Trojan.Multi.Donut.b



對於卡巴斯基用戶，建議啟用**全 KSN、行為偵測、HIPS、自我防護...等安全設定 (詳細說明可參考附件資訊)** 並確保更新至最新病毒碼及定期進行病毒掃描，就能夠有效偵測並阻擋保護免於勒索病毒的威脅。另建議用戶平常需多注意日常內部系統安全維運事項，已降低被攻擊入侵的風險。包含：

1、 確保端點安全防護更新及定期病毒掃描

2、 檢視內部已知的漏洞及補丁修正管理機制

3、 定期備份及災難還原計畫演練

4、 強化帳號安全與身份認証

5、 監控 AD 相關安全事件及定期檢視 GPO 安全設置

6、 內部員工安全意示訓練。

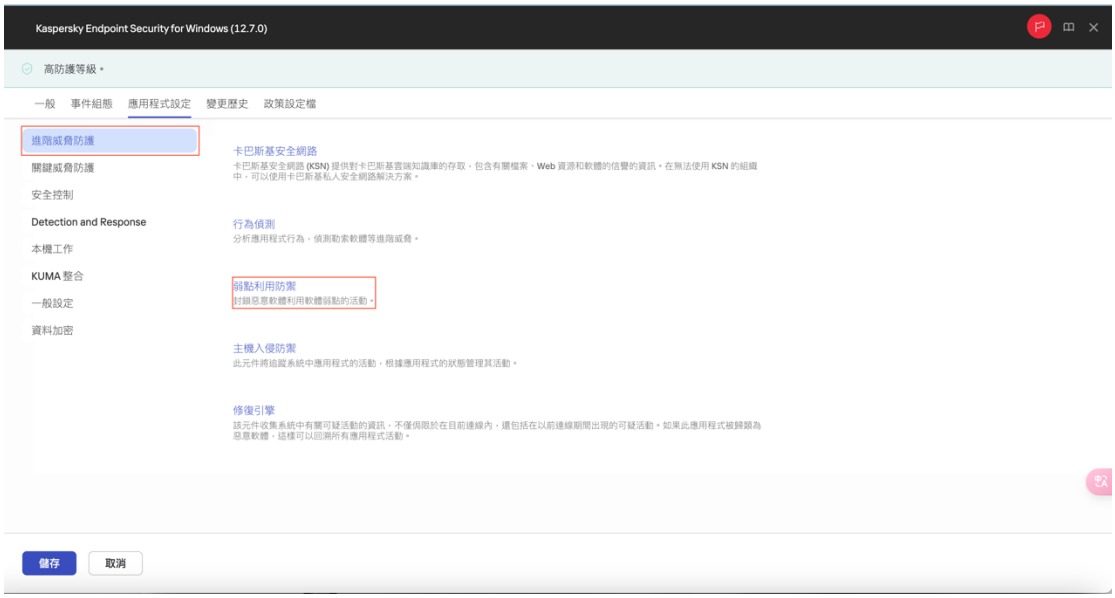
如有任何未知的威脅樣本，歡迎將其檔案壓縮加密並提供密碼，寄送至 techsupport@kaspersky.com.tw 回報或有任何問題，亦可歡迎與我們聯繫。

