Kaspersky® Embedded Systems Security

專為嵌入式系統設計的多合一安全防護

威脅環境的進展速度十分驚人，導致關鍵業務流程、機密資料和金融資源遭遇零秒攻擊的風險持續增加。為緩解貴企業的風險，您必須比鎖定您的網路專業人員更聰明、設備更精良，而且消息更靈通。

現在我們隨處都能看到嵌入式系統：售票機、ATM、資訊站、銷售點系統、醫療設備等眾多裝置，都屬於嵌入式系統。嵌入式系統通常分散在各地，因而對管理構成挑戰，而且甚少執行更新，所以會產生特定的安全隱憂。這些系統在執行處理現金和信用卡認證的操作時，也需要高度的容錯和抵抗能力。不能只針對嵌入式系統本身來防範威脅：還要讓網路犯罪者或內部攻擊者無法存取嵌入式系統做為企業網路的進入點。

適用於嵌入式裝置的標準安全規範，往往只包含以防毒為主的安全或系統強化，如此並不足夠。若要防範目前的嵌入式系統威脅，僅採用防毒方法的效果有限，這在近期的攻擊中獲得充分證明。現在採用獲得充分驗證的技術 (例如，裝置控制及預設拒絕) 正是時候，並視需要對關鍵系統套用額外的防毒保護。

解決方案產品特性

低階硬體

Kaspersky Embedded Systems Security 經特別設計，即使是低階硬體亦能有效操作。高效率設計可帶來強大的安全防護，且沒有系統過載的風險。在「僅預設拒絕」模式下操作時，Windows XP 系列的最低需求僅需 256 Mb 的 RAM，而系統硬碟僅需約 50 Mb 的空間。

針對 Windows XP 最佳化

大多數的嵌入式系統仍在目前不受支援的 Windows® XP 系列作業系統中執行。Kaspersky Embedded Systems Security 經過最佳化調整，可以在 Windows XP 平台，以及 Windows 7、Windows 2009 及 Windows 10 系列中執行完整功能。

大部分端點安全防護的領導供應商現在也結束對 Windows XP 的支援。預期在一段時間內，Kaspersky Embedded Systems Security 絕對會致力於為 Windows XP 系列提供 100% 的支援。

預設拒絕

近 10 年來我們發現，開發用來攻擊嵌入式系統的惡意程式數量有所增加，包括 Tyupkin、Skimer、Carbanak 及其系列。大部分的傳統防毒解決方案，無法完全防止此類進階針對性惡意程式威脅。傳統的防惡意程式解決方案無法有效防止許多針對性威脅；這些針對性威脅不是以惡意程式為基礎，而是使用內部人士的中介軟體，並採用其他攻擊方式。預設拒絕功能無法執行軟體防護以外的可執行檔、驅動程式和程式庫，除非獲得安全系統管理員的核准。

裝置控制

卡巴斯基實驗室的裝置控制，可讓您控制 USB 儲存裝置，這些裝置可能已經連接到系統硬體，或是以實體方式正在嘗試連線。防止未經授權裝置的存取，表示您可以封鎖網路犯罪者一般用來做為惡意程式攻擊第一步的關鍵進入點。

所有 USB 裝置的連接都會受到監控與分析，因此可以在事件調查與回應流程期間，將不適當的 USB 用途辨識為可能的攻擊來源。

SIEM 整合

Kaspersky Embedded Systems Security 現在可以將應用程式記錄轉換為 Syslog 伺服器支援的格式，因此這些記錄可以傳輸至所有的 SIEM 系統，並且讓這些系統順利辨識。

記憶體防護

Kaspersky Embedded Systems Security 現在可以防護處理程序記憶體不受入侵程式影響。動態載入的處理程序防護代理程式插入受保護的處理程序，因此可以監控其完整性並減少弱點遭到入侵的風險。

集中式管理

安全原則、特徵碼更新、防毒掃描和結果收集，都可以透過單一的集中式管理主控台 Kaspersky Security Center 輕鬆進行管理。區域網路中的所有代理程式都可以透過任何本機主控台進行管理，這在使用嵌入式系統典型的隔離式區段網路時特別實用。

維護及支援

我們的營運範圍超過 200 個國家，全球擁有 34 間辦公室，全年無休致力於提供全球支援，我們的維護服務合約 (MSA) 支援套件亦表現出此特性。

我們的專業服務團隊隨時待命，確保您可以藉由安裝卡巴斯基實驗室安全防護獲得最大優勢。

如需進一步了解更有效保護您嵌入式系統的做法，請造訪 www.kaspersky.com/enterprise

防火牆及 CD/DVD 管理

考量到部分嵌入式系統攻擊的本質，防範惡意的內部人士活動非常重要。在網域範圍之外運作的嵌入式系統，其內部的 CD/DVD 光碟機和 USB 隨身碟應隨時受到集中管理的裝置控制以及防火牆保護。

檔案完整性監控

檔案完整性監控會追蹤範圍內的特定檔案及資料夾所執行的活動。您也可以設定在監控中斷期間追蹤檔案的變更。

記錄稽核

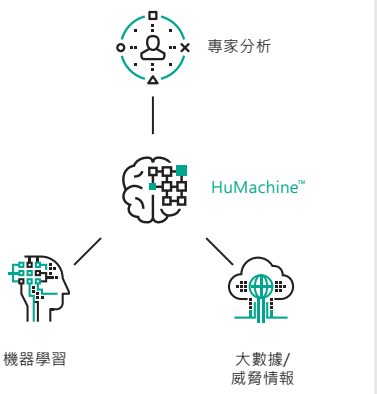
Kaspersky Embedded Systems Security 可以檢查 Windows 事件記錄檔，據此監控受保護環境的完整性。若應用程式偵測到可能為試圖發起網路攻擊的異常行為，會通知系統管理員。

此解決方案會檢查 Windows 事件記錄檔，並根據使用者或啟發式分析器設定所指定的規則來辨識入侵事件。

防毒軟體和 Kaspersky Security Network

防毒軟體以選購模組的方式提供。使用傳統的「防惡意程式方法」並不切實際，因為受到低階硬體的限制，而且在這種獨特的威脅情況下，傳統的方法大多無效。一旦以裝置控制和預設拒絕模式安裝 Kaspersky Embedded Systems Security，便不一定需要安裝額外的防毒，但可以在需要更高的安全等級時新增。

卡巴斯基實驗室也建議以 Kaspersky Security Network 知識庫的形式實行智慧安全，以防止和緩解入侵程式型安全風險，並將反應時間縮到最短。



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/

連繫 台灣卡巴斯基實驗室
OP@kaspersky.com.tw

真正的網路安全
HuMachine

www.kaspersky.com