kaspersky

近期關於說明的 MoonBounce UEFI 的攻擊手法揭露的資訊，因其工作原理是感染在 UEFI 韌體中，再利用 Bootkit 在開機程序的過程中載入系統，來規避系統的安全機制 (因為是在作業系統開機階段就被載入)，開機後即可對系統進行後續惡意腳本的佈署/執行。其中惡意執行的階段，部份是在記憶體中執行的，屬於無檔案式的執行方式，所以即使要做進一步的追蹤調查的難度較為困難。

一但有被感染相關的 UEFI 惡意威脅的主機，常見的做法只需要將被感染的 UEFI 韌體重新更新還原至正常的版本或是將被置換的硬體元件更換後，再對主機進行全機掃描的動作，就可清除。但因為被感染的對像是 UEFI 的韌體或相關的硬體元件。此類修補的動作與硬碟重新格式化或是重灌系統的動作不同。所以才會有一但主機上有 UEFI 的韌體被感染，格式化、重灌系統都沒用的狀況。

此類的威脅感染方式，會需要透過升級韌體或是置換硬體(主機上的元件)的方式才能達成相關的感染。所以確保 UEFI 的韌體更新並啟用 BootGuard 的防護機制已避免未經驗証的韌體更新所造成的風險。再搭配 TPM 可信任平台模組來管理相關的更新。皆可有效降低預防此類威脅的發生。

