kaspersky

卡巴斯基
針對近期重大勒索事件
卡巴斯基能否偵測及阻擋
Conti 勒索軟體事件

針對近期重大勒索事件-卡巴斯基能否偵測及阻擋 Conti 勒索軟體事件

卡巴斯基相關產品於 2021/1/21 時，就已可利用**行為偵測、啟發式引擎、沙箱模擬等防護機制**進行相關偵測及阻擋。亦可搭配**卡巴斯基 EDR** 的產品針對下列 IoC 的資訊檢查內部是否有相關聯的主機。

KIS、KESL、KES 可偵測到的相關威脅名稱如下：

以下為沙箱偵測機制判定名稱：

Trojan-Ransom.Win32.Agent.sb

Trojan-Ransom.Win32.Cryptor.sb

Trojan-Ransom.Win32.Encoder.sb

Trojan.Win32.Udochka.sb

以下為行為模式分析判定名稱：

PDM:Trojan.Win32.Generic

以下為啟發式引擎判定名稱：

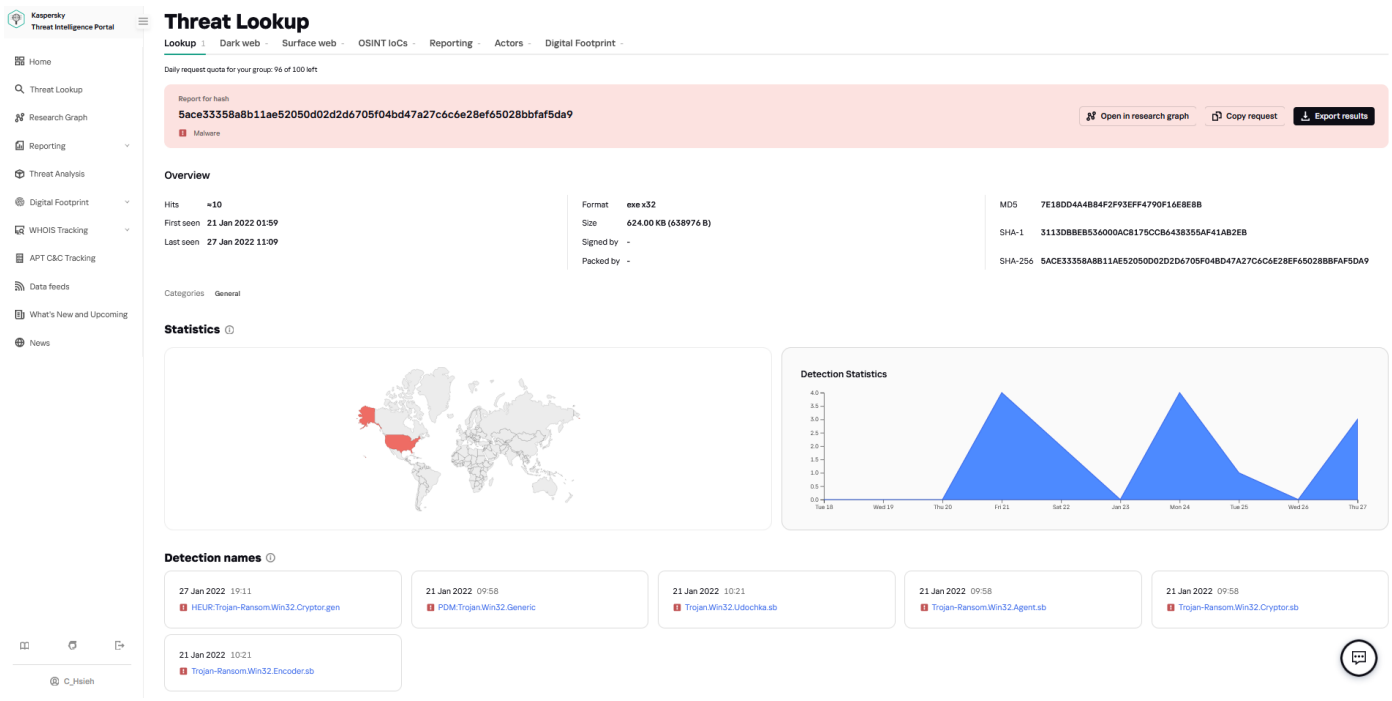
HEUR:Trojan-Ransom.Win32.Cryptor.gen

已知的相關 Indicators of compromise (IOC)資訊：

7E18DD4A4B84F2F93EFF4790F16E8E8B

A3A1C7B6F5B84D4F46A722DBB4FD4FF0

另卡巴斯基情資部份已於 2022/1/21 即可偵測到相關威脅資訊。



kaspersky

