資安的超級英雄：

如何打敗勒索者、擊敗病毒

備份是您的絕招！

Evan Wang
evan.wang@nakivo.com

NAKIVO®

資訊安全框架

NAKIVO®

https://www.nist.gov/cyberframework

主要資料損毀原因

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

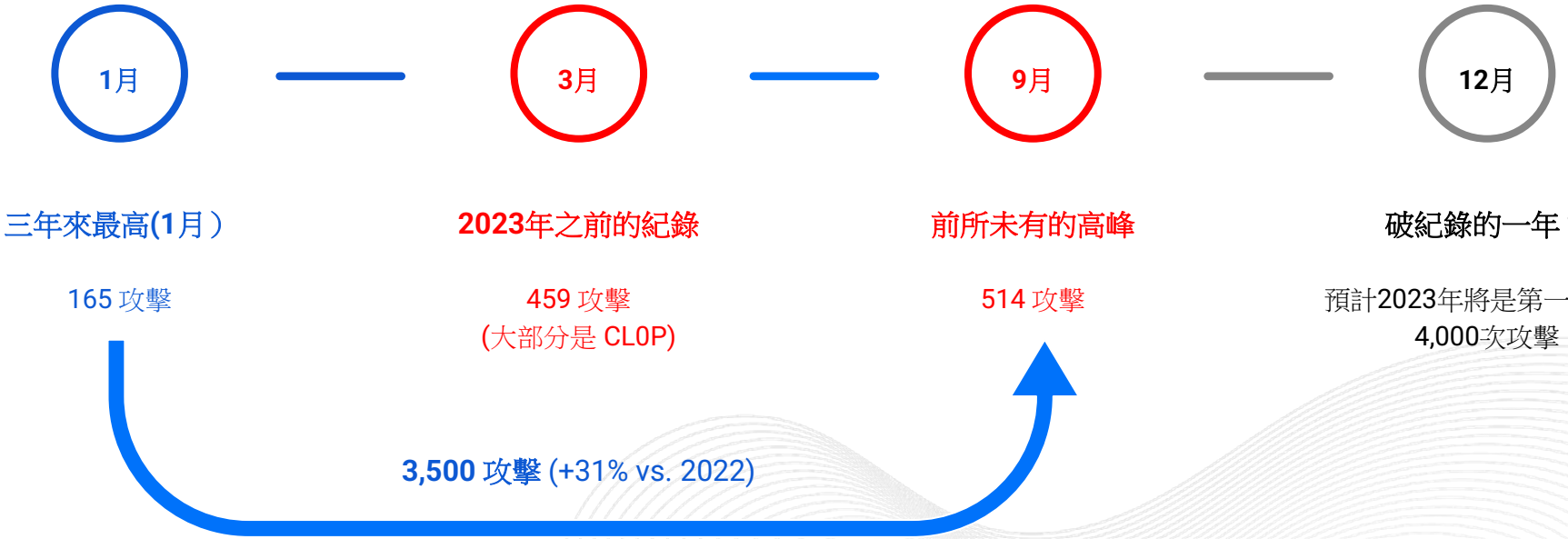
軟體錯誤

NAKIVO®

2023 勒索軟體回顧

勒索軟體的事實與數據

NAKIVO



勒索軟體的運作方式

NAKIVO®

佈局 → 感染 → 搜尋檔案 → 加密 → 贖金要求

新趨勢？

雙重攻擊

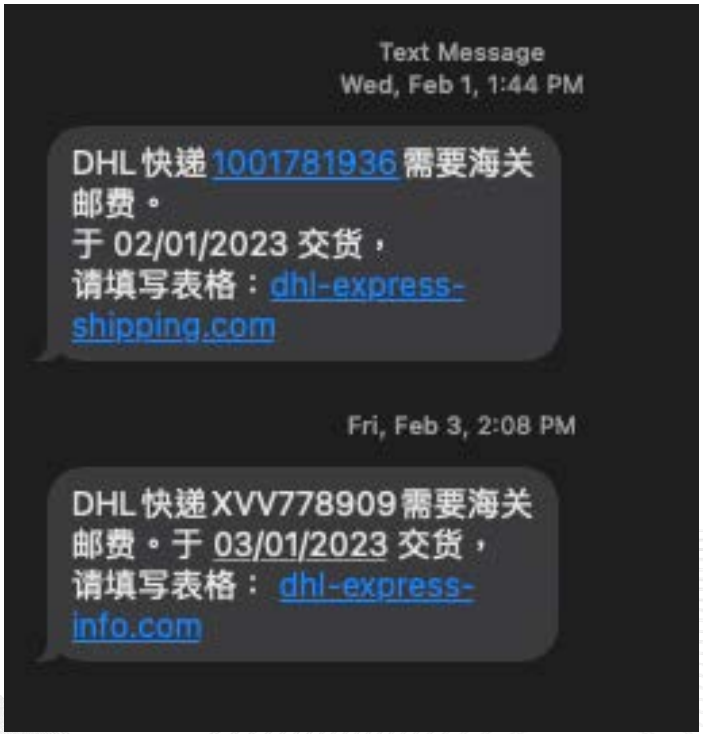
Hive

48 小時

LockBit

勒索軟體佈局- >_< !!

NAKIVO®



2023 停機問題 (研究報告)

NAKIVO

96%