另請確保端點防護產品相關的設定有正確啟用，降低當惡意腳本執行時對系統造成的影響。

針對「MoonBounce」的相關 IoC 資訊及詳細技術說明，可參考下列連結內容：

https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

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

EFI Rootkit – Malicious CORE_DXE

D94962550B90DDB3F80F62BD96BD9858

Modified WMI DLL Launcher

C3B153347AED27435A18E789D8B67E0A

StealthVector

4D5EB9F6F501B4F6EDF981A3C6C4D6FA

E7155C355C90DC113476DDCF765B187D

899608DE6B59C63B4AE219C3C13502F5

4EF90CEEF2CC9FF3121B34A9891BB28D

CFF2772C44F6F86661AB0A4FFBF86833

InstallUtil Launcher

5F9020983A61446A77AF1976247C443D

StealthMutant

0603C8AAECBDC523CBD3495E93AFB20C

8C7598061D1E8741B8389A80BFD8B8F5

F9F9D6FB3CB94B1CDF9E437141B59E16

Microcin

5FE6CE9C48D0AE98EC2CA1EC9759AAD9

kaspersky

50FF717A8E3106DDBF00FB42212879C5

D98614600775781673B6DF397CC4F476

Go Implant

C9B250099E2DD27BB4170836AC480FE0

97EF7B8FCDCB0C0D9FBB93D0F7E6E3B6

Mimikat_SSP

4E4388D7967E0433D400C60475974D50

5F1C7602688E67F299F5BD533FA07880

xTalker Rootkit

45E862964EF4EFDEA181F3927D20E96D

4BC82105403974AA24BF02CFB66B8F7C

Domains and IPs

mb.glbaitech[.]com – MoonBounce

ns.glbaitech[.]com – ScrambleCross

dev.kinopoisksu[.]com – ScrambleCross

st.kinopoisksu[.]com – ScrambleCross

188.166.61[.]146 – ScrambleCross

172.107.231[.]236 – ScrambleCross

193.29.57[.]161 – ScrambleCross

136.244.100[.]127 – ScrambleCross

217.69.10[.]104 – ScrambleCross

92.38.178[.]246 – ScrambleCross

m.necemarket[.]com – Microcin

172.105.94[.]67 – Microcin

holdmem.dbhubspi[.]com – Microcin

5.188.93[.]132 – Go malware

5.189.222[.]33 – Go malware

5.183.103[.]122 – Go malware

5.188.108[.]228 – Go malware

45.128.132[.]6 – Go malware

92.223.105[.]246 – Go malware

5.183.101[.]21 – Go malware

5.183.101[.]114 – Go malware

45.128.135[.]15 – Go malware

5.188.108[.]22 – Go malware

70.34.201[.]16 – Go malware

File Names

wbwkem.dll – StealthVector

wkbem.dll – StealthVector

wmiwk.dll – StealthVector

C_20344.nls – StealthVector

C_20334.nls – StealthVector

compwm.bin – ScrambleCross Shellcode

pcomnl.bin – ScrambleCross Shellcode

wmipl.dll – ScrambleCross encrypted shellcode

Microsoft.Service.Watch.targets – StealthMutant

MstUtil.exe.config – ScrambleCross encrypted shellcode

System.Mail.Service.dll – InstallUtil launcher for StealthMutant

schtask.bat – Batch launcher for StealthMutant

CmluaApi.dll – Microcin

ScrambleCross Mutexes

Global\GouZUAkmtdpUmves

Global\PtUojBxCOZGVmQQn

Global\EGuUCpyYIJRTQJAV

Global\YCtiqMgRrpLGbfDo

kaspersky

隨附如何利用卡巴斯基安全產品來防護進階威脅的攻擊，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。

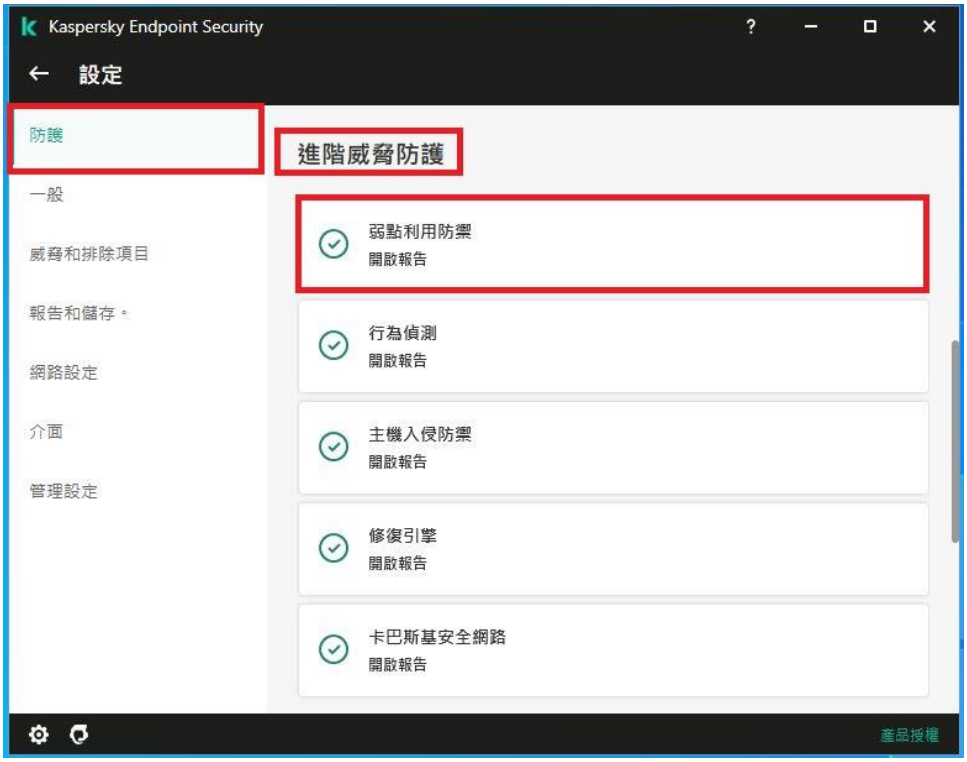
卡巴斯基端點(Kaspersky Endpoint Security for Windows)