隨附如何利用卡巴斯基安全產品來防護這類威脅漏洞利用的建議方式，請確認相關防護功能皆有開啟：

1. 系統監控功能必須開啟(包含弱點利用防禦、行為偵測、主機入侵防禦及修復引擎功能) 。
2. KSN 功能必須啟用。

其他下列相關功能建議開啟及注意事項，可讓您的環境有效降低被攻擊感染的風險。

1. 卡巴斯基密碼保護功能有啟用(避免被惡意程式自行關閉) 。
2. 自我防護功能必須啟用(增加惡意程式停用防護機制的困難度) 。
3. 檔案、網頁及郵件防護必須啟用。
4. 確認安全機制政策鎖頭必須鎖上(有強制套用) 。
5. 針對網芳之共享資料夾，若要使用請務必設定密碼存取，已避免遭惡意程式存取利用，及避免使用過舊的 SMB 通訊協定及請確保無對 Internet 外直接提供 RDP 服務的使用。
6. 確保重要資料有完善的備份機制。
7. 內部環境必須都有安裝防毒，以免造成資安漏洞缺口。
8. 密碼定期更換，避免使用弱密碼。
9. 定期病毒掃描及更新病毒碼至最新。
10. 勿點選任何可疑的郵件連結，郵件附件開啟前請再三確認來源的可靠性。

有任何未知的威脅樣本，歡迎將檔案壓縮加密並提供密碼，寄送至 techsupport@kaspersky.com.tw 或 https://opentip.kaspersky.com/ 協助回報。

以下為相關端點設定的參考資訊：

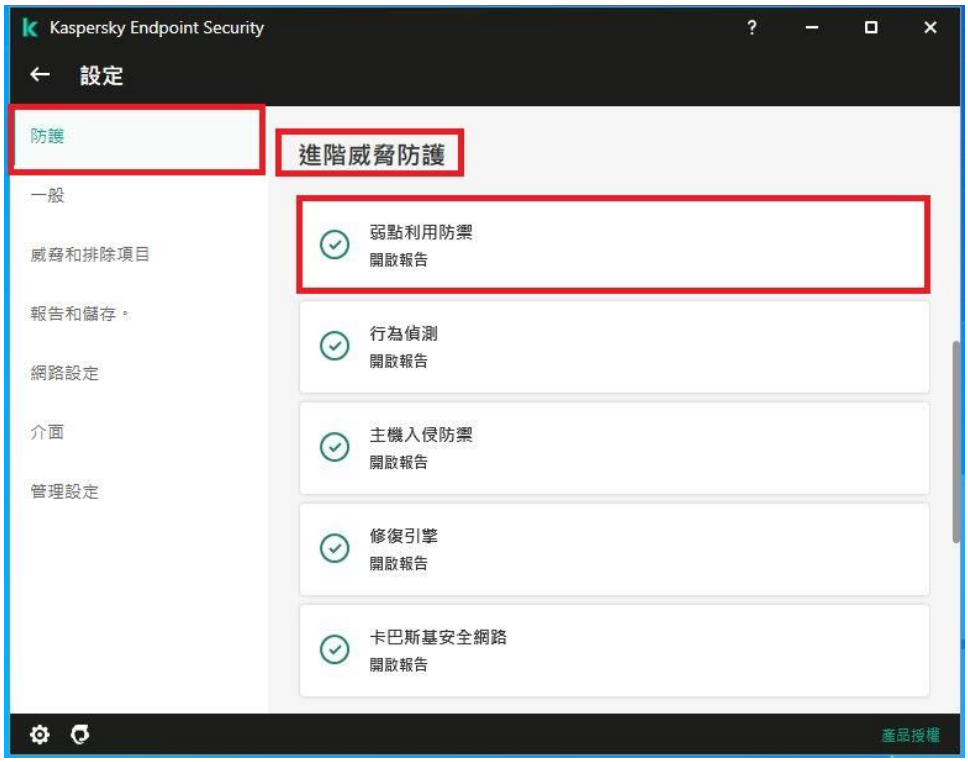
卡巴斯基端點(Kaspersky Endpoint Security for Windows)

