透過 Zerto 打造數據安全方舟計畫 Cyber Resilience Vault

被勒索軟體攻擊後，如何在實體隔絕環境極速還原

近年來，勒索軟體（ ransomware ）及網路攻擊之頻仍、嚴重、複雜程度皆不斷升高。IDC（ International Data Corporation，國際數據資訊有限公司） 近期出爐的一篇研究顯示，過去十二個月，企業進行災難復原（ disaster recovery ）的原因，多數為遭受勒索軟體或惡意軟體攻擊。隨著勒索軟體成為一項服務，執行網路攻擊的成本愈來愈低，而企業支付的贖金，更成為駭客開發次世代惡意軟體的資金。

企業需採取主動、強大之縱深防禦策略，先一步預防並阻止攻擊 - 即所謂「戰前防衛」（ left of boom ）技術。同樣重要的是「戰後修復」（ right of boom ）技術，主要著眼於受攻擊後的復原。企業組織必須採用可組合式（composable）資料保護機制，建立起快速、可擴充的解決方案，才能於遭受攻擊的第一時間發現、應變、還原。

今日尤其必要

儘管預防性「戰前防衛」解決方案不斷改良，但企業 IT 需符合的標準也日趨嚴苛。當前，資安保險公司紛紛要求企業採取更完善的保護措施，包括使用資料保險庫（vault）服務。美國的情況尤其如此，美國證券交易委員會（SEC）已在研議以更嚴格的標準要求上市公司，包括須指定資安韌性策略負責人。資安韌性的重要度已來到新高，全面而嚴謹地處理此問題，刻不容緩。

使用傳統資料保險庫Vault（Traditional Vault），您安心嗎？

一般資安韌性對策，仰賴有風險的資料保險庫（Vault）技術及架構。最為人詬病的問題之一為還原速度，即所謂的「RTO」（recovery time objective，復原時間目標）。從磁帶提取，或由較低層（lower tier）儲存區移回壓縮的檔案，使還原過程可能拖延數日、甚至數週之久。若需掃描辨識乾淨檔案，或還原至營運級陣列（production-grade array）以外的地方，更是曠日費時。如果有調查單位或資安小組欲針對企業基礎設備進行鑑識分析（ forensic analysis ），資料復原後，您可能須暫時將業務轉移至別處進行 - 沒有任何專用備份設備（PBBA）或雲端冷儲存服務（cold cloud storage）能支援這項需求。迅速恢復正常營運攸關企業命脈，然而傳統備份或檔案庫（archive）解決方案並非為此設計。

Zerto 協助企業快速復原

Zerto 為美國慧與科技 Hewlett Packard Enterprise（HPE）旗下公司，能為企業量身打造堅若磐石的還原資料保險庫（vault），即使遭受最兇猛的勒索軟體攻擊，亦能順利降低危害。Zerto數據安全方舟計畫Cyber Resilience Vault提供三大後盾，採用去中心化、零信任（zero trust）架構運作，能隨時於實體隔絕（air-gapped）環境，極速還原企業資料。

備份及偵測

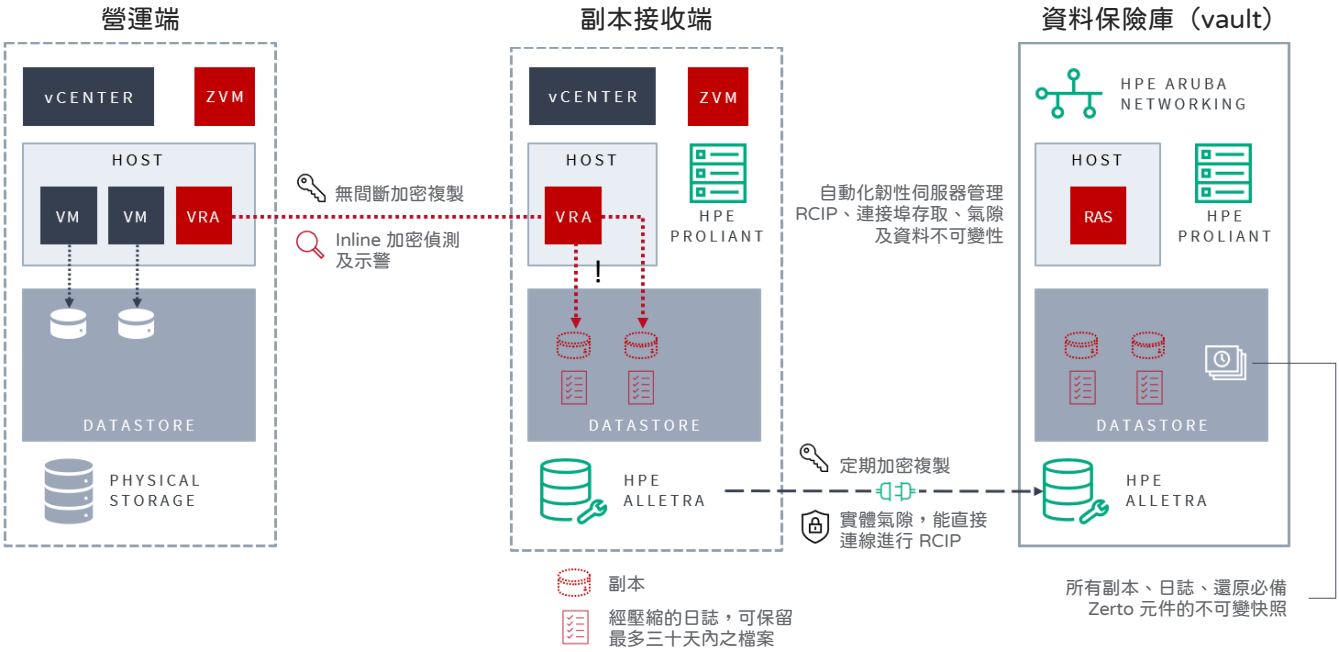
近同步串流資料副本，即時保護營運端的任何寫入，並於可疑異常出現時立刻察覺、發出警示。

