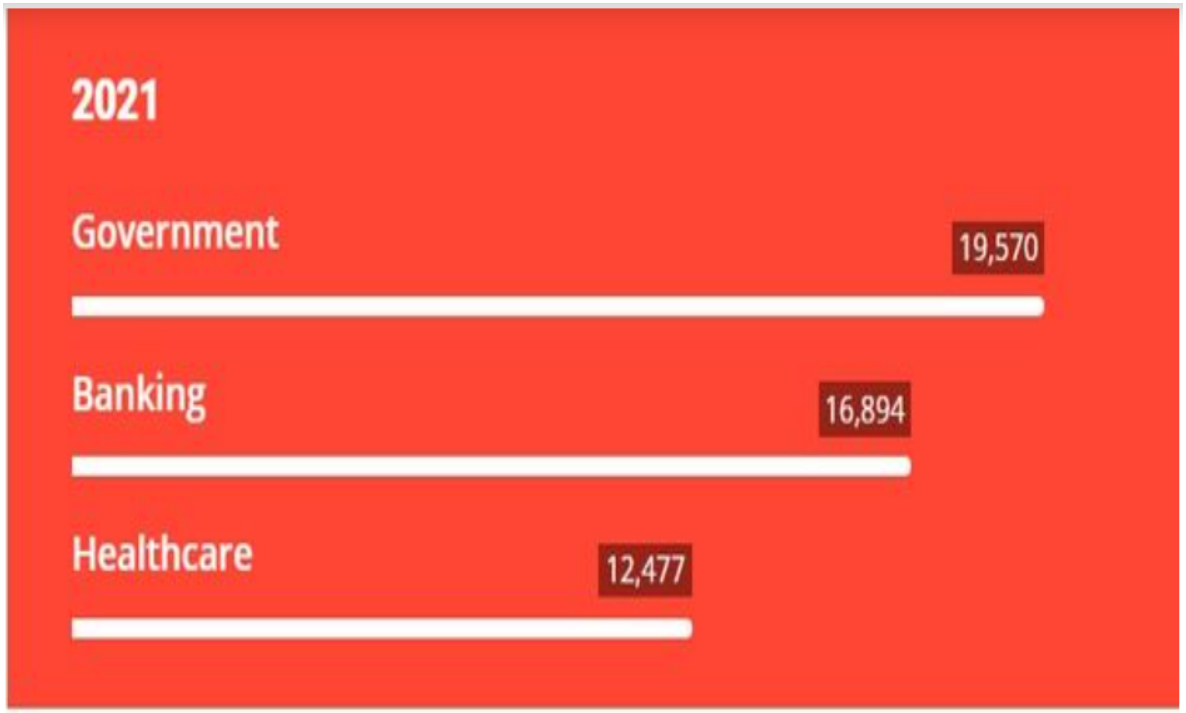
面對勒索病毒，你的備份是助力？還是所託非人？

silvershine
銀興科技股份有限公司

儲存。服務。夥伴。運行不止

2021年度資安報告



The top three industries in terms of ransomware file detections in 2021

台灣位列在全球前十名、亞洲區前五名

- 目標集中在更可能支付贖金的關鍵企業及產業
- 政府機構、銀行與醫療產業
- 勒索病毒即服務 (Ransomware-as-a-service)