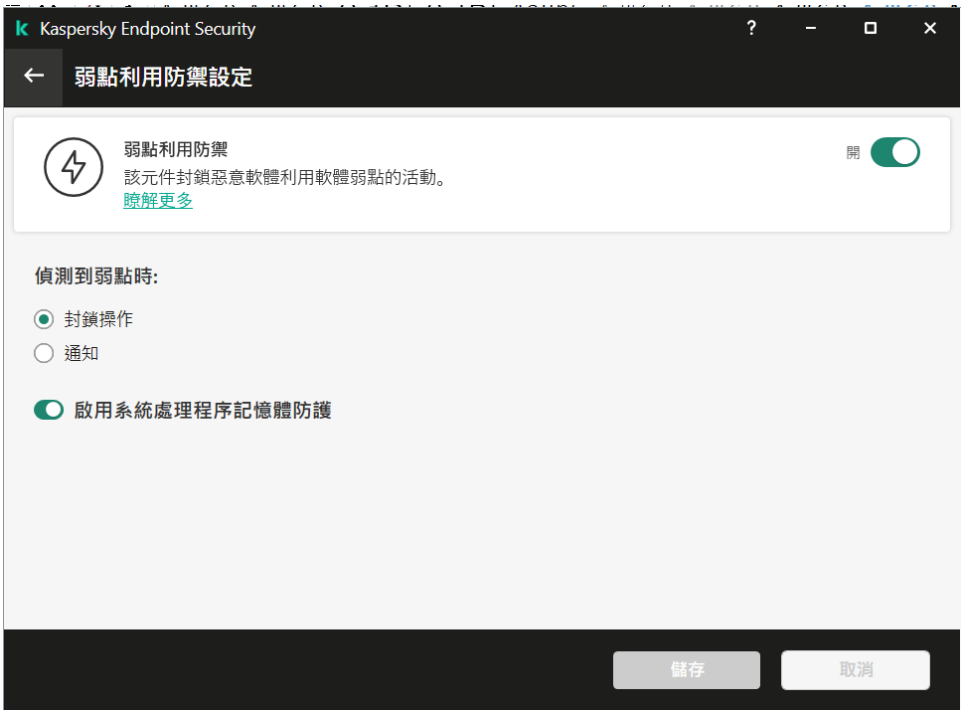
如何有效阻擋進階、未知威脅及勒索軟體威脅：

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)：

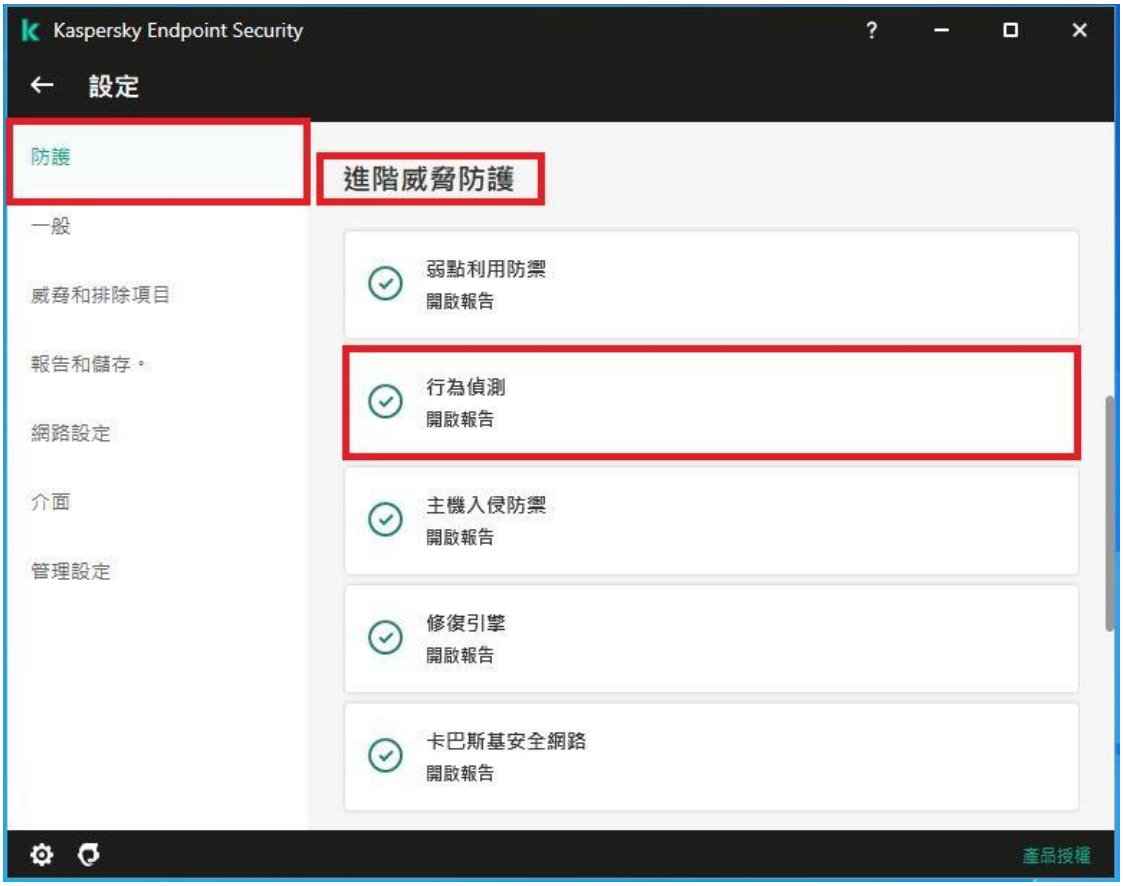
會自動封鎖惡意軟體利用已知軟體弱點的活動。