附件、卡巴斯基端點防護建議設定參考資訊

卡巴斯基除了檔案防護外，還提供了多層次安全機制，來避免未知、新的威脅。包含：

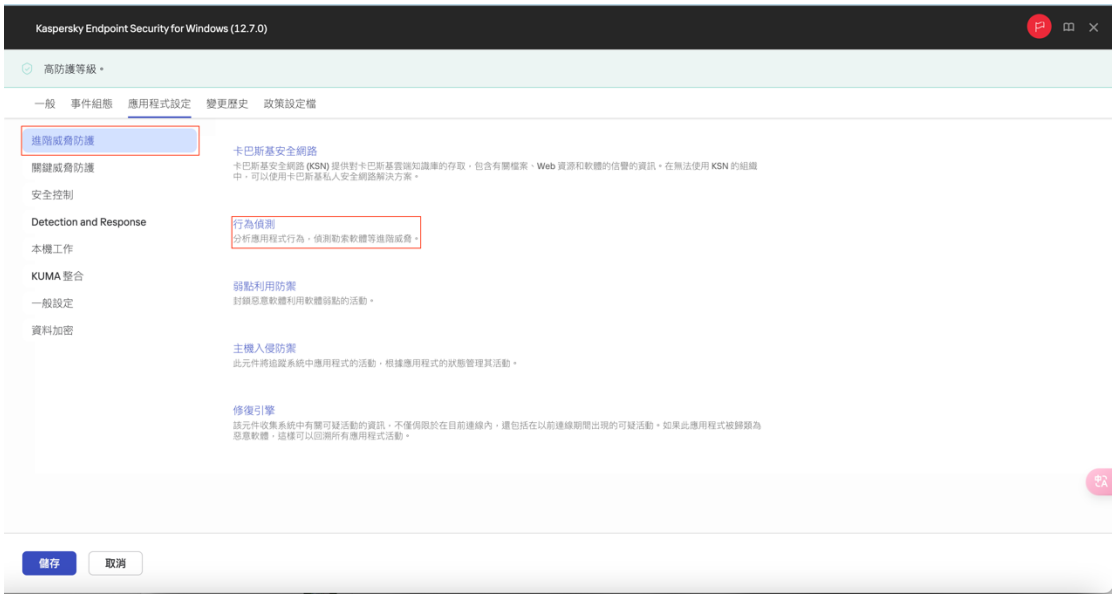
1. 弱點利用防禦(Exploit Prevention)