台灣是家庭連網受到攻擊的前三名國家

- 利用人為錯誤來攻擊雲端基礎架構與遠端工作者
- 「WFH」成為普遍工作型態

資安威脅偵測量增長42%

- 2021威脅數量成長，來到 940 億次以上

silvershine

4大關鍵作為

使用者的教育訓練

- 分辨各種網路威脅
- 勒索病毒、網路釣魚、社交工程
- 惡意電子郵件

隨時保持軟體更新

- 裝置韌體、作業系統
- 惡意程式防護軟體

主動偵測勒索病毒

- 定期掃描，提早發現威脅
- 監測網路異常流量
- 異常檔案變動行為

完整的備份規劃

- 3-2-1 備份原則
- 異地備份、雲端備份

silvershine

面對勒索攻擊的三階段

事前預防

強化具派送功能伺服器安全
最小化開放埠的設置
網路分段區隔並監控流量
人員的最小使用權限
保持最新的備份並保持離線

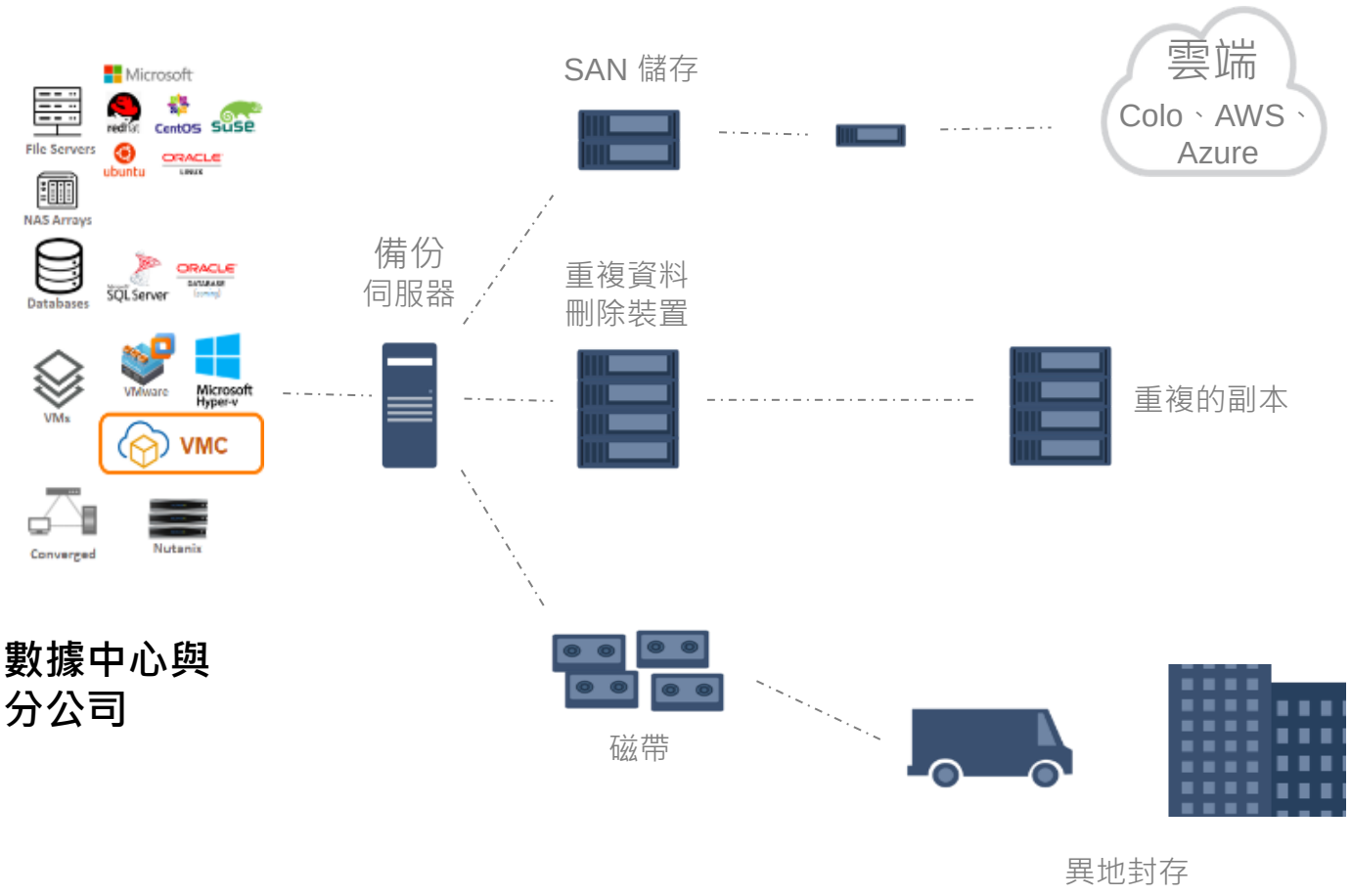
事中處理

立即斷開所有網路的連接
重置密碼及權限憑證

事後回復

確認受感染設備已完全的清除
確認備份中沒有任何惡意軟體
進行備份還原作業
安裝、更新和執行防毒軟體
監控網路流量並執行防毒掃描

3–2–1 備份原則



數據中心與分公司

至少擁有 3 份資料備份

將這些備份存放至 2 種不同的儲存媒體

