Symantec
A Division of Broadcom

產品型錄

Symantec Critical System Protection
強化物聯網與操作技術

快速一覽

本文概述 Symantec Critical System Protection 強化物聯網與操作技術。

- 完整的物聯網防護
- Critical System Protection 可提供主機防火牆、裝置和組態控制、檔案完整性監控、入侵偵測、作業系統強化、應用程式許可清單、自動化沙箱，以及許多其他功能
- 強大的安全性
  - -- **自動沙箱**
  - -- **廣泛相容性**
  - -- **完整防護**
  - -- **自動化廠商互通性**

網路實體系統已成為日常生活不可或缺的部分，將自動化與智慧功能整合到我們的現實生活之中。但新的威脅也快速演化，鎖定這片富饒又極為脆弱的新大陸。

隨著各行各業將運算與連線能力內嵌至各種裝置，例如：汽車、噴射引擎、工廠機器人、醫療設備與工業用可程式化控制器等，而因安全漏洞所引發的後果也日益嚴重。

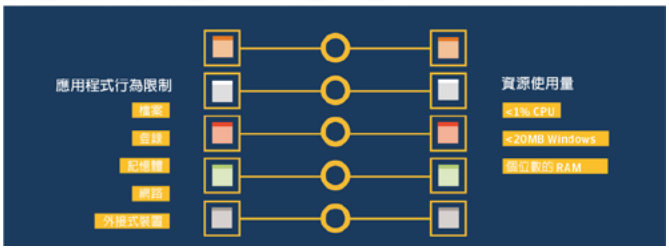
完整的物聯網防護

Symantec Critical System Protection 是一種精巧的安全引擎，可為您的物聯網 (IoT) 裝置提供最全方位和最深度的保護。Critical System Protection 可依照物聯網裝置的固定式功能和可預測性啟用政策，以定義系統的預期行為，僅允許執行非惡意和無毒的作業。

賽門鐵克防護 10 億台以上的物聯網裝置

Critical System Protection 已針對像是工業控制系統和操作技術等內嵌式系統和資源有限的環境最佳化，可擴增 EOL/EOS 和新作業系統，不用更新內容或特徵，也無需任何雲端連線。系統通過認證，能與衆多自動化廠商和機器人互連。

無論您的工業控制系統已有 20 年之久，或為全新的機器，Critical System Protection 都能相容並提供穩固的保護。



Critical System Protection 功能

Symantec Critical System Protection 可提供主機防火牆、裝置和組態控制、檔案完整性監控、入侵偵測、作業系統強化、應用程式許可清單、自動化沙箱，以及許多其他功能。

尺寸精巧

Critical System Protection 採用核心層級的保護引擎，在 Windows® 平台上僅需 20 MB 記憶體，一般 CPU 使用量不到 1%。

應用程式控制

Critical System Protection 使用專利的自動隔離技術，可將應用程式限制在沙箱內，依各應用程式的需求提供最低權限存取，無需變更任何程式碼，亦無功能限制。

應用程式許可清單

Critical System Protection 在政策內提供應用程式許可清單功能， 可只允許指明的應用程式執行。此外，還能指定政策，以用在特定的應用程式和應用程式類型。如此一來，即使攻擊者取得遭入侵的憑證，Critical System Protection 也能阻止任何未經核准的行動嘗試。其精細的控制功能，可決定任何應用程式允許執行和不能執行的動作。

入侵偵測

Critical System Protection 政策提供數千條預建規則，可監控及強化整個作業系統，目僅需少量調整。此功能可監控檔案、設定、事件、記錄、應用程式行為等，基本上涵蓋了整個系統，確保能立即偵測出任何的惡意軟體動作嘗試 。

入侵預防

Critical System Protection 可避免入侵造成損害，精細控制整個作業系統，封鎖任何未經授權的行為嘗試，讓攻擊者無功而返。

零時差攻擊防禦

零時攻擊行為是指在製造階段便存在的安全瑕疵，在您購買裝置時，裝置早有問題。Critical System Protection 使用預先建立的基準政策組，自動對已知的作業系統元件加已限制，並限制只能存取必要的系統資源。此外，採用將所有未知應用程式置入最低權限沙箱的政策，可避免主機系統上未知的應用程式遭到零時差攻擊。

網路上的惡意軟體控制

Critical System Protection 可控制應用程式的網路存取，這很重要，因為多數的惡意軟體會在安裝後立即透過網際網路散佈或下載其他的惡意軟體。由於 Critical System Protection 不會辨識惡意軟體， 因此也不會擔供網路存取。

強大的安全性

- **自動沙箱**：包圍程序、系統、記憶體、作業系統、登錄、Microsoft® PowerShell®、網路和其他資源
- **廣泛相容性**：支援任何內嵌式／非內嵌式／ POSReady Windows OS，最舊至 Windows NT、2000、XP、7、8、10、Linux®，以及 QNX® 受管或非受管模式
- **完整防護**：提供多階段的零時差防禦，和入侵預防系統與入侵 偵測系統組態
- **自動化廠商互通性**：CSP 夠輕量化，能輕鬆提供防護，不會干擾 SCADA/DCS 控制器、HMI 和機器人控制器的日常作業。

更多資訊

若要深入瞭解 Symantec Critical System Protection，請造訪 https://www.broadcom.com/solutions/integrated-cyber-defense 或保安資訊網站 https://www.savetime.com.tw/

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。
若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或
賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw