解決方案簡介

使用 FlashBlade SafeMode 減緩勒索軟體影響

利用 Pure Storage FlashBlade 與 SafeMode 提升資料安全性。

勒索軟體攻擊始終是企業與 IT 領導者的心頭大患。這並不難想像，勒索軟體攻擊侵入你的資料，後果可能不堪設想。預測2031年時，勒索軟體在全球造成的損失預計將超過2650億美元，每2秒就有一次新的攻擊[1]。雖然我們每年花費數百萬美元來保護資料登錄點，但許多人依然低估了加強資料保護的策略價值。

現有的資料保護可能不夠

一般情況下，備份可以完善保護資料，例如天災人禍的災後復原、資料毀損、管理人員蓄意破壞、意外刪除等。然而，勒索軟體攻擊對於現行資料保護架構的危害超出預期—尤其是建置在傳統基礎上，如磁碟和磁帶上的資料。

如果光是符合復原SLA就讓你力不從心，那麼勒索軟體造成的延長停機時間只會讓情況愈加惡化。備份系統和資料可能遭到破壞，若發生則需要重新安裝與重新配置備份解決方案，甚至在考量如何恢復資料之前就得完成。

保護恢復資料便能保障業務順暢

在勒索軟體襲擊之前、期間、之後確保資料安全需要仔細規劃，尤其攻擊者越來越傾向於發動具有針對性的攻擊。

附有 SafeMode™ 的 Pure Storage® FlashBlade® 可確保你從網路攻擊中恢復所需的關鍵資料，以便您能夠迅速重新開展業務服務，無需屈服於攻擊者的任何要求。SafeMode 是 Purity 作業環境的內建功能，在 FlashBlade 及 FlashBlade//S 中皆有提供。

完全牢不可破

即使管理憑證遭到破壞，也可確保資料不因惡意攻擊或管理失誤而造成加密外洩。

簡易的備份整合

FlashBlade 與現有的軟體與工具一起運作，所以你不需要改變現有軟體來改善備份和恢復目標。

迅速恢復

PB 級規模的恢復行動，讓你的業務能夠重新上線。

只要使用 SafeMode，在進行完整備份流程之後，便可為備份資料和相關中繼資料目錄建立牢不可破的唯讀快照檔。勒索軟體無法刪除、修改或是加密此種快照檔，即使管理員身分已遭盜用的狀況下也是如此。你能夠直接從快照檔中恢復資料，幫助你在勒索軟體攻擊後迅速回歸正軌。附有 SafeMode 的 FlashBlade 能為你帶來下列益處：

- **加強保護**：SafeMode 確保勒索軟體無法根除受保護的資料。
- **快速恢復**：FlashBlade 提供 PB 級的恢復行動，能夠迅速恢復你的業務。
- **備份整合**：FlashBlade 與你現有的資料保護軟體相容。
- **投資保護**：FlashBlade 內含 SafeMode，不收取額外費用。你的 Pure 訂閱或維護支援合約已涵蓋加強功能。

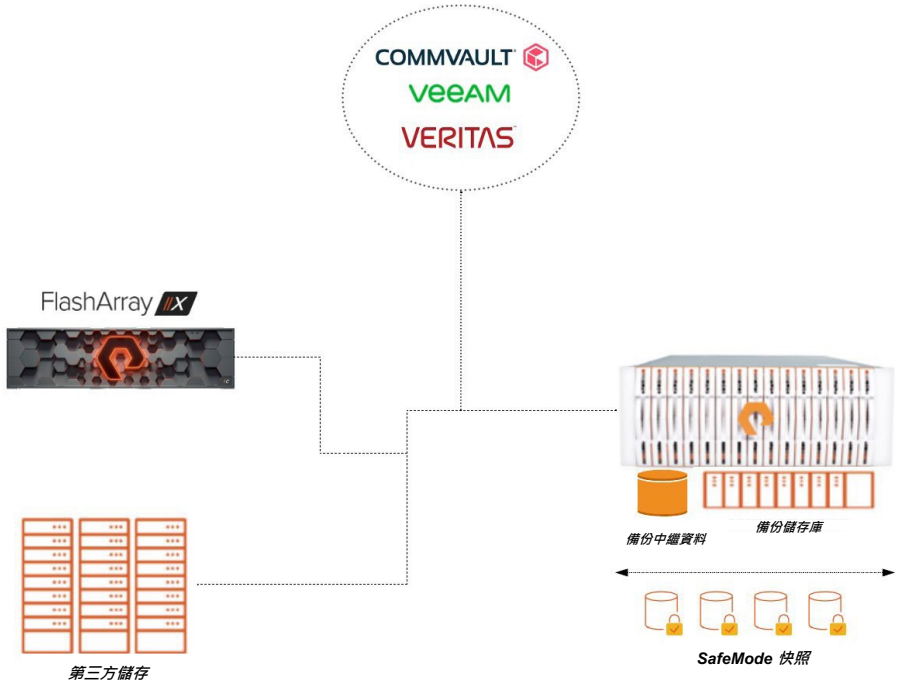

圖 1：使用 FlashBlade SafeMode 牢不可破的快照檔保護資料。

附加資訊

- 瞭解更多FlashBlade//S。
- 瞭解 SafeMode snapshots。
- 查看更多關於勒索軟體緩解及恢復的解決方案。

[1] *2022 年網路安全年鑑 (2022 Cybersecurity Almanac)*； Cybersecurity Ventures，2022年1月

PS1030-03 05/2022