   此功能自動封鎖利用已知漏洞的攻擊行為，有效防止勒索病毒利用系統弱點進行入侵。



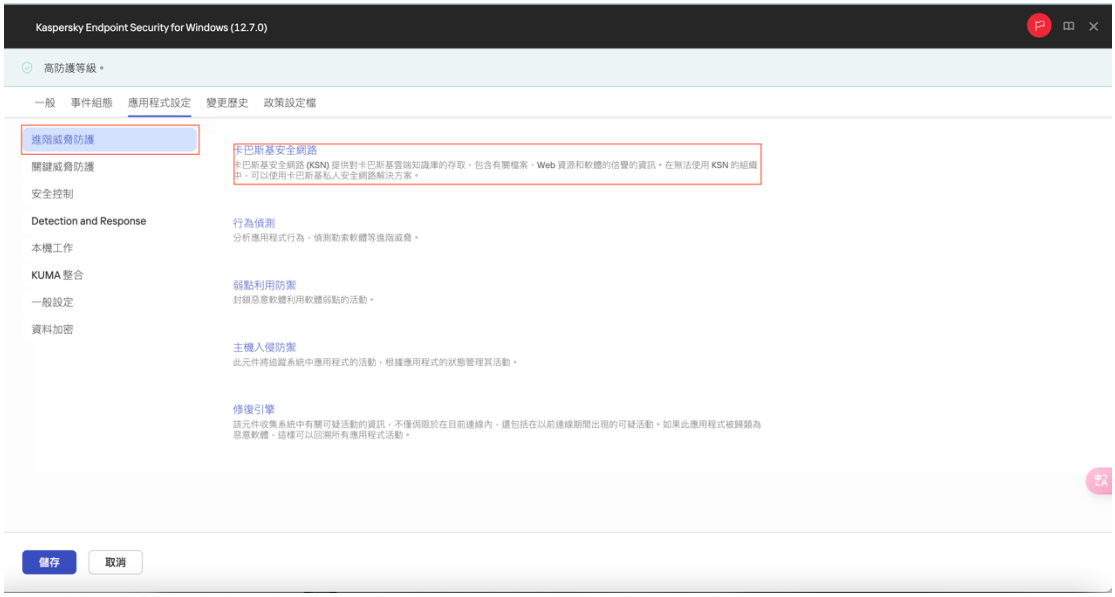
2. 行為偵測(Behavior-based)：

   卡巴斯基分析應用程式行為模式，偵測並即時攔截異常行為，可有效防止勒索病毒在系統內擴散感染。



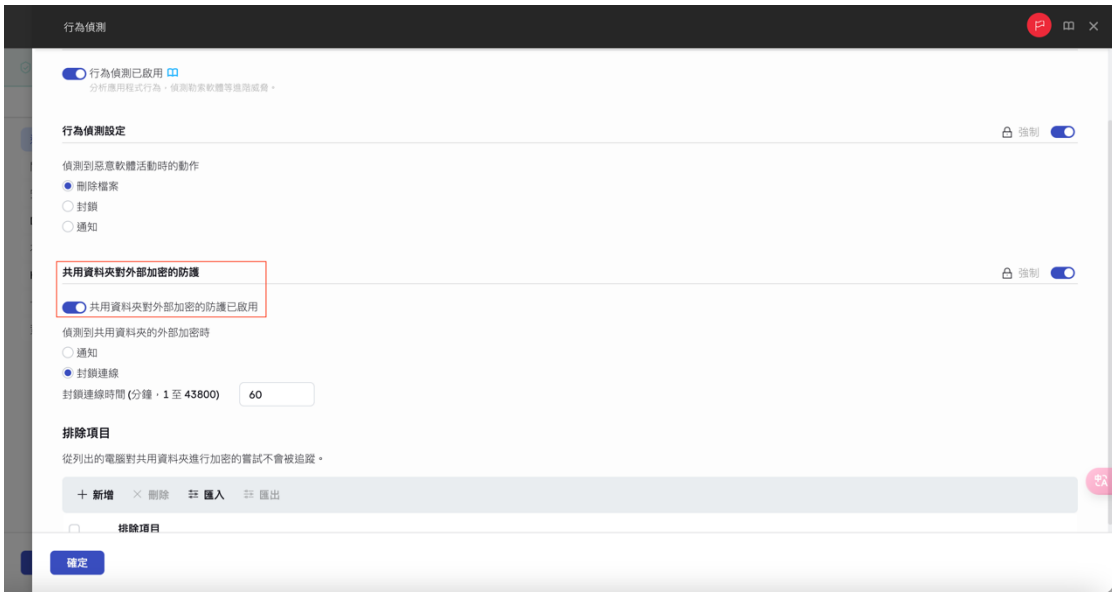
3. 卡巴斯基安全網路(KSN)：

卡巴斯基安全網路可提供卡巴斯基全球威脅情報網絡獲取最新相關資訊，提升端點防護準確性。可即時提供用戶關於新的威脅偵測及阻擋及降低誤判率。建議一定要開啟。