企業組織至少面臨
一次停機

1 in 5

企業組織在過去3
年內發生嚴重中斷

$300,000/Hour

中型和大型企業的
停機成本

24%

由於硬體老舊而導
致長時間停機

60%

由於人為錯誤而導
致停機

Only 54%

企業組織有災難復
原計畫

以收入損失計算的停機成本

每停機一分鐘都會損失的金錢和生產力

以收入損失計算的停機成本

停機成本 = 停機分鐘數 x 每分鐘成本

確定損失的生產力

生產力成本 = 受影響的員工人數 x 小時工資

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®

透過 NAKIVO Backup & Replication

保護您的資料

虛擬化 | 實體 資料保護

無代理程式的增量虛擬機備份：

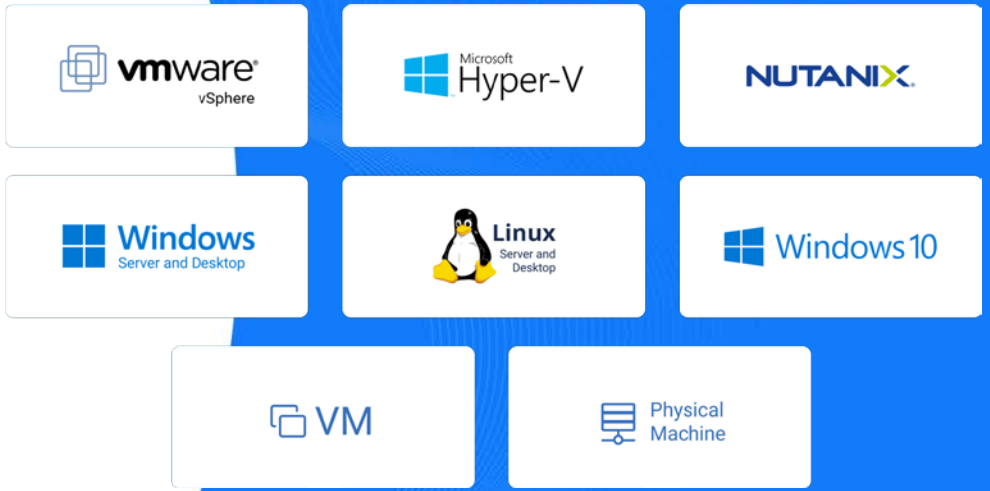
- ✓ VMware vSphere
- ✓ Microsoft Hyper-V
- ✓ Nutanix AHV

