Actiphy

白皮書

沒有備份，就沒有資安 • 沒有備份，就沒有未來

No Backup, No Security • No Backup, No Future

Actiphy

摘要

隨著臺灣企業加速數位轉型，資料已成為企業營運的核心資產。但同時，這些數位技術也讓組織更容易受到網路攻擊、設定錯誤、內部威脅與系統故障的衝擊。

沒有可復原的資料，就沒有資安
沒有資安，企業就沒有未來。

Actiphy

資料是企業價值的核心

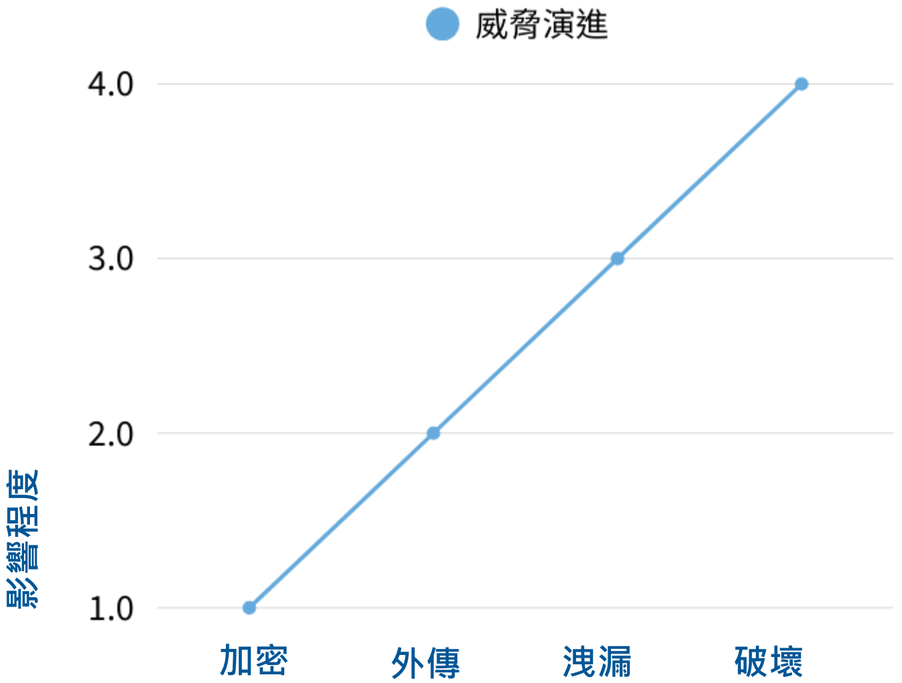
資料驅動著企業的各項運作：營運、決策、客戶互動、資料分析與 AI、以及法規遵循。一旦資料遺失或損毀，將立即導致停機、財務損失、法律風險、合規風險與客戶信任流失。保護資料就是保護企業價值本身。

保護資料等同於保護企業價值。

現代威脅正在針對 " 復原能力 " 下手

典型的「威脅進程模式」包含四個階段：

1. 加密（Encryption）
2. 竊取（Exfiltration）
3. 洩漏（Leak）
4. 破壞（Destruction）



攻擊者會刻意針對備份儲存庫、Hypervisor、雲端快照、備份設定檔與保留政策下手。

備份是最後的防線

- 在現代資安架構中，從端點/雲端、網路、身分與安全控管一路到備份/復原
- 備份與復原提供了最終且往往是唯一能確保營運延續的機制。

端點 / 雲端

網路

安全控制

復原 (備份)

Actiphy

威脅演進模型：為何影響會升級

攻擊進程階段

1. 加密 (Encryption)
2. 外傳 (Exfiltration)
3. 洩漏 (Leak)
4. 破壞 (Destruction)

升級的影響程度

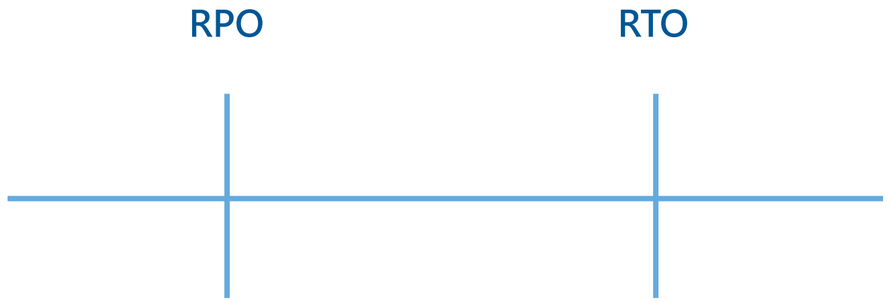
- 還原過程變得極度複雜化
- 業務停機時間顯著延長
- 損害蔓延至整個企業系統
- 法律與監管風險大幅增加
- 財務損失與品牌衝擊加速

結論：沒有安全異地備份或不可變備份的組織，
當破壞發生時可能面臨無法恢復營運的絕境。

RTO / RPO：決定韌性的兩個關鍵指標

RTO（復原時間目標）
RPO（復原點目標）

- 不是理論，而是企業的生存時間表。
- 無法在危機中達標，將面臨收入流失、SLA 罰款、客戶流失與供應鏈中斷。



Actiphy

3-2-1 原則：最低可行的備份策略

抵禦攻擊的起點

3	2	1
份關鍵資料副本	種存儲介質類型	份異地或不可變副本

實現韌性通常還需要：

- 不可變物件儲存
- 隔離式備份
- 持續或接近零 RPO 保護
- 自動化測試還原
- 備份與檢測技術深度整合

備份不只是保險，而是主動防禦的一部分。

Actiphy

備份是戰略性資安資產

備份是最後一道防線，也是安全的第一項要求

- 網路韌性 (Cyber Resilience)
- 從勒索軟體中更快還原
- 防止內部威脅
- 符合法律和監管要求
- 客戶信任的持續性
- 長期穩定性和競爭力

沒有備份，就沒有資安 • 沒有備份，就沒有未來

Thank You

備份軟體 Actiphy

ActiveImage Protector(AIP)是一款由日本Actiphy公司所研發的系統備份軟體，於台灣地區發行繁體中文版。ActiveImage Protector針對EFI&GPT磁區、Microsoft Hyper-V虛擬環境及Linux環境的備份有著非常優異的設計。

世達先進科技股份有限公司

https://www.gati.com.tw

02-2789-1100