NAKIVO

校務不中斷的秘密武器：現代資料中心備援全攻略

Evan Wang
大中華區產品技術
evan.wang@nakivo.com

為何需要保障資料？

NAKIVO

人為錯誤

勒索軟體攻擊

內部威脅

硬體故障

電源失效

自然災害

資料異常

軟體錯誤

勒索軟體的事實與數據

NAKIVO

59% 企業組織
2024年 攻擊

70% 攻擊
導致資料加密

94% 受害者
聲稱攻擊者瞄準了他們的備份

34% 受害者
花一個月以上才恢復

68% 受害者
使用備份資料恢復成功

57% 嘗試次數
成功了

$2.73 百萬
平均恢復成本
(不保含贖金)

$2 百萬
平均初始贖金要求

94% 初始贖金
支付

SOPHOS. The State of Ransomware 2024

勒索軟體的進化

	目標	攻擊方式	應對方式
之前	資料	加密	備份 & 還原
現在	資料 備份資料 備份系統 特定平台	加密 + 洩密 (雙重攻擊)	備份 & 還原 不可變動性 監控 早期偵測

NAKIVO®

為何需要
營運不中斷計劃

為何需要營運不中斷計劃

NAKIVO

1. **停機時間會摧毀企業**
   - 業務營運中斷
   - 聲望受損
   - 潛在客戶、收入和生產力損失
   - 法律費用/罰款

1. **備份不足以應對營運中斷**
   - 備份可以還原資料，但無法恢復業務營運
   - 備份可能需要數小時甚至數天
   - 沒有自動故障移轉/故障復原機制

停機會摧毀企業

NAKIVO

100%

2025年，企業因
停機而損失的資金

$300k/Hour

中小企業和大型企
業的停機成本

18%

聲稱其基礎設施已為災
難復原事件做好準備

24%

擁有災難復原計劃的企業

網路安全
不斷演變的威脅

- **人工智慧驅動的攻擊**：網路犯罪分子正在利用人工智慧製造更複雜的威脅
- **勒索軟體即服務 (RaaS)**：讓勒索軟體攻擊更容易被攻擊、傳播範圍更廣
- **新的惡意策略**：攻擊者不斷創新來繞過防禦
- **混合工作模式的風險**：遠端和混合工作環境帶來了新的漏洞

NAKIVO®

重新思考資料防護策略

今天的備份 → 明天的還原

資料防線？

備份、備份再備份 (很重要)

- 建立全方面的備份計畫
- 自動化備份流程
- 實行備份安全措施

NAKIVO®

備份的備份？

3-2-1 備份策略

3

至少建立三個副本備份資料
(1 主要備份和 2 備份副本)

2

儲存您的備份在兩個不同儲存媒介(NAS, 磁帶, 本地磁碟, 雲端, 等等...)