至少異地儲存 1 份

silvershine

關於druva

4000+

客戶遍布全球

SaaS

aws

AWS 合作ISV夥伴
前 5 名及全球帶最多數據
到AWS平台之一

200PB+

管理200PB+資料
(重複刪除後的資料)

Marriott HOTELS · RESORTS · SUITES

SEPHORA

SIEMENS

vmware

McAfee

pwc

KPMG

DHL

微服務(無伺服器架構)

企業數據

手機設備

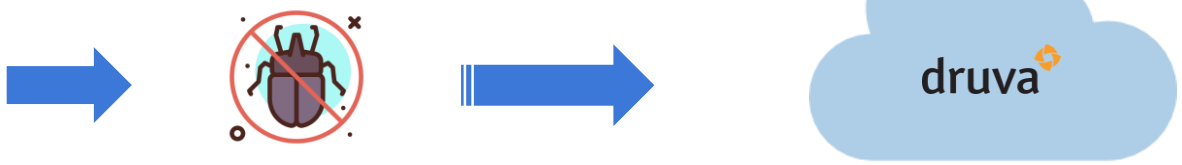
桌面電腦/ 筆電

檔案伺服器 /
NAS:網路附加儲存

虛擬機

資料庫

勒索軟件無法影響儲存在
Druva 雲中的數據



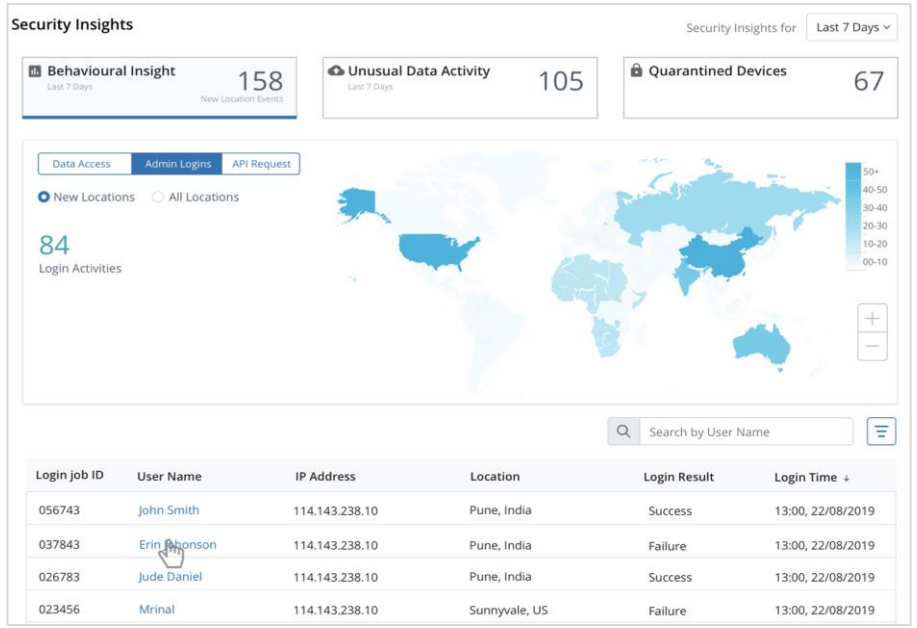
勒索軟件無法在 Druva Cloud 儲存系統中執行

- 無法使用客戶操作系統/系統憑證訪問 Druva 備份
- 沒有SSH、網絡、NTFS 或 RDP 對 Druva 雲的訪問
- 資料儲存在 Object Storage 上，**不可以被修改**
- 資料被分解並儲存為更小的區塊
- 勒索軟體無法Phone Home 與其命令和控制中心建立任何通信**觸發攻擊**