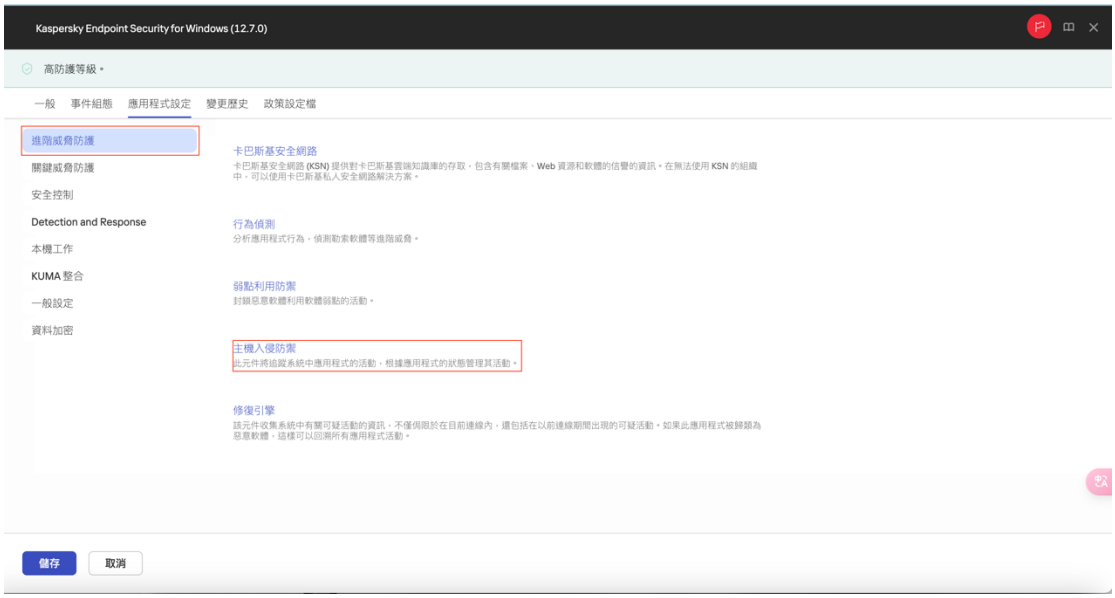
4. 共用資料夾對外部加密防護：

可針對本機電腦共用的資料夾提供保護，避免被其他受感染的主機將其資料夾內容進行加密攻擊。



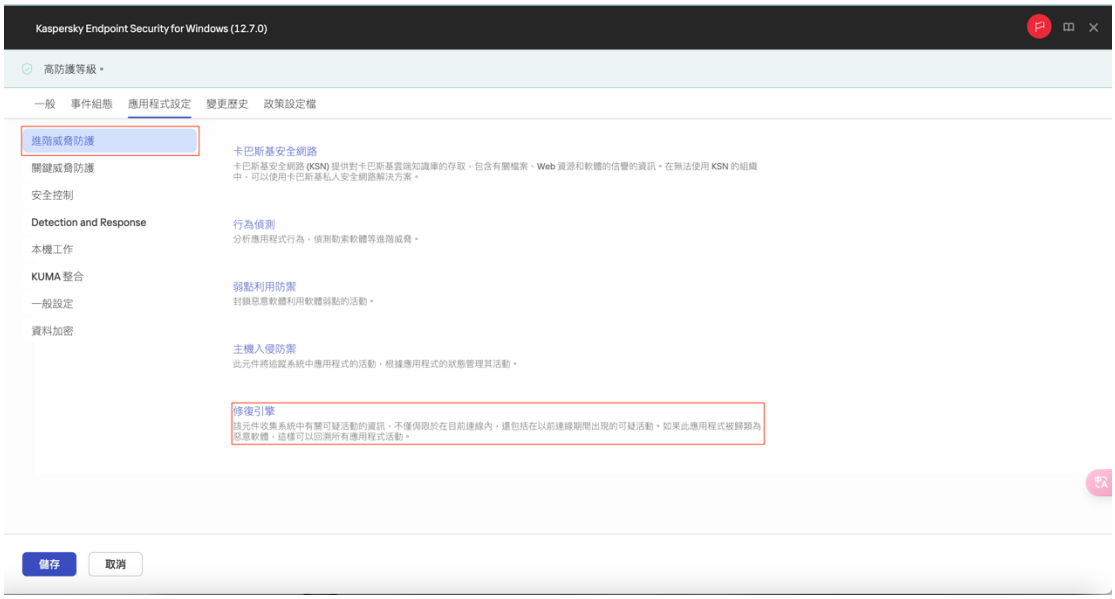
5. 主機入侵防禦(HIPS)：

利用 KSN 信譽資料庫 和行為偵測技術，對未知可疑/惡意程式或未信任的程式進行限制。依對已知及未知執行程序的信任等級來限制對系統存取應用的權限。可有效減少未知程序對系統的破壞及影響。