1

保留一份在異地端

NAKIVO®

備份目的端

Copy 1

內接式磁碟, 外接式硬碟, 外部儲存設備,USB隨身碟 ....等等

Copy 2

NAS設備或磁帶

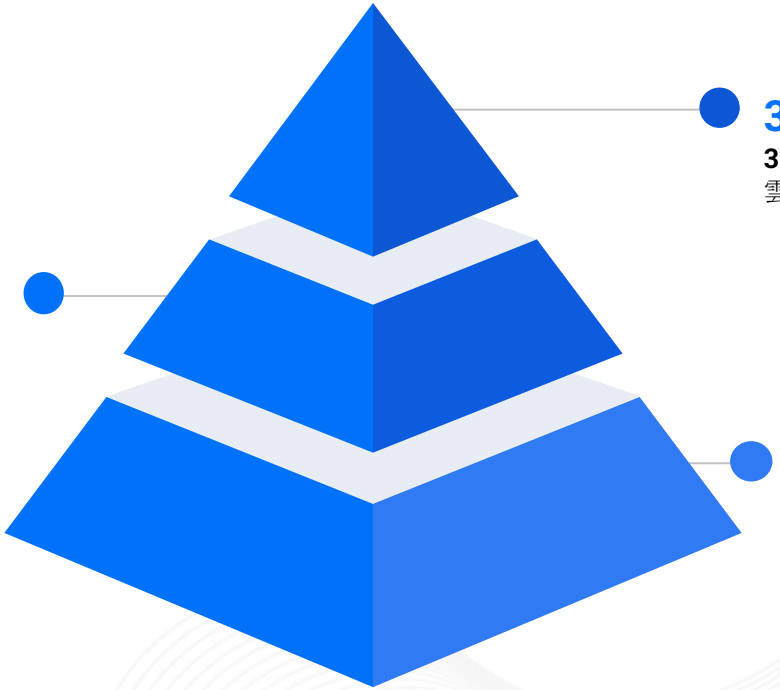
Copy 3

- 異地端儲存設備(NAS, 磁帶, 儲存設備)
- 公有雲(Azure, Amazon S3, Amazon EC2 or Wasabi)

NAKIVO®

備份法則 3-2-1：重新檢視備份策略

NAKIVO



3-2-1-1-0: 無錯誤恢復

3 個副本，儲存在 **2** 不同媒介，**1** 個異地/雲端，**1** 個離線，**0 備份資料錯誤**

3-2-1-1: 增加離線保護

3 個副本，儲存在 **2** 不同媒介，**1** 個異地/雲端，**1 個離線**

3-2-1: 基本策略

3 個副本，儲存在 **2** 不同媒介，**1** 個異地/雲端

NAKIVO®

全方面的備份計畫

企業混合架構

NAKIVO

本地系統架構

雲端或服務系統架構

提供完整資料保護

NAKIVO

自動化備份

NAKIVO®

簡化備份管理

讓資料保護變得簡單有效

- 使用規則自動化備份和複製 (機器名稱、大小、位置、標籤等)
- 使用行事曆模式追蹤資料保護活動避免重疊
- 使用全域搜尋快速尋找任何對象
- 透過HTTP API 輕鬆與各種第三方解決方案整合
- 從單一介面追蹤作業狀態、儲存區、傳輸等等

