# 資料洩漏總是後知後覺

2024 年 2 月 7 日發布｜專家觀點

Rob Marti
賽門鐵克產品行銷經理
(屬於博通軟體事業群)

## 現在您可以採取哪些措施來保護關鍵和敏感資料

上週發現歷史性資料外洩事件。雖然這些被盜的資料對受害者的長期影響仍未知，但我們預計損失將會很高。據 IBM 研究，到 2023 年，全球單一次資料洩漏的平均成本將達到 445 萬美元的歷史新高。僅投資資料洩漏預防技術已不再是解決問題的方法。就在本週，能源管理和自動化巨頭施耐德電機成為頭條新聞，因為有消息稱該公司遭受 Cactus 勒索軟體攻擊，導致數 TB 的公司資料被盜。

組織需要了解資料洩漏事件是時間早晚的問題、而不是會不會的問題，並且必須保護其關鍵資產，從客戶和員工資料、智慧財產權到財務資料、業務計劃甚至原始程式碼。資料應在生命週期的每個階段受到保護，從資料進入組織直到被銷毀。在本文中，我們將探討為什麼資料如此難以保護，並分享寶貴的見解，以幫助您開發強大而有效的資料生命週期保護。

## 從資料保護開始

越來越多組織將邊界的安全轉向採用零信任框架。如今，「身份」已成為新的邊界。事實上，零信任框架的前兩個原則是：「驗證每個請求存取的使用者和裝置的身份」和「強制執行最小權限」。這有助於組織防止未經授權的資料存取。這是一種由外而內的觀點。然而，第三個原則「假設資料已經洩漏」則採取不同的視角。現在你要問自己的問題是：好吧，儘管我有所有的安全層級，但一個壞人已經進來了。我如何減輕他所造成的損害？我可以做什麼來進一步降低資料被盜的風險？這是一種由內而外的觀點。

這就是我們的故事開始的地方--資料：它是在哪裡被建立？它儲存在哪裡？它是如何使用？什麼時候不再需要了？它是如何被銷毀？企業需要關注資料生命週期的每個階段並詢問：我該如何保護這些資料？如果有人突破我的一層或多層安全措施，我該怎麼做才能最大程度地減少損失？我們是否擁有完整資料保護生命週期的所有保護措施？

請記住，資料無所不在--從大型主機和企業設備到多混合雲環境。隨著資料的成長，風險也隨之增加。例如：假設資料進入組織並進入單一資料庫。然後，您會發現該資料被複製到其他資料庫或其他使用者儲存位置五次。問問自己：這有必要嗎？我真的需要為惡意用戶建立五個目標來執行我的業務嗎？有些組織在一百個不同的地方擁有相同的資料。您所需要做的就是在其中一個地方犯一個錯誤，這樣就會使資料面臨風險。了解您擁有哪些資料，如果資料位於

多個位置，請將其整合--保護一個位置比保護數百個位置更容易。

以資料為中心的安全方法意味著所做的每項決策、執行的每項策略和採取的每一項行動都是以資料保護為首要考量。以資料為中心的實作依據每個控制點套用強大的 DLP，為 Web、SaaS 和私人應用程式套用一致的策略。 DLP 為使用中、動態和靜態的資料提供保護。但事情並沒有就此結束。作為最終的保護措施，還有最後一道以資料為中心的保護措施--加密。

## 加密：資料洩漏的最後一道防線

在我們最近出版的電子書「Welcome to the Jungle: Safeguarding your most valuable asset -- your data」中，我們對資料保護的挑戰進行全面概述，並提供五種有價值的最佳作法，可以幫助您解決資料生命週期保護策略。雖然我鼓勵您下載此資源以獲得我們的完整建議，但讓我們仔細看看五種最佳實踐之一，「加密您保管的資料，並當您不再需要時將其完全銷毀」。

監管單位的要求使加密成為許多公司必要的防護措施。需要遵守持續診斷和緩解威脅 (CDM)、支付卡產業資料安全標準 (PCI DSS)、健康保險流通與責任法案 (HIPAA) 以及歐盟通用資料保護規範 (GDPR) 等法規，企業必須實施可稽核的加密解決方案，保護客戶資料的隱私。加密資料也是最後一道防線--即使敵手已經突破您的每一層保護，他們依然無法存取它。這是緩解減資料洩漏後傷害影響的最後機會。

Symantec PGP® Encryption Suite 是一個新的多料號套裝，透過三種產品提供靈活的靜態資料和傳輸中資料保護。Symantec Endpoint Encryption 將強大的全磁碟和抽取式媒體加密與直覺的中央管理平台結合，以防止敏感資料遺失或被盜。它還可以幫助管理員證明設備在遺失時已加密。 Symantec PGP File Share Encryption 擴展檔案伺服器存取控制，包括強大的點對點加密。管理員可以為文件、工作表、簡報、影片檔和聲音檔等內容設定加密政策。

Symantec PGP Encryption Suite 還提供透過第三種產品 Symantec Desktop Email Encryption 來保護動態資料的選項，該產品透過自動加密、解密、數位簽章和訊息驗證來保護電子郵件通訊。此加密過程發生在用戶端 (Client) 級別，確保檔案傳遞在穿越內部網路或儲存在雲端儲存庫之前就已經完成加密確保安全。您可以在我們的解決方案簡介「Safeguarding Data throughout Its Lifecycle」中找到更多有關該解決方案在整體資料保護策略中可以發揮作用的詳細資訊。

## 下一步是什麼

隨著州長於 2024 年 1 月 16 日簽署新澤西州隱私法，新澤西州成為美國第 14 個通過全面資料保護法的州。展望到年底，我們預期資料保護的需求將持續發展，處罰也將增加。好消息是，您今天可以採取一些措施來降低風險。我們邀請您聯絡 Broadcom，了解我們如何提供協助。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/after-breach
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。2024/2

## 關於作者

### Rob Marti

賽門鐵克產品行銷經理 ( 屬於博通軟體事業群 )

作為產品行銷經理，Rob 負責博通軟體事業群旗下賽門鐵克的 PAM 和 IAM 產品組合的資訊傳遞、定位和上市戰略。Rob Marti 在身份認證和存取管理領域擁有超過 19 年的經驗。

## 關於賽門鐵克 (Symantec)

Symantec
A Division of Broadcom

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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

## 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**。