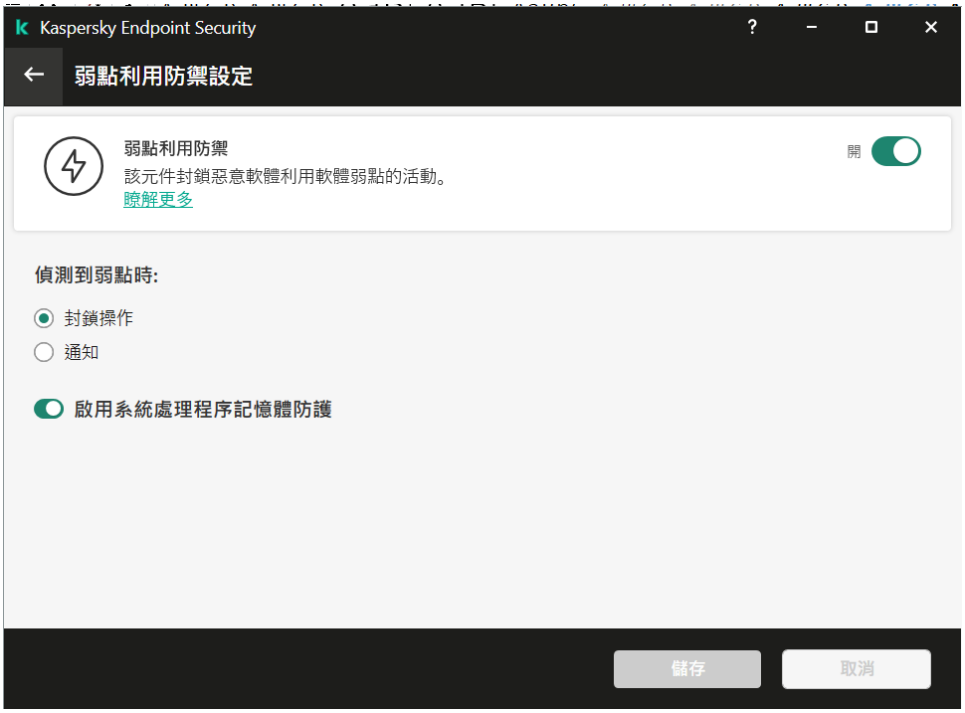
如何有效阻擋進階、未知威脅及勒索軟體威脅：

除了防毒引擎外，卡巴斯基端點防護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)：

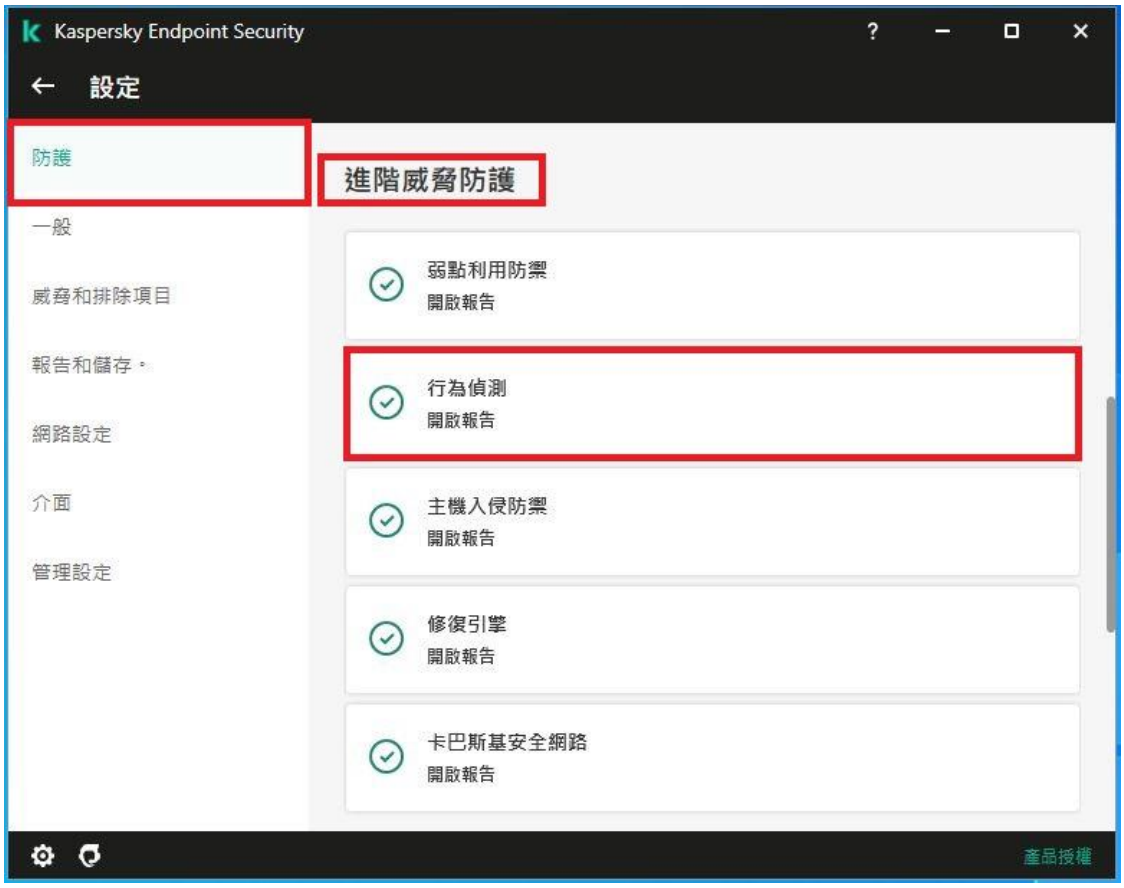
會自動封鎖惡意軟體利用已知軟體弱點的活動。





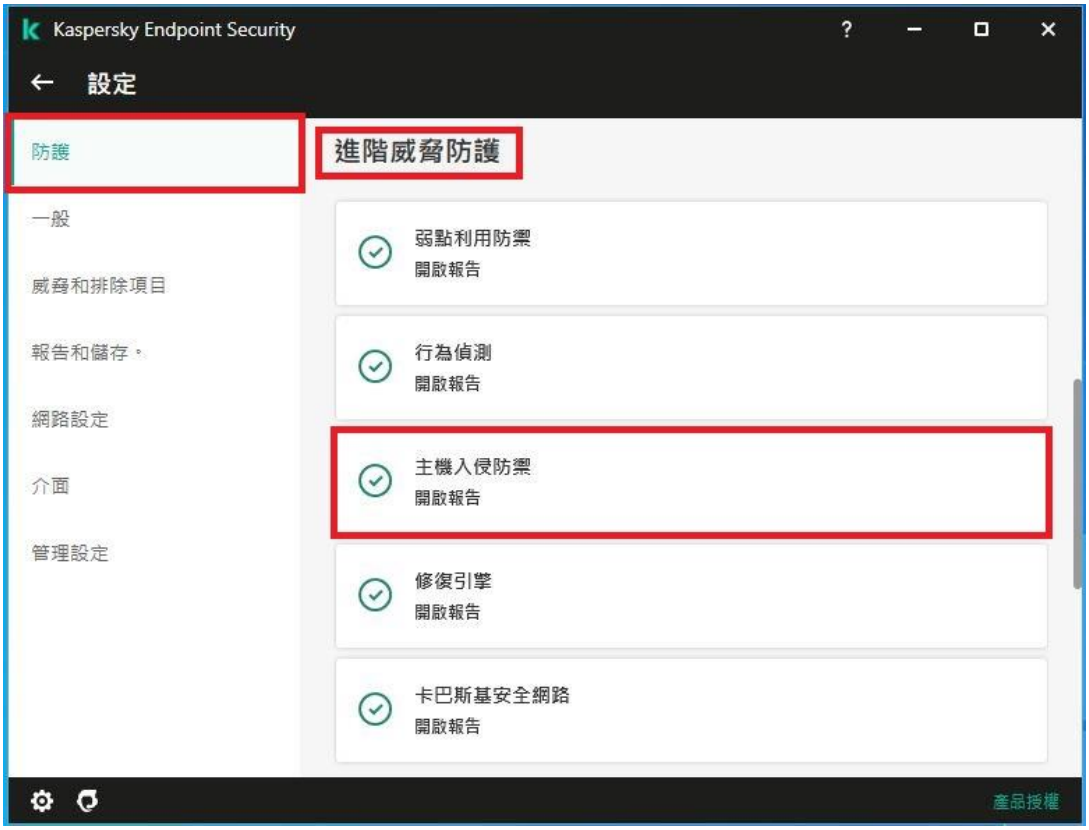