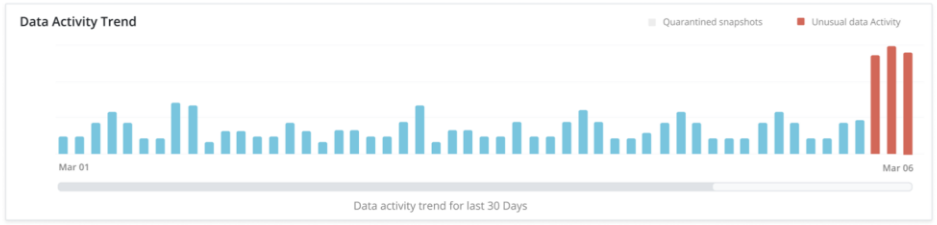
silvershine

異常行為監控及回應

1. 存取訪問洞察力



2. 異常檢測**:** 資料異常變動的洞察



3. 隔離**:** 隔離快照以防止污染風險

使用 UDA 識別最後一個已知的良好快照

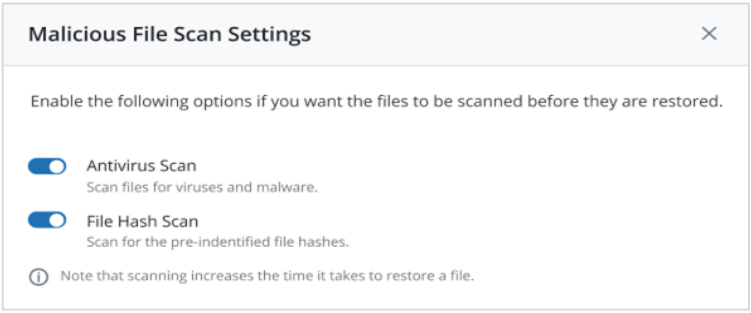
隔離受感染的快照

更換主機 + 安裝 Druva

