COMODO

IT and Security Management

Comodo ITSM 將您所需的資訊技術和安全管理簡化成單一的控制平台

當資安危機發生時的經典名言

您可能常常聽到…

01 這些病毒木馬都是資安廠商搞出來的！

02 都照標準的規定做，怎麼會出事？都是駭客的問題！

03 使用者自己操作不當，感染病毒或被安裝木馬程式！

04 我們不預設立場，這只是單一個案！

哇咧！

面對**資安威脅**，梁靜茹

只能給你勇氣！

但是...

誰給你**武器呢**？



目前市場中
常見知名品牌防毒軟體
的運作方式

黑名單機制

基於防毒軟體病毒碼、特徵碼進行判斷，若符合則進行隔離、阻擋、刪除等機制。倘若未符合，則將該程式、行為視同系統的一部分，予以放行。

行為判斷

針對未知應用程式的特定行為，例如：綁定、注入、掛勾、修改等對於系統參數異動的特殊行為進行阻擋、禁止、應用程式隔離等預防措施。



怪我囉！

誰知道還是會中獎？



COMODO

自動沙箱防堵技術

唯一經過驗證的遏制技術
帶入企業的防病毒公司

COMODO是如何有效防禦未知的攻擊型態？

白名單

檢視應用程序廠商檔案數位憑證，透過智慧型掃描機制，生成合法程序白名單列表。

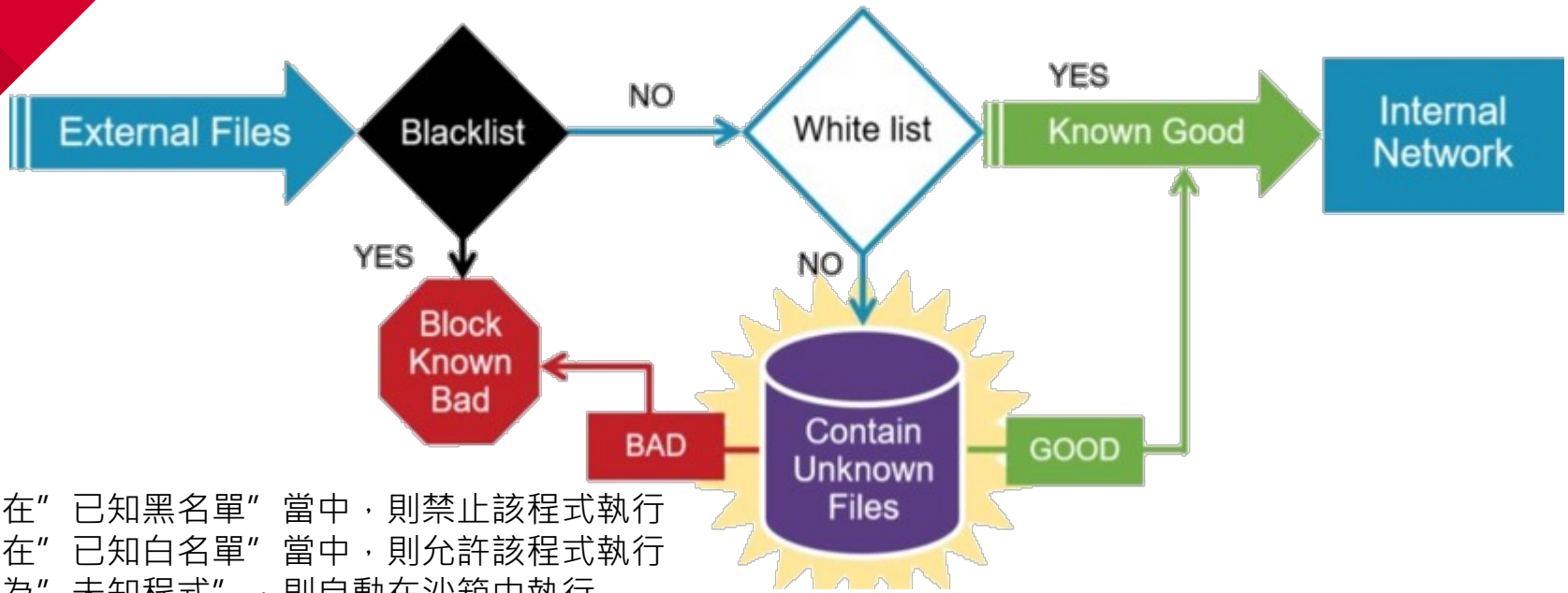
黑名單

透過COMODO AV實驗室長久維護的惡意程式特徵資料庫，有效防堵已知的惡意程式、威脅與風險。

未知程序進沙箱

自動沙箱保護功能的Default Deny（預設拒絕）機制，解決使用者尚未發現的問題程式，以及面對未知威脅的能力。

COMODO 的防禦運作機制



1. 判定在”已知黑名單”當中，則禁止該程式執行
2. 判定在”已知白名單”當中，則允許該程式執行
3. 判定為”未知程式”，則自動在沙箱中執行
4. 不會有未知程式能夠存取您的實體電腦設備或網路
5. 自動進行本地和雲端分析以確定執行程式是否是白名單程式
6. 判定後允許或禁止程式運行
7. 不影響使用體驗

Thanks!