(2) 行為偵測(Behavior-based)：

當程式對系統有惡意/不正常動作時，會自動中斷。



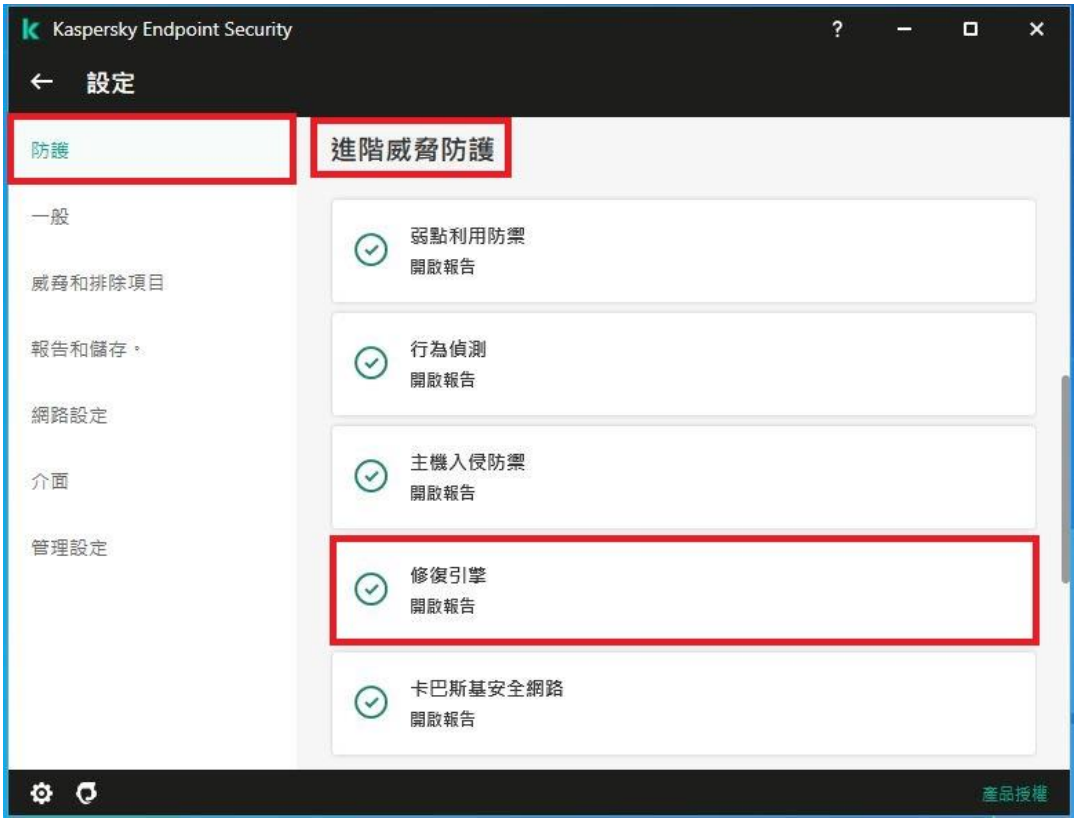
(3) 主機入侵防禦(HIPS)：

搭配 KSN 的信譽資料庫，可針對未知的程序自動限制可支援的動作，避免造成系統的傷害。

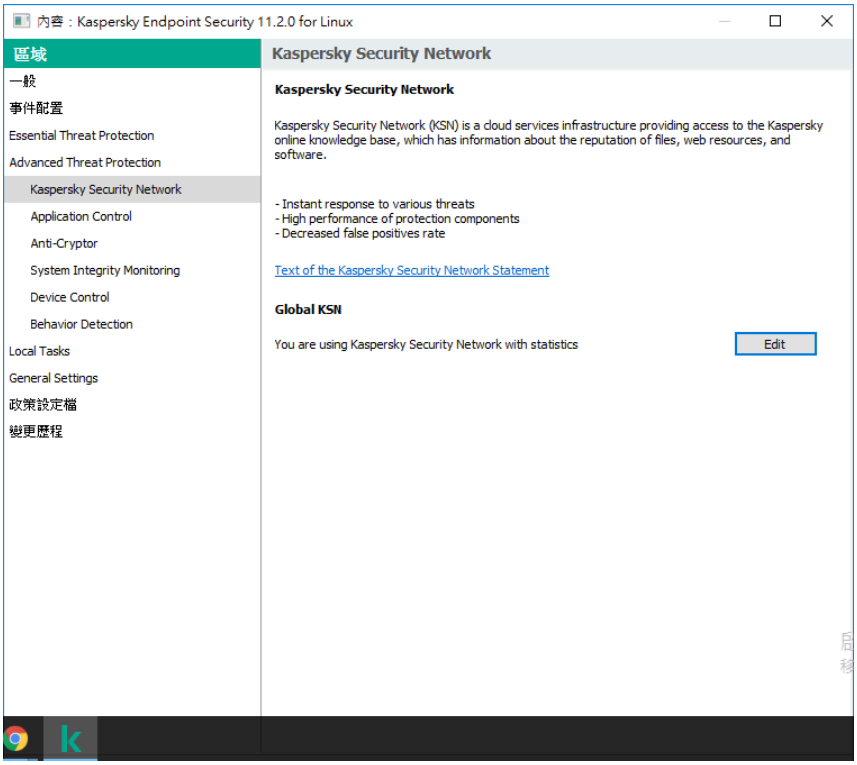


(4) 修復引擎：

