



保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

## 運用 Symantec 資料中心安全解決方案，保護容器化應用程式免受零日威脅

2026 年 7 月 1 日發布



點擊此處可獲取--最完整的賽門鐵克解決方案資訊

容器徹底改變了組織建置與部署應用程式的方式。無論是處理數百萬筆交易的線上零售商、運行微服務的金融機構，還是面向病患應用程式的醫療託管服務業者，容器都能提供現代企業所需要的速度與靈活性。

但這也為攻擊者創造了新的機會。

挑戰在於，許多攻擊並非始於已知的惡意軟體。相反地，攻擊者會利用先前未知的漏洞、濫用合法工具，或採用無檔案技術，而這些手法可能被傳統基於特徵檔偵測的安全解決方案所忽略。

**超越特徵檔偵測的資安防護：**當 Microsoft Exchange ProxyLogon 漏洞曝光時，全球各組織正忙於部署修補程式，而攻擊者則積極利用尚未修補的系統發動攻擊。在此期間，DCS 客戶得益於現有的防禦措施，即使在尚未有特定特徵檔偵測可用的情況下，這些措施仍能有效抵禦各種攻擊手法。DCS 透過結合入侵防禦、作業系統鎖定、應用程式控制、應用程式隔離及沙箱技術，實現了這項防護能力。

同樣的哲學也適用於容器化工作負載。

DCS 並非僅依賴偵測已知的惡意軟體，而是著重於控制哪些應用程式、程序和工作負載被允許執行哪些操作。

**遏止「利用現有資源」的攻擊：**現代攻擊者越來越傾向於使用合法的系統工具，而非惡意軟體。

例如：在入侵容器化應用程式後，攻擊者可能會嘗試執行：

- PowerShell
- 命令列殼層
- 網路工具
- 腳本引擎

這些工具之所以常被使用，是因為它們原本就存在於該環境中，且能夠規避傳統的偵測機制。

DCS可制定政策，讓企業能定義哪些子程序允許從特定應用程式中啟動。若某個網路服務突然試圖啟動殼層或腳本引擎，該動作將被立即阻擋。

此方法與 DCS 長期以來為 Microsoft Exchange 和 IIS 環境等關鍵任務工作負載所提供的保護措施道理相同。

容器安全不僅僅是部署前對映像檔進行掃描。基於容器的攻擊最終目標在於「容器逃逸」——徹底打破隔離邊界，直接在主機上執行程式碼。此攻擊向量的典型例子便是 CVE-2022-0492，這是一項高嚴重性漏洞，涉及 Linux 核心對 cgroups v1 release\_agent 功能的處理；由於權限驗證不當，導致容器內的 root 使用者能逃逸至主機命名空間。

許多成功的攻擊發生在部署之後，情況包括：

- 發現新的漏洞
- 憑證遭竊
- 受信任的應用程式遭到入侵
- 攻擊者取得執行時存取權限

預設的 DCS Linux 防禦政策會限制未經授權或容器化的守護程式向 /sys/fs/cgroup/ 下的敏感系統檔案結構寫入資料。即使底層的 Linux 核心在執行命名空間權限檢查時出現誤判，DCS 代理程式仍會在核心層級阻擋該寫入操作，從而瓦解此種突破防禦的技術。

DCS 透過多層次防護來應對這項挑戰，因此容器技術不僅加速了創新，也改變了資安格局。企業已無法僅仰賴漏洞掃描和基於特徵檔偵測的偵測來保護關鍵工作負載。

賽門鐵克資料中心安全解決方案透過主動式防範控制、應用程式隔離、作業系統鎖定以及執行時防護功能，為容器化應用程式提供安全保障，旨在阻擋已知與未知的威脅。

在這個世界裡，下一波攻擊可能會利用尚未被發現的漏洞，因此以預防為基礎的安全措施，仍是目前最堅實的防禦手段之一。

如欲進一步了解賽門鐵克的資料中心資安解決方案，請點擊 [此處](#)。

原廠網址：<https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-protecting-containerized-applications-from-zero-day-threats-with-symantec-data-center-security>  
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。



### 關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，

是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦 (CA Technologies) 以及雲端運算及「硬體虛擬化」的領導廠商--VMware，也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署 (CISA) 宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC (Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。



### 關於保安資訊 [www.savetime.com.tw](http://www.savetime.com.tw)

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。  
保安資訊連絡電話：0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家  
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>