勒索病毒來勢洶洶

企業客戶如何因應？

Application

Background

2017年5月，WannaCry 勒索病毒造成全球大恐慌，台灣被列為此波疫情重災區；同年6月，新型態的勒索病毒 Petya 肆虐，再度引發用戶人心惶惶。根據手法的不同，勒索病毒被區分為多種類型，有會每隔一段時間就刪除一批檔案，超過時限未支付贖金則刪除全部檔案；有的則是鎖住電腦螢幕且加密檔案，類型達200多種。病毒變種防不甚防，唯一不變的是，對使用者帶來的心理恐懼和實質損失皆無法被等閒視之。

Challenges

WannaCry 勒索病毒利用作業系統漏洞，經網芳或 NAS 大舉入侵。系統管理者為維護企業資安，被迫關閉使用者習慣的檔案交換環境，如網芳或 NAS，造成員工使用不便。找尋資訊安全與辦公便利的平衡點，實為企業當務之急。

- 避免已知的資安漏洞，建置高安全性的儲存與分享空間
- 導入的解決方案須維持現有操作體驗，減少使用者學習時間成本
- 有備無患，存越多越安全，建立在高儲存成本上的資安是否為企業首選

Solutions

快速部署

ASUS OmniStor 能快速銜接現有IT架構，並支援多AD網域，降低管理成本；整合現有防毒軟體，體現高資安的雲端平台

有善介面

獨家的 Remote Drive 遠端檔案總管，直覺式拖拉資料，使用情境如同傳統網芳或 NAS，輕鬆上手無煩惱

檔案安全、儲存空間優化

- **多版本機制**: 檔案變動時自動備份，若本地端檔案不幸被綁架，可迅速取回先前版本
- **資料減量**: 大量存檔，易造成儲存空間的負擔，平台藉由資料減量技術去除重複資訊，有效率地維持兩者間的平衡