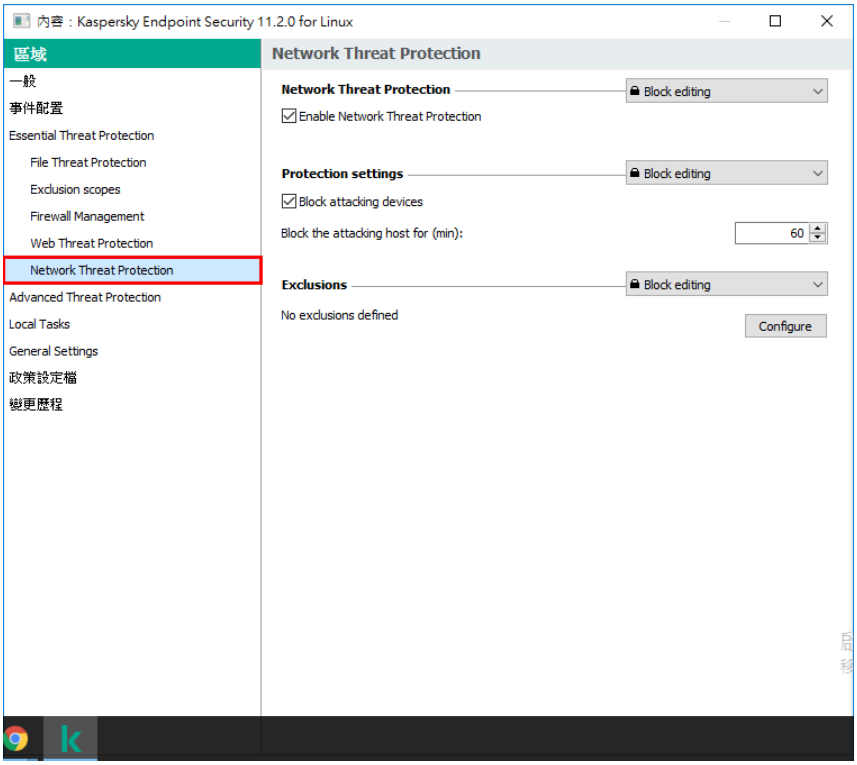
當發生異常行為時，可以回滾至發生異常行為前的狀態



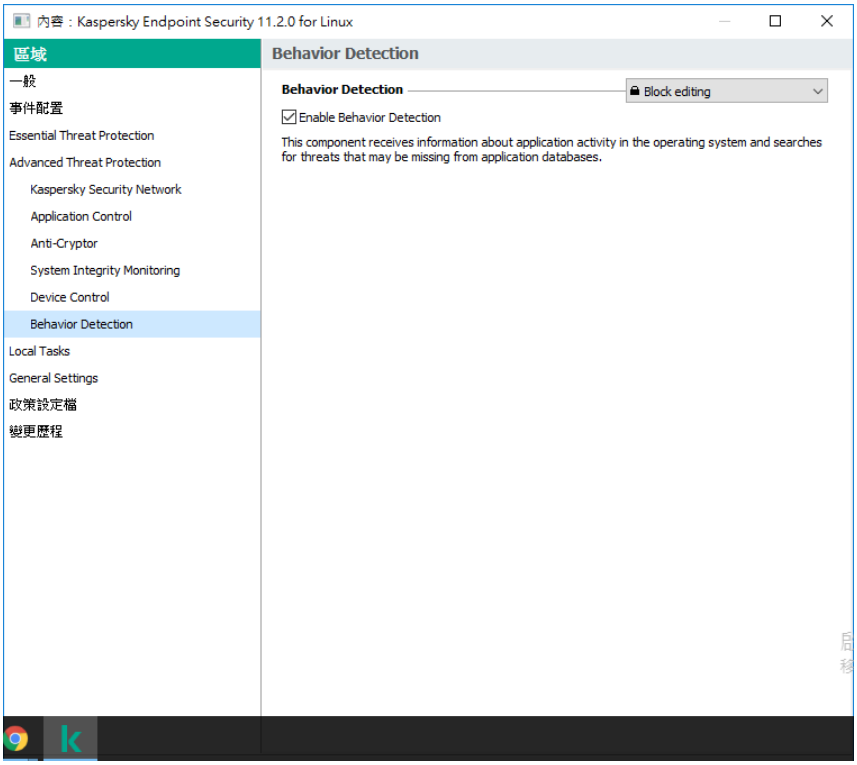
卡巴斯基端點(Kaspersky Endpoint Security for Linux)，如何有效阻擋威脅、及進階威脅，以下截圖在 KSC 主控台進行設定操作。請務必將 KSC Linux 政策中的 KSN 進行同意開啟。



請務必將 KSC Linux 政策中的網路攻擊防護的元件勾選，並且鎖頭鎖上確保該功能開啟。



請務必將 KSC Linux 政策的行為偵測防護的元件勾選，並且鎖頭鎖上確保該功能開啟。



註：上述功能在 KES 10 的版本即有「系統監控」功能提供相關防護機制，但在 KES 11 時，將這些功能重新定義名稱及方便管理者分開單獨設定使用。

註 2：相關機制如何阻擋 Demo 影片：

阻擋勒索軟體：https://www.youtube.com/watch?v=qmKa2_eITIY

行為模式偵測：https://www.youtube.com/watch?v=izTB9mea6U4

無檔案異常行為偵測：https://www.youtube.com/watch?v=41VpndBIOLk

其他進階防護機制：

https://www.youtube.com/results?search_query=kaspersky+tech+dive+

相關技術原理說明：

https://www.kaspersky.com/enterprise-security/wiki-section/home