隔絕及上鎖

資料保險庫（vault）獨立設置於運用氣隙（air-gapped）實體隔絕網路的環境，能將資料副本以不可變（immutable）方式，儲存於安全、高效能、符合美國聯邦資訊處理標準（FIPS）的硬體設備。

測試及還原

輕鬆辨識出乾淨還原點，迅速將多 VM（virtual machine，虛擬機器）應用程式完整還原至高效能儲存設備，同時保持跨 VM 一致性，即使 VM 數量破千亦游刃有餘。



運作方式

這套資安韌性解決方案，核心為 HPE Alletra、HPE ProLiant、HPE Aruba Networking 及 Zerto 的厚實技術，基礎架構方面融入三項關鍵概念，分別對應了前述的三大後盾。

1 副本接收端

此為採用 vSphere 虛擬化架構的著陸區域（landing zone），透過安全方式與企業營運環境配對，可設置於本地或遠端。設於遠端時，它亦可同時作為傳統異地備援地點。這個區域為 Zerto「無間斷資料保護」（continuous data protection，簡稱CDP）技術的副本接收端（replication target）。Zerto 的 CDP 採無代理（agentless）模式，因此惡意軟體將無法停用或劫持受保護的 VM 內之任何部分。受保護的各 VM 上一旦有任何寫入，均會經過加密、壓縮、傳送至副本接收端，並儲存於動態 CDP 日誌中——即一個包含數千復原點，維持跨 VM 一致性及原有寫入順序的串流紀錄檔。日誌保留期限可自訂，最短一小時、最長三十天，遭勒索軟體攻擊時，由日誌還原為最優先及最佳的選項。

日誌及所有相關副本，皆會送至虛擬設備（virtual appliance），這些虛擬設備在 HPE ProLiant 伺服器上運作，使用 HPE Alletra vLUN 作為數據儲存區（datastore）。Zerto 將寫入複製到日誌中的同時，會利用即時加密偵測（encryption detection）檢查檔案，一旦發現疑似感染的跡象，便能於第一時間送出警示。您亦可透過 API（應用程式介面）查看加密分析，進一步評估及視覺化目前的資安解決方案堆疊（solution stack）。

2 數據安全方舟計畫（Cyber Resilience Vault）

資料保險庫（vault）與副本接收端位於相同地點，亦同樣採用 HPE ProLiant 與 HPE Alletra 技術。此一獨立隔絕的資料保險庫（vault），就像一間無塵室，藉由實體氣隙，達到隔離外部網路及營運網路的效果。由於去除了中心化的控制層（control plane），資料保險庫（vault）並不具有暴露的管理連接埠（management port），因此攻擊者無法經由單一破口（single point of compromise）入侵。備援地點的 HPE Alletra 與資料保險庫（vault）內部的 HPE Alletra 之間，能直接連線進行 RCIP（remote copy over IP，經 IP 遠端複製），將備援地點的所有資料，包括 Zerto 日誌及副本，點對點複製一份至資料保險庫（vault）。此方法結合了同步複製的優點（包括高效能、極低RPO［recovery point objective，復原點目標］等）及傳統非同步複製之益處（包括佔用空間較少、延遲容忍能力［latency tolerance］更強等）。

3 資料保險庫（vault）自動管理

資料保險庫（vault）內部的自動化韌性伺服器（Resilience Automation Server，RAS）為一台輕量化 VM，能與 HPE Aruba 及 HPE Alletra的原生服務配合運作，控制資安韌性的關鍵措施，包括：