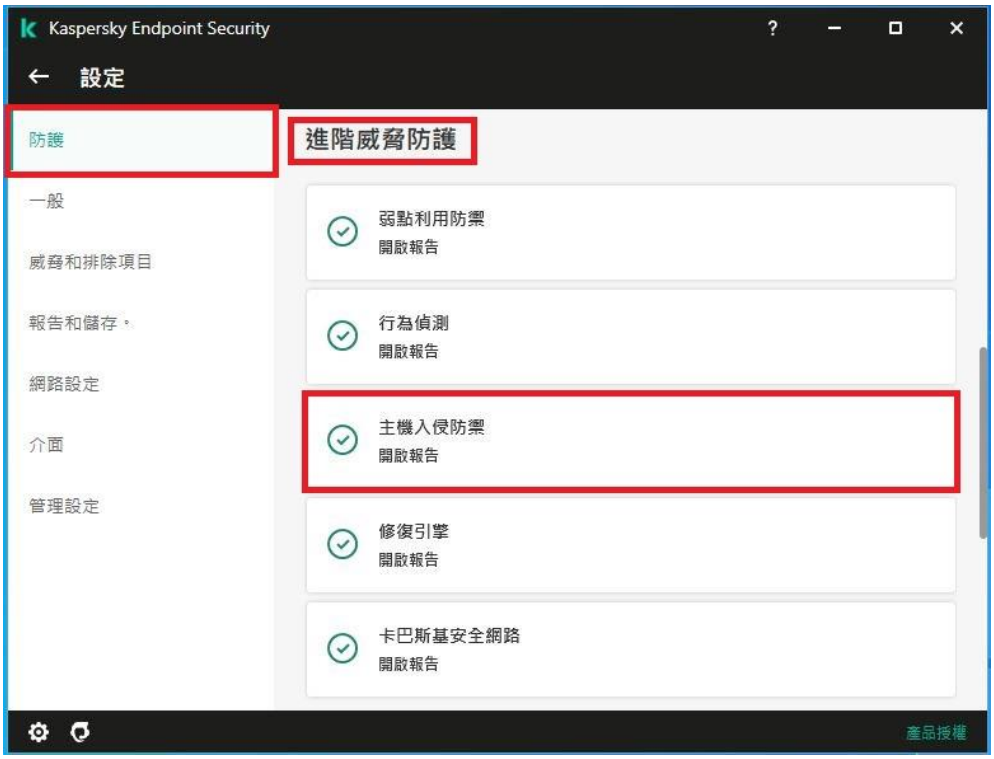
(2) 行為偵測(Behavior-based)：

當程式對系統有惡意/不正常動作時，會自動中斷。



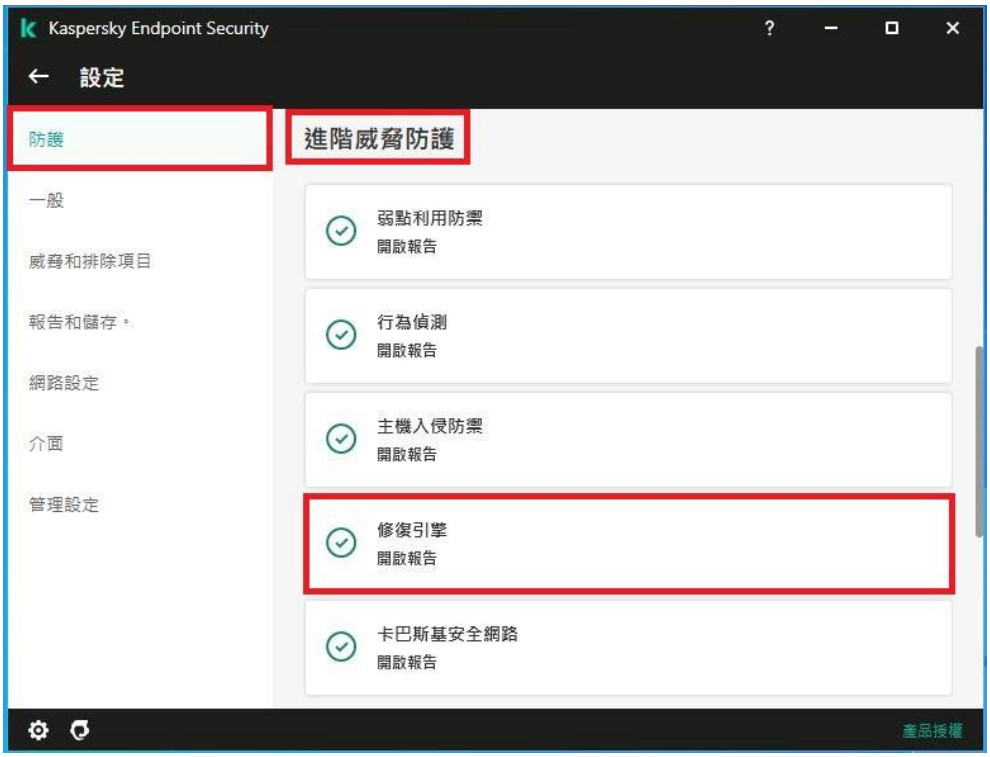
(3) 主機入侵防禦(HIPS)：

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。



