
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

# 最能兼顧安全與持續運轉～保護Microsoft SQL Server免受勒索軟體威脅的首選：Symantec Data Center Security

2024 年 4 月 16 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

## 勒索軟體鎖定資料中心的攻擊正在竄升

勒索軟體威脅以多種不同的方式產生，並利用各種入口來入侵企業，但攻擊者越來越常用的一種方法是直接鎖定資料中心的伺服器和工作負載服務作為攻擊鏈的初始步驟。這些系統可能無法安裝建議的修補程式，通常還在繼續使用供應商早已不再提供更新的老舊的應用系統／程式，或者工作負載可能無法安排進行修補更新，以保持企業營運的持續性 (BCP)，避免由於任何停機時間而導致的風險。因此，資料中心環境遭受網路攻擊和勒索軟體活動的風險非常高。入侵單個資料中心可以存取多個相互連接的系統和應用程式，進而將攻擊的潛在影響最大化。

資料庫工作負載承載著企業的敏感性資料，為關鍵任務業務提供服務動能，所以成為勒索軟體攻擊者竊取資料並透過加密關鍵資料檔案勒以索贖金的重要目標。雖然有許多不同的資料庫應用程式，但 Microsoft SQL Server 是全球最受歡迎的資料庫之一，也是勒索軟體最虎視眈眈的目標，這主要是因為它部署在 Windows 平台上，攻擊者在 Windows 上有大量惡意軟體工具可用作有效酬載，也有一些可以利用就地取材攻擊 (living off the land)。

## 微軟的 SQL Server--主要的攻擊目標

最近報告凸顯一種模式，即勒索軟體攻擊者將 Microsoft SQL Server 作為其進入資料中心的開端。沒有妥善配置的 SQL 伺服器和薄弱的管理員密碼為暴力攻擊或 SQL 注入攻擊另闢蹊徑，讓未經授權的存取和資料外洩常常不費吹灰之力。遭入侵的系統可能會被用作存取點出售給其他方，或用於安裝額外的惡意有效酬載，最終實現資料滲出或金錢勒索。最近，美國網路安全暨基礎設施安全局 (CISA)，通令軟體發行商採取預防措施消除 SQL 注入漏洞，這突顯出企業需要特別注意 Microsoft SQL 伺服器的安全性。CISA 的通令是針對檔案傳輸應用程式 MOVEit 中的 SQL 注入漏洞發出的，該漏洞已被 CL0P 勒索軟體利用來做遠端執行程式碼。

針對 Microsoft SQL Server 的一些著名網路威脅活動包括

- Mimic勒索軟體 (Mimic ransomware)，透過對暴露的 Microsoft SQL 伺服器進行暴力攻擊獲得初始存取權限
- Mallox 勒索軟體，使用字典暴力攻擊進行初始存取嘗試，然後執行 cmd shell 進行進一步活動
- CLR SQLShell，類似於用於在 Microsoft SQL 伺服器上執行 shell 命令的 xp_cmdshell 預存程序
- CL0P 勒索軟體利用 MOVEit 檔案傳輸應用程式中的 SQL 注入零日時差漏洞 CVE-2023-34362，安裝名稱為 LEMURLOOT 的 web shell。
- Freeworld 勒索軟體是 Mimic 的新變種，也是透過暴力手段存取不安全的 Microsoft SQL 伺服器
- Bluesky 勒索軟體還透過暴力登入 sa 帳戶獲得初始存取權限，然後啟用 xp_cmdshell 預存程序來執行 shell 命令

## Data Center Security--有效的解決方案

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：提供一種全面的縱深防禦方法，可確保 Microsoft SQL 伺服器和底層作業系統的安全。我們的解決方案能夠有效提供零時差保護，抵禦日益猖獗的勒索軟體攻擊和其他針對資料中心環境的網路威脅。

## 為Microsoft SQL Server量身打造的DCS沙箱

專用於 Microsoft SQL Server 的賽門鐵克 sym_win_hardened_sbp 強制政策具有最小權限原則建構的內建 DCS 沙箱 (mssqlsrv_ps)，用於鎖定 Microsoft SQL 工作負載：

- 網路控制為用戶端應用程式與受信任的網路和設備之間定義其邊界，以限制其初始存取。此外，您也可以只讓可接受的通訊埠上進行網路連接。
- 啟用軟體執行控制後，可防止在未經授權的情況下任意執行命令直譯器，例如：cmd.exe、cscript.exe。這可以有效防止利用系統命令進行惡意活動的就地取材攻擊，並防止接觸 C&C 伺服器下載有效載荷和進一步的命令。
- 軟體安裝限制和作業系統限制可防止任何企圖常駐以便後續存取和對關鍵 Windows 作業系統資源篡改的行為。
- 程序存取控制防止使用 procdump 或 Mimikatz 工具轉存 LSASS。
- 受保護應用程式控制可確保在信任 MS SQL 程序執行的同時，它們不會被用來安裝批次檔、powershell 腳本、Cobaltstrike、Mimikatz 等工具和勒索軟體程式類型的惡意軟體有效酬載。

## Symantec Windows Baseline Detection Policy

Symantec Windows Baseline Detection Policy 具有 Microsoft SQL Server 監控規則集，可提供 SQL 伺服器事件的可見性，並對可能的可疑活動發出警報：

- Microsoft SQL Server Login Activity Monitor 可審查 Microsoft SQL 伺服器 sa 帳戶的成功和失敗登入，有助於對暴力攻擊發出警報
- Microsoft SQL Server Service Activity Monitor 會列出 Microsoft SQL 服務的啟動和停止情況
- Microsoft SQL Server File and Registry Monitor 可即時監控任何篡改 SQL 伺服器檔案和註冊表資源的行為。

保護資料中心的環境，尤其是資料庫工作負載的安全非常重要。企業必須優先採取安全措施，包括及時安裝修補程式、強大的存取控制和持續監控，以降低勒索軟體滲透的風險，保護敏感性資料不被利用。這些開箱即用的賽門鐵克資料中心安全預設政策，可確保針對資料中心伺服器和工作負載入口點嘗試的上升趨勢提供強大的保護。

要了解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

## 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

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 年起就全心全力於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，以及基於比原廠更孰悉用戶環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。保安資訊連絡電話：**0800-381-500**。