- 啟用及停用 HPE Alletra 上的 RCIP，確保資料保險庫（vault）為眞正與外部隔絕的環境。
- 隨機分配複製連接埠，降低傳輸行為之可預測性。
- 創建快照，並以 HPE Alletra 虛擬鎖（Virtual Lock）技術保障快照不可變性（即使 HPE 技術支援團隊，亦無法覆寫這項防竄改保留鎖定［retention lock］）。
- 於外部遭受入侵時，在資料保險庫（vault）內部還原 Zerto 虛擬管理員（Virtual Manager）、日誌、副本，重建乾淨的 Zerto 部署。
- 記錄資料保險庫（vault）內部所有活動，以供稽核。

還原流程

Zerto 此套架構能對付數種不同感染情境，包括：

檔案／資料夾／VM 感染：若勒索軟體攻擊的範圍不超過一台 VM 上的檔案或資料夾，Zerto 能近即時將其復原，從遭受感染前五至十五秒的日誌時間戳記（timestamp），將相關檔案或資料夾還原至原始位置。若一或多台 VM 遭到勒索軟體加密，Zerto 亦能近即時將資料還原回營運端，無需透過任何間接步驟（例如藉由 Storage vMotion 進行遷移）。這項還原功能，同樣可適用於構成多 VM 應用程式堆疊（application stack）的所有 VM，且還原時使用完全相同的乾淨時間點檢查點（point-in-time checkpoint），以秒為單位區隔，並維持原有時間順序，而非仰仗分散於夜間備份時段中、參差不齊的時間戳記。

工作負載全面感染：若營運／原始資料場址的所有 VM 皆遭感染，但備援地點仍可正常運作，Zerto 會執行完整的故障轉換（failover），確保停機時間不超過幾分鐘。由於 HPE Alletra 為頂尖營運級儲存設備，專為關鍵任務工作負載（mission-critical workload）而設計，應用程式將能從備援地點直接執行，效能不打折扣，也毋須另外遷移資料至能支援工作負載的其他儲存設備。

多場址感染：假如營運地點及備援地點皆被攻擊而無法運作 - 例如 host 遭加密，或網路分割無法防止快速橫向入侵 - 這時，Zerto 的數據安全方舟計畫 Cyber Resilience Vault 便成為一間最安全的無塵室，供企業於其中進行還原。主要還原步驟摘要如下：

1. 重建備援地點：在獨立隔絕的資料保險庫（vault）中，利用不可變快照重新部署 VMFS，同時保存 UUID（唯一識別碼）簽章。
2. 還原 Zerto：由於Zerto 具有強大韌性，此時虛擬管理員及資料轉移程式（data mover）會自動上線，毋需手動重新設定或安裝，即能接續先前的作業。
3. 還原資料：利用 Zerto 日誌，於數千個可用還原點中選取正確還原點，Zerto 將依照您定義的開機順序，重啟所有 VM。Zerto 的協調引擎（orchestration engine）配上 HPE Alletra 的頂尖效能，使 RTO 長度僅僅幾分鐘，不是數小時、數天或數週。多 VM 應用程式堆疊很快便能全數上線，且各 VM 還原至完全相同的時間點，使還原後需要的手動設定減到最少。

「為安全而生」遇上「為效能而生」

Zerto 數據安全方舟計畫 Cyber Resilience Vault 融合安全與效能，以滿足當前企業面對的各項規範要求，關鍵優勢包括：

- 實體隔絕網路的獨立資料保險庫（vault）
- 零信任架構
- 通過 FIPS 140-2 驗證
- 安全性加強的 Linux 虛擬設備
- 內建最小權限原則（principle of least privilege）
- 無法移除的虛擬鎖技術，保障遠端／離線副本不可變性
- NTP 防竄改保護
- Inline 即時加密偵測
- 可擴充至每座 vCenter 一萬台 VM
- 靜態加密（encryption at-rest）與傳輸中加密（encryption in-flight）
- 依據密文、時間、加密技術產生的強大密碼
- 備援地點儲存空間保證可用 99.9999%
- 營運級陣列，能執行任何高負載應用程式
- 搭載 AI、具自我修復能力的儲存設備
- 所有硬體採用晶片信任根（Silicon Root of Trust）技術
- 去中心化管理，杜絕單一破口入侵

開啟眞正的資安韌性

Zerto 數據安全方舟計畫 Cyber Resilience Vault，提供企業一個安全且高度客製化的選項，能針對自家業務量身訂做，建構最妥適的解決方案。Zerto 獨特、具彈性的架構，讓您的企業能於遭受攻擊時快速恢復，不再受勒索軟體威脅。

- 大幅縮短攻擊後的停機時間，避免蒙受直接或間接營收損失。
- 符合相關法規，包括歐盟 GDPR、美國 HIPAA、SOX 及聯邦資訊安全管理法（FISMA）NIST SP 800-34。
- 簡單不繁複：單一銷售者、單一解決方案，結合還原過程各步驟所需的最佳產品。

歡迎您與我們聯絡，取得產品展示、報價，或瞭解能從勒索軟體攻擊中迅速復原對於企業的重大意義。

聯絡我們