- → 多個**備份目的端**
- → 快速還原**整個虛擬機**或**物件**
- → 彈性化的**保留策略**

增量與應用程式感知的實體機備份：

- ✓ Windows 伺服器/工作站
- ✓ Linux 伺服器/工作站

- → 完整**裸機還原**
- → 快速**精細還原**
- → 快速**實體轉虛擬還原P2V**



Microsoft 365 | Oracle 資料庫 資料保護

快速、增量備份：

- ✓ Exchange Online
- ✓ OneDrive for Business
- ✓ SharePoint Online
- ✓ Teams

- ➔ 原生 Microsoft 365 變動追蹤
- ➔ 快速**精細還原**
- ➔ 進階搜尋： **合規性**與**電子證據**

Oracle 資料庫： 透過與內建Oracle RMAN備份，實現集中保護

NAS/檔案分享 資料保護

快速、增量備份的**SMB/NFS 協定分享**：
- ✓ NAS 設備
- ✓ Windows 機器
- ✓ Linux 機器

建立整個共用或**特定資料夾**的異地備份

將整個共用或單一檔案/資料夾還原到 SMB/NFS 協定分享，或透過電子郵件與瀏覽器下載

備份資料分層與相關性連結

NAKIVO

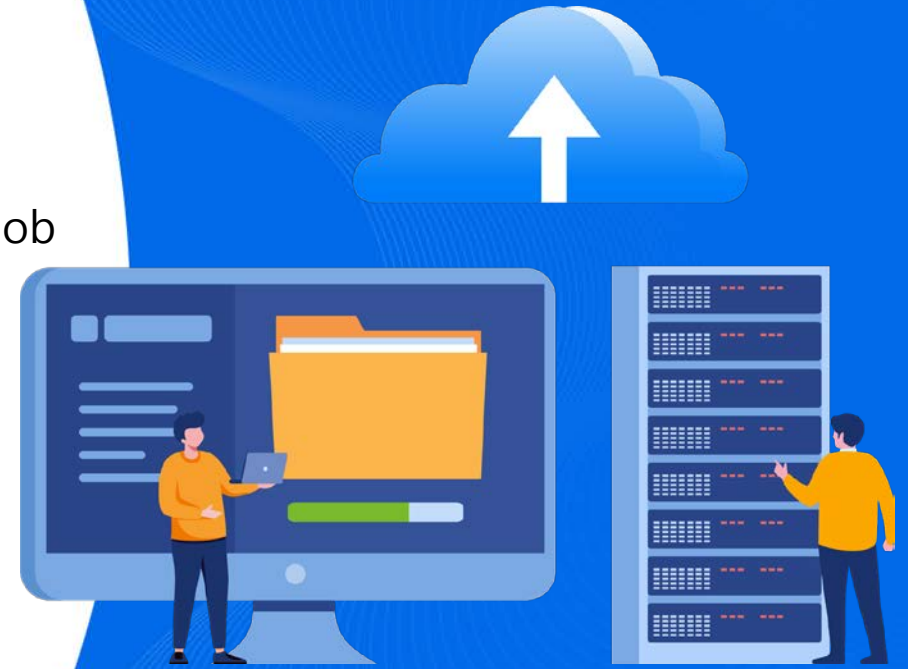
計畫： 備份資料分層

- 本地儲存：即時連線
- 雲端空間 (Amazon S3 / Wasabi/ Azure Blob / Backblaze B2): 高可靠性和可用性
- 磁帶： 封存、隔離備份
- 不可變動性儲存：勒索軟體防護

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



惡意軟體掃描

NAKIVO®

還原之前掃描備份是否有惡意軟體

- 整合性： Microsoft Windows Defender, ESET NOD32 Antivirus, Kaspersky Internet Security, Sophos Intercept X, Clam AV, and Sophos Protection.
- 將受感染的備份還原到隔離區域，以便進行分析
- 遵守嚴格的資料保護規範

NAKIVO Backup & Replication

防勒索軟體的備份

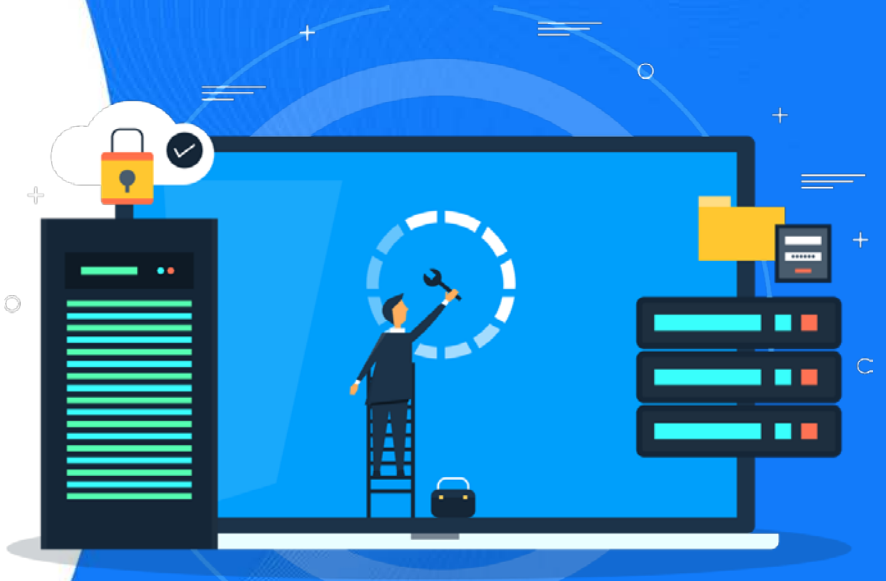
- **不可變動性備份：** Write-once-read-many (WORM)
  - 公有雲： Amazon S3, Wasabi Hot Cloud, Backblaze B2 和 Azure Blob Storage
  - S3相容性儲存設備：支援物件鎖定
  - 本地端以Linux架構的儲存區
- **強化版AMI：** 透過Amazon Machine Image內建的Linux不可變動儲存區