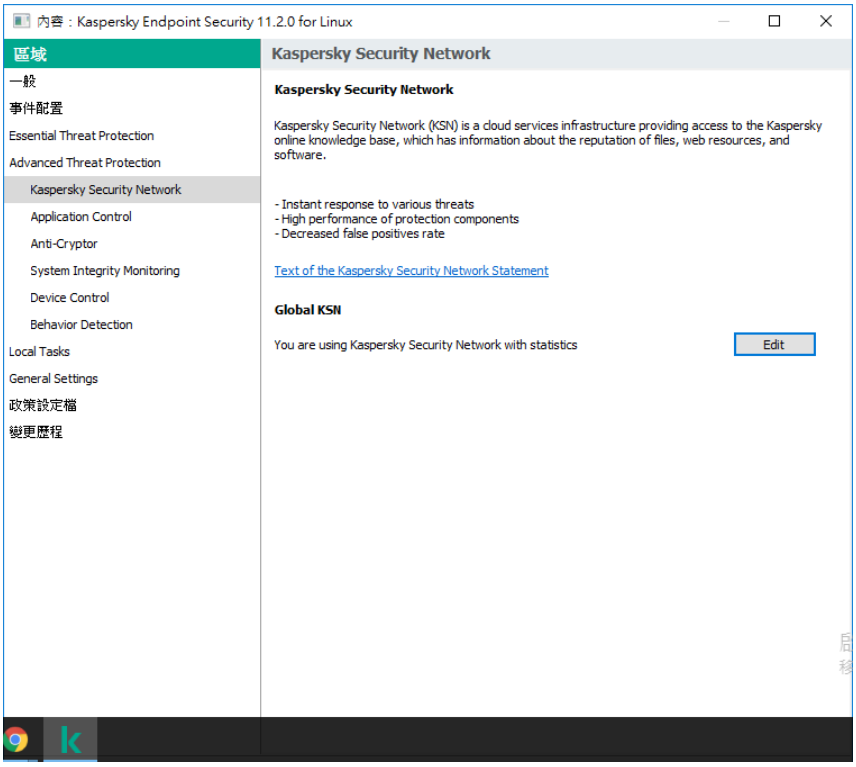
(4) 修復引擎：

當發生異常行為時，可以回滾至發生異常行為前的狀態

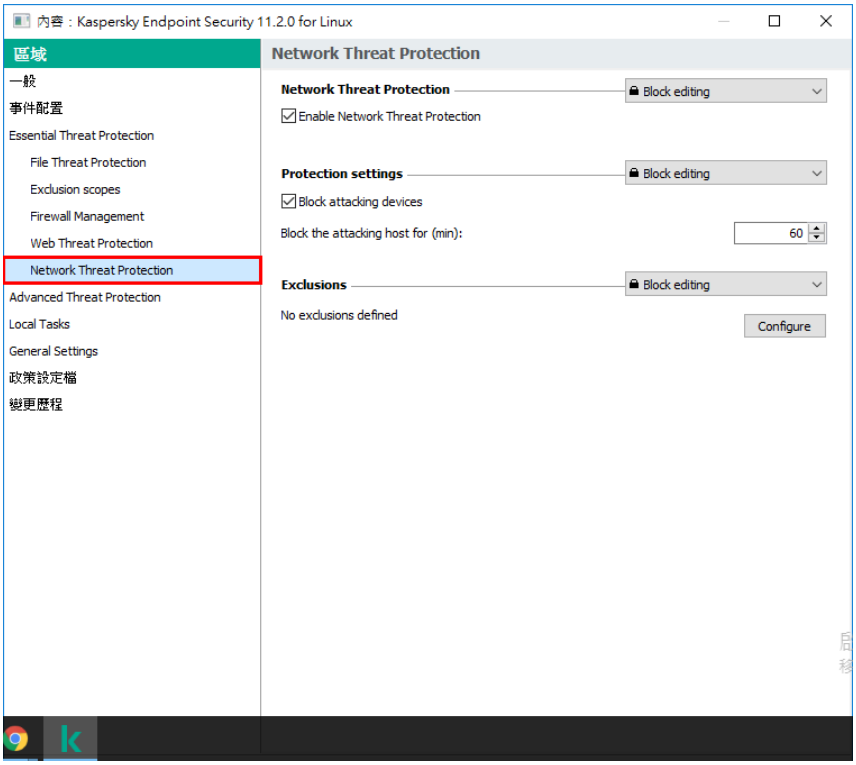


卡巴斯基端點(Kaspersky Endpoint Security for Linux)，如何有效阻擋威脅、及進階威脅，以下截圖在 KSC 主控台進行設定操作