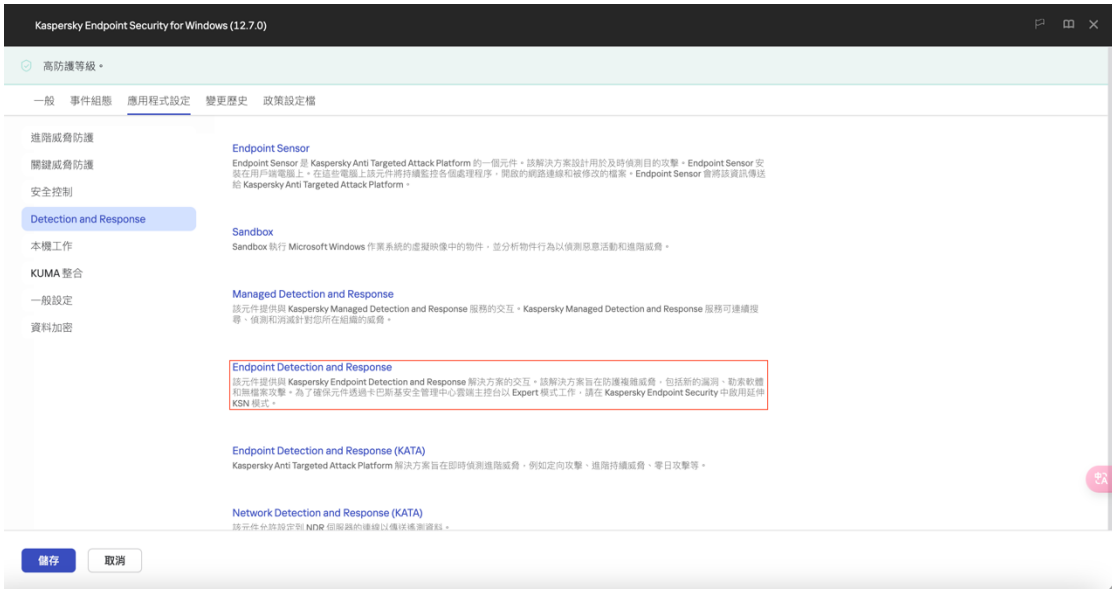
6. 修復引擎：

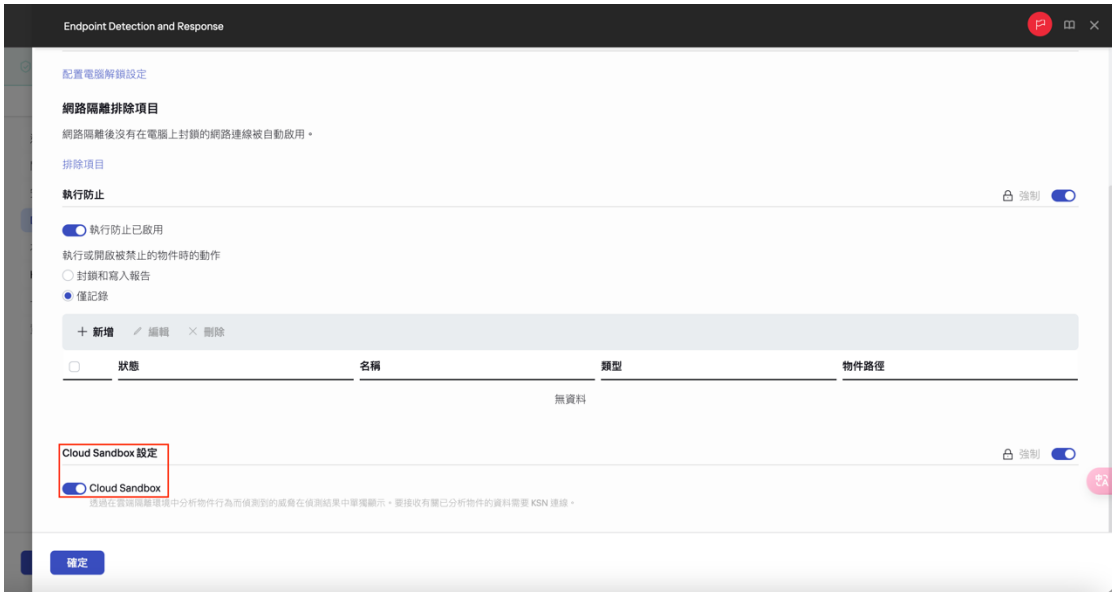
系統回滾功能，可幫助使用者自動回溯至惡意程式觸發執行前的狀態。



7. EDR 和 Cloud Sandbox：

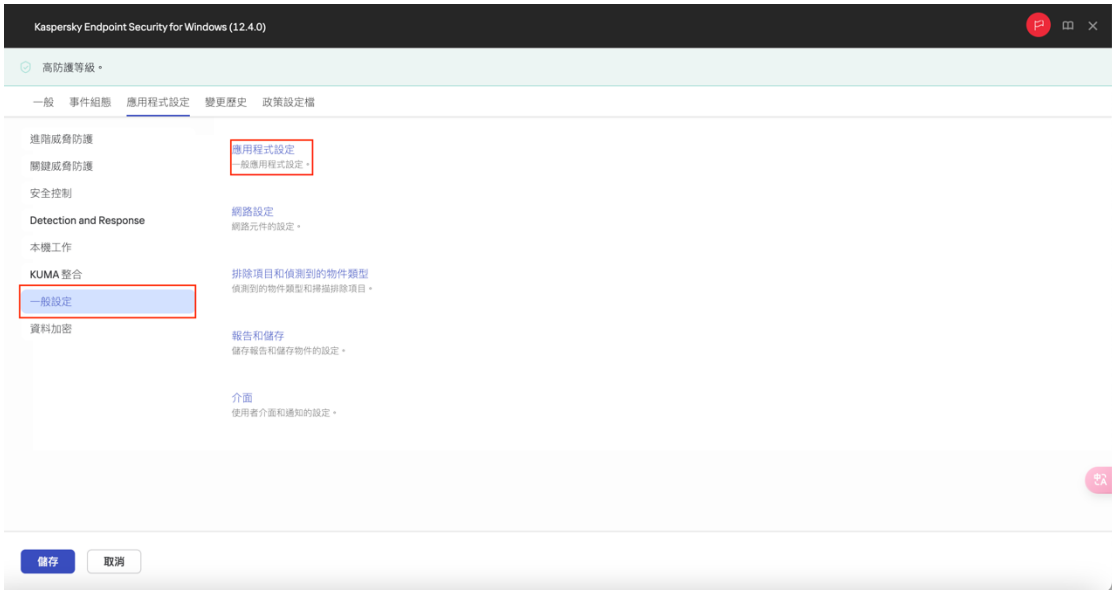
啟用 EDR 功能，提供相關威脅執行關聯圖及雲端沙箱的分析模擬整合技術，可以有效偵測未知威脅，多一層安全檢測防護機制。