NAKIVO Backup & Replication

完整與精細還原

任何時刻恢復您所需的資料：

- 直接從已壓縮備份來啟動虛擬機
- 立即恢復文件、資料夾、Exchange、SQL和Active Directory 物件
- 只需點擊幾下，可透過通用性物件還原恢復您的資料
- 每個備份最多可以選擇10,000個還原點



NAKIVO Backup & Replication

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

NAKIVO Backup & Replication

備份存取控制

- **AES 256-bit 加密：**

  保護傳輸中和存放的備份

- **雙因數認證(2FA):**

  增加額外的安全，防止未經授權的存取

- **角色權限控管 (RBAC):**

  確保對資料存取與操作的權限

- **最小特權原則 (PoLP):**

  授予最低權限以提高安全性

目標：增強對勒索軟體和未經授權的防禦能力

NAKIVO Backup & Replication

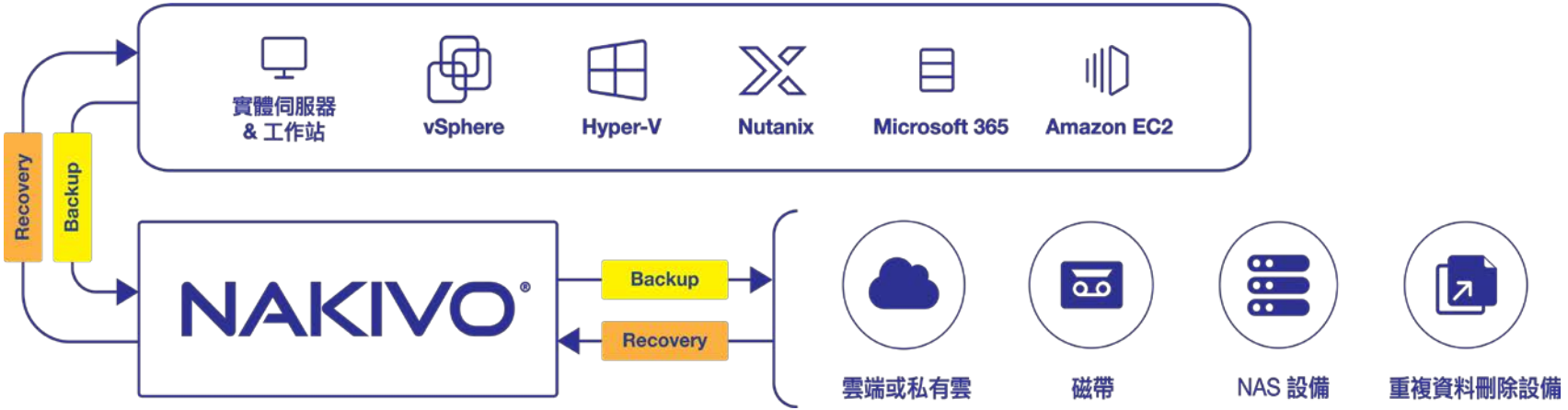
儲存空間與效能最佳化

內建最佳化工具：

- 增量備份
- 三種壓縮層級
- 資料重複刪除
- LAN-free資料傳輸
- 排除暫存資料空間
- 進階的網路頻寬控制

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, 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

NAKIVO®

Thank You!

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