解決方案簡介

Pure保護你免受勒索軟體危害

Pure Storage® FlashBlade™ SafeMode 快照功能，增進資料保護力

勒索軟體攻擊至今仍是業界與IT領導者的心頭大患。這是其來有自。它們危害了公司的命脈：資料，害得業務無法順利運行。可能造成嚴重後果。要不付錢請駭客幫你解碼資料，還不一定成功，或者自己用破解軟體瞎子摸象一番，不然就只能做備份復原賭一把了。每年業界花了上百萬美元替資料的入口點做防毒，卻依然低估了提升資料保護性的策略價值。

你目前的資料保護可能不夠周全

妥善備份能保護重要資料免受危害，常見情況包括：自動復原、人為損害，或資料毀損。然而，勒索軟體攻擊可能會對現存的資料保護架構造成超乎預期的傷害，這些架構建置在老舊裝置上，像是磁片、磁帶等。

首先，即使復原時你已經面臨一連串的服務層級協議(SLA)轟炸，勒索軟體也會造成更長的停機時間，讓狀況惡化。再者，你的備份系統和資料可能遭受危害，因而需要重新安裝，備份解決方案也得重新配置，之後才是考慮資料復原。

你也許認為勒索軟體只會攻擊Windows系統，你的備份存在Linux的伺服器，因此不會受到影響。但是2019年一種全新類型的勒索軟體出現，名稱為Lilocked，又稱Lilu，它們專門針對Linux的伺服器及相關資料發動攻擊。[4]

企業的潛在威脅

2018年勒索軟體攻擊總件數雖然減少了，但針對商務企業發動的攻擊卻增加了12%[1]。

財務損失

Maersk每季因NotPetya類型勒索病毒而產生的損失就有2.64億美元之多[2]。

生產力減損

2018年，停機時間成本是勒索病毒平均贖金的23倍之多[3]。

[1] 2019年2月，Symantec公司，“網路安全威脅報告，卷24”。
[2] 2017年8月，《富比士》雜誌，“勒索軟體NotPetya攻擊Maersk，貨運巨頭損失逾$2億美元”。
[3] 2019年10月，Datto公司，“2019年勒索軟體概覽”。
[4] 2019年9月，SecurityIntelligence，“勒索軟體Lilocked感染上千台Linux伺服器將檔案加密”。

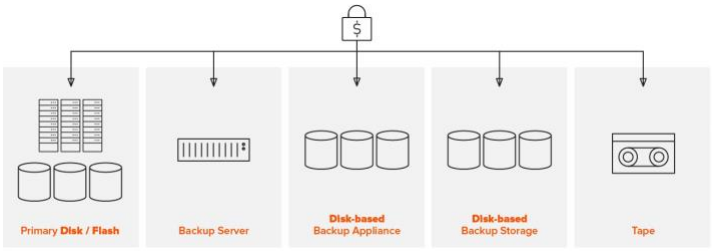

圖1：勒索軟體攻擊會損害資料保護架構的關鍵要素。

運用SafeMode快照功能，提升資料保護

Pure Storage®認知到勒索軟體的隱憂，我們很榮幸為大家介紹減輕資安攻擊危害的全新方案：Pure FlashBlade™。SafeMode快照功能內建於FlashBlade，讓你在進行全套備份之後能夠建立備份資料和相關詮釋資料目錄的唯讀檔。你可以直接從快照檔案復原資料內容，從此免受勒索軟體攻擊之擾，甚至一併排除行政程序上的異常行為。FlashBlade提供以下好處：

- **加強保護**：勒索軟體無法刪除、修改，或將SafeMode的快照檔加密。此外，只有經授權的公司指定人員可以直接使用Pure Technical Support來建置功能、修改使用政策，或手動刪除快照檔。
- **備份整合**：不論公司內部採行哪一款備份產品或本機裝置來管理資料保護程序，都適用相同的快照檔流程。
- **彈性使用**：快照檔的循環週期和刪檔排程皆可量身打造。
- **快速還原**：運用大規模的平行架構和隨著資料大小靈活應變的表現，來加快備份甚至復原速度。
- **投資保護**：包含SafeMode快照功能的FlashBlade不需額外花費。只要有Pure訂閱方案或維護支援合約即可享有此功能。

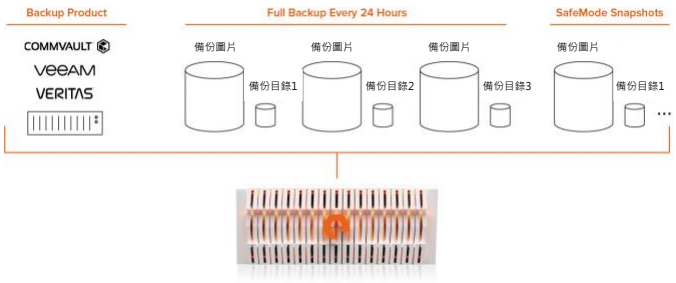

圖2：日常運作即會生成備份圖片及詮釋資料目錄的快照。

更多資源

更加了解SafeMode快照功能。

purestorage.com | 800.379.PURE

PS1030-01 11/2019