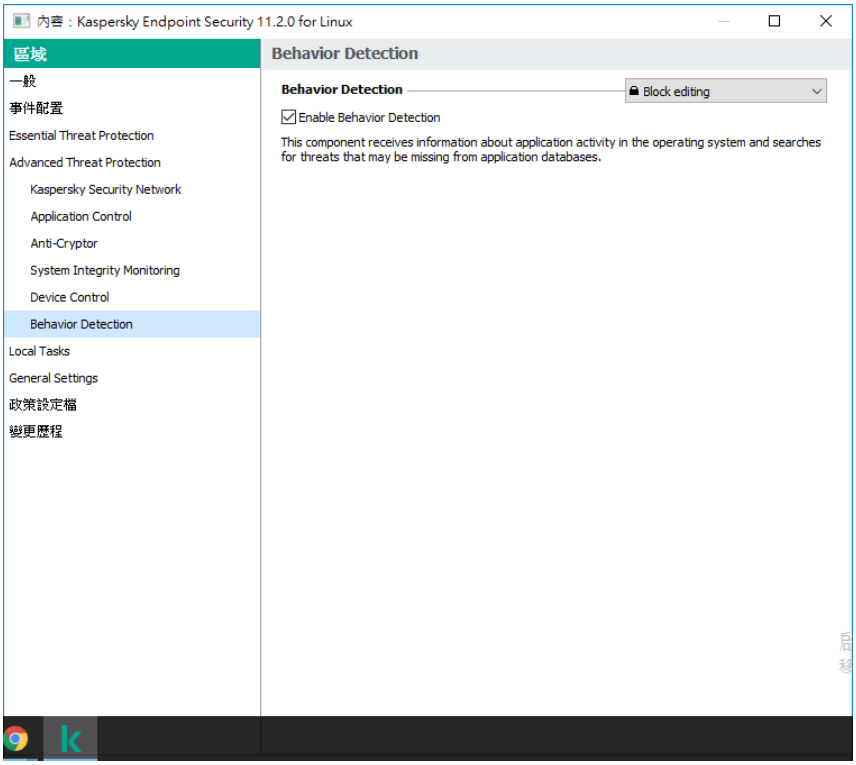
請務必將 KSC Linux 政策中的 KSN 進行同意開啟



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，KES10 產品生命週期即將結束，請儘快進行相關版本更新升級。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