自動化：工作關連

備份完成後-->自動複製備份資料到

雲端空間/磁帶/異地點

NAKIVO Backup & Replication

自動化備份驗證

- 確保虛擬機可以成功啟動
- 截圖驗證與開機驗證方式
- 不需影響網路效能
- 透過網頁介面或郵件了解所有狀態

網路安全

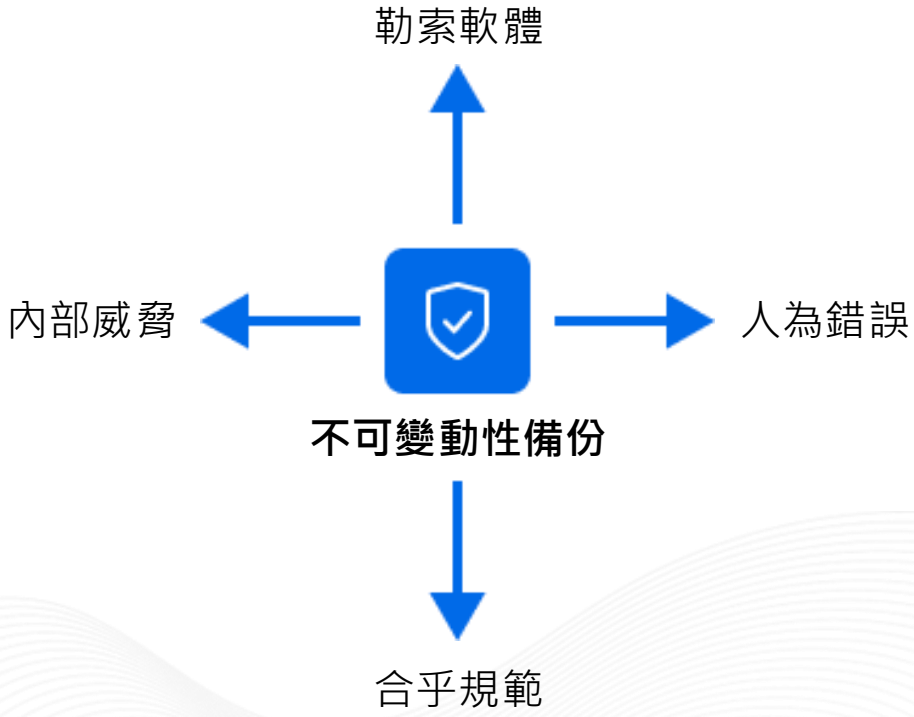
備份資料安全？勒索軟體威脅？

NAKIVO®

不可變動性備份

優勢

- 強大的勒索軟體防護
- 預防意外資料丟失
  (性能下降、人為錯誤等等)
- 簡化合乎規範
- 針對**內部威脅**的額外防禦



NAKIVO Backup & Replication
防勒索軟體的備份

- **不可變動性備份：** Write-once-read-many (WORM)
  - 公有雲： Amazon S3, Wasabi Hot Cloud, Backblaze B2 和 Azure Blob Storage
  - S3相容性儲存設備：支援物件鎖定
  - 本地端以Linux架構的儲存區
- **強化版AMI：** 透過Amazon Machine Image內建的Linux不可變動儲存區

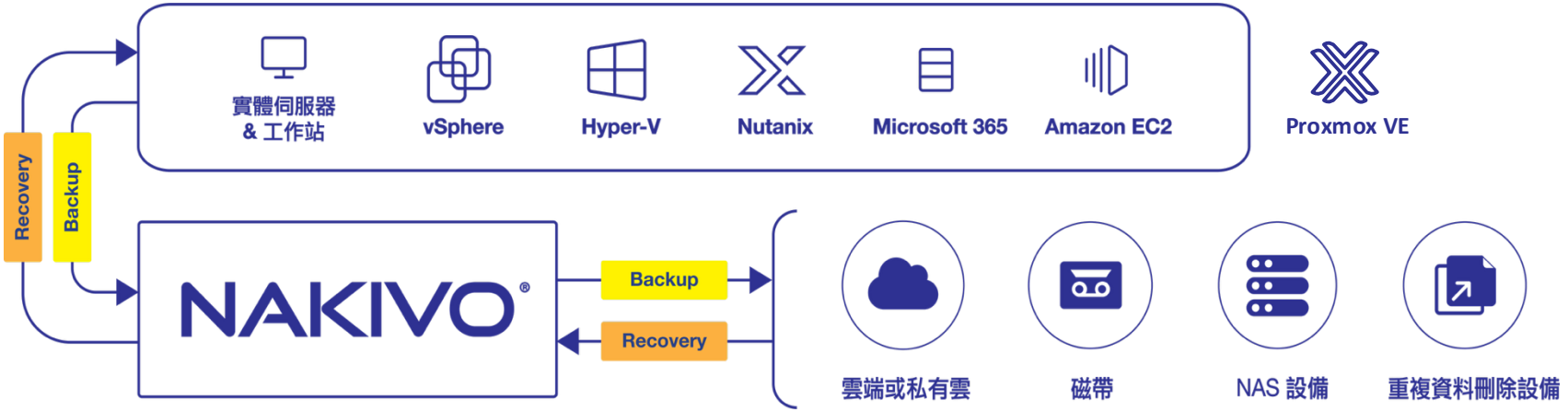
NAKIVO Backup & Replication

備份存取控制

- **備份檔加密**：加密備份資料與NAKIVO系統設定檔
- **AES 256-bit 加密**： 保護靜態和傳輸中的備份
- **雙因數認證 (2FA)**： 增加額外的安全層以防止未經授權的存取
- **基於角色的存取控制 (RBAC)**： 確保對資料保護活動的授權存取

提供客戶完整資料保護解決方案

NAKIVO



› **All-in-one 解決方案**
備份、複製、精細還原、勒索軟體防護、 災難恢復

› **支援虛擬、實體與雲端**
VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, Amazon EC2, Microsoft 365, Windows, Linux

› **全方面部署**
NAS, Linux, Windows, VA, AWS AMI

› **降低IT管理**
易學易用沒負擔

Thank You!

Evan Wang
大中華區產品技術
evan.wang@nakivo.com