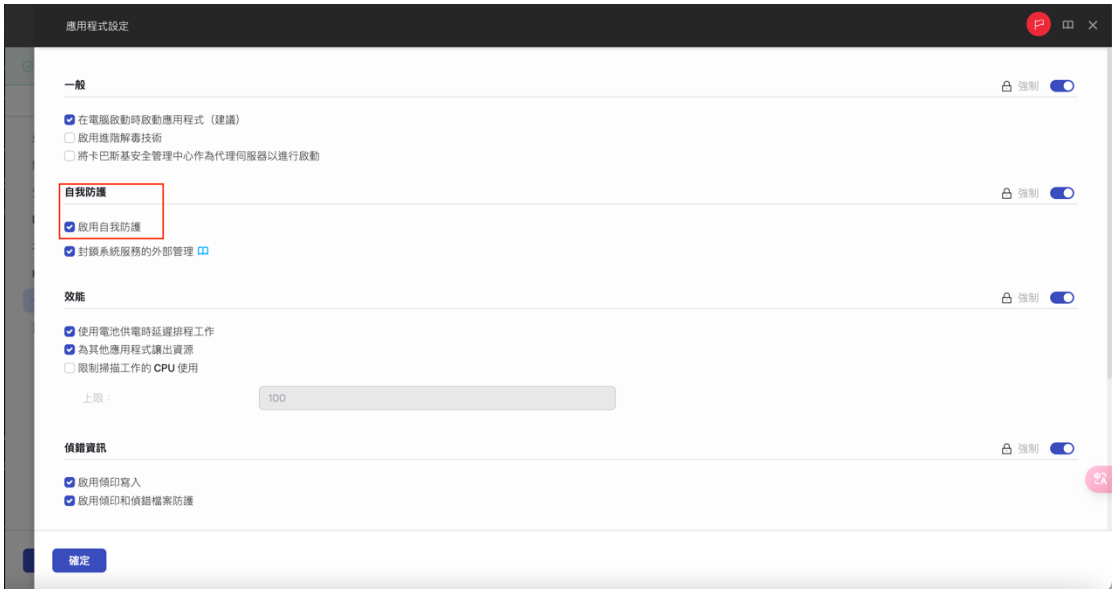




8. 自我防護

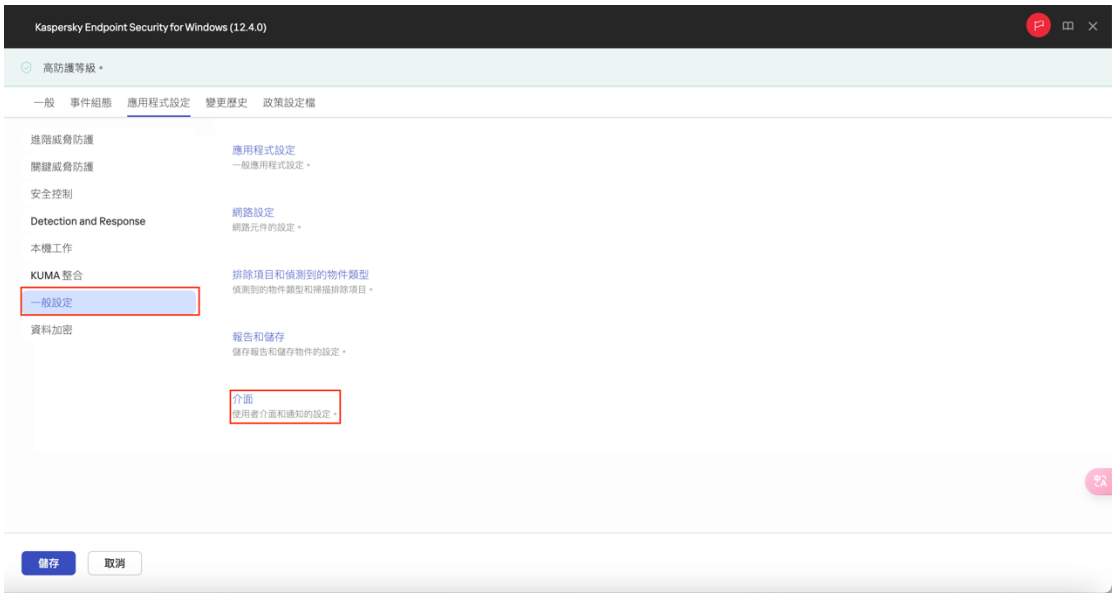
可避免被壞人強制將卡巴斯基端點防護關閉及惡意修改卡巴斯基相關系統檔案。



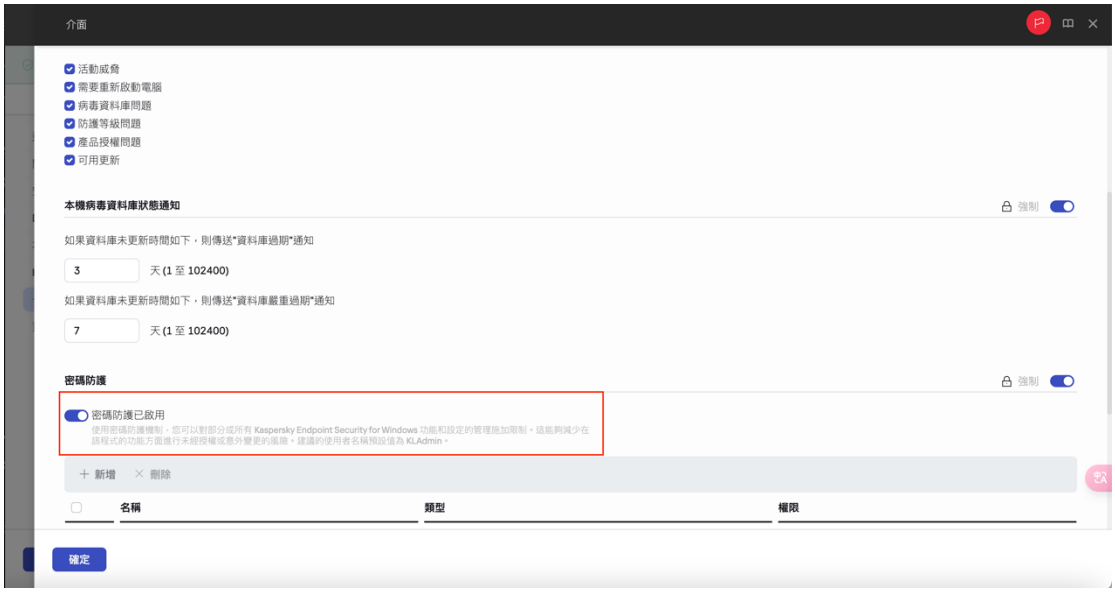


9. 密碼防護：

設定要修改端點設定，已避免用戶或攻擊者將端點防護功能自行關閉。



kaspersky


介面
活動威脅
需要重新啟動電腦
病毒資料庫問題
防護等級問題
產品授權問題
可用更新
本機病毒資料庫狀態通知
強制
如果資料庫未更新時間如下，則傳送"資料庫過期"通知
3
天 (1 至 102400)
如果資料庫未更新時間如下，則傳送"資料庫嚴重過期"通知
7
天 (1 至 102400)
密碼防護
強制
密碼防護已啟用
新增
刪除
名稱
類型
權限
確定