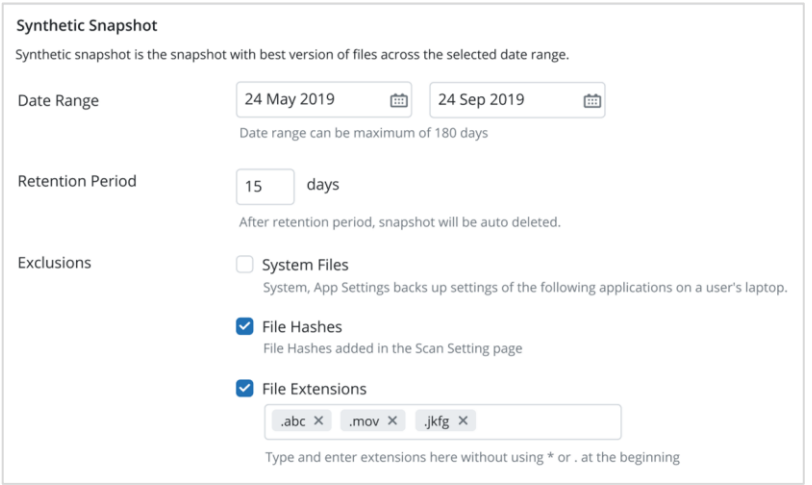
自動從最後一個已知的好的副本中恢復數據

刪除受感染的快照

4. 恢復掃描**:** 恢復前對快照進行掃描

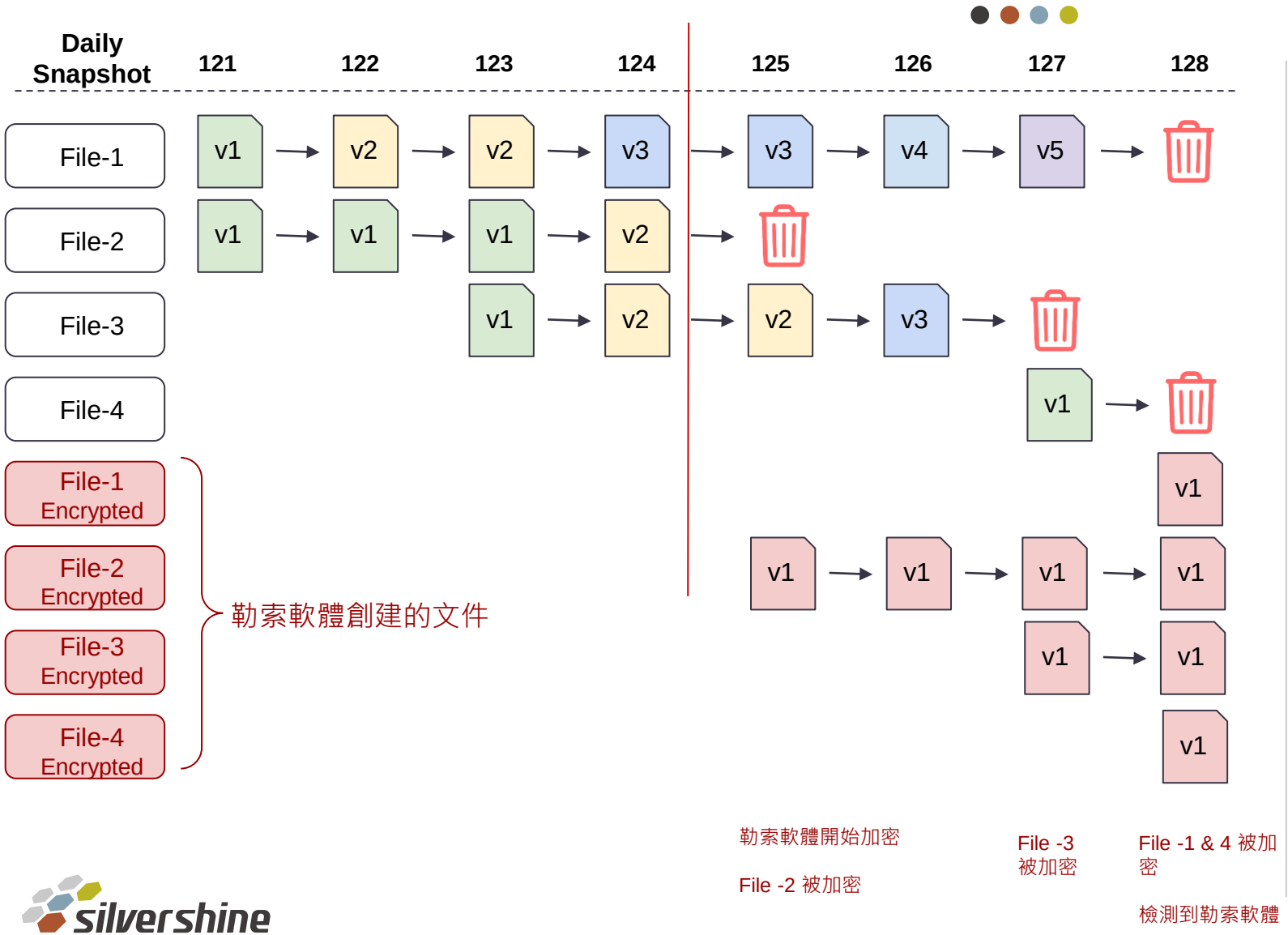


5. 黃金快照**:** 自動恢復每個文件的最新乾淨版本



silvershine

傳統備份可能遺失90天數據！



勒索軟體在開始加密文件前，幾天前就進入系統? (估計在檢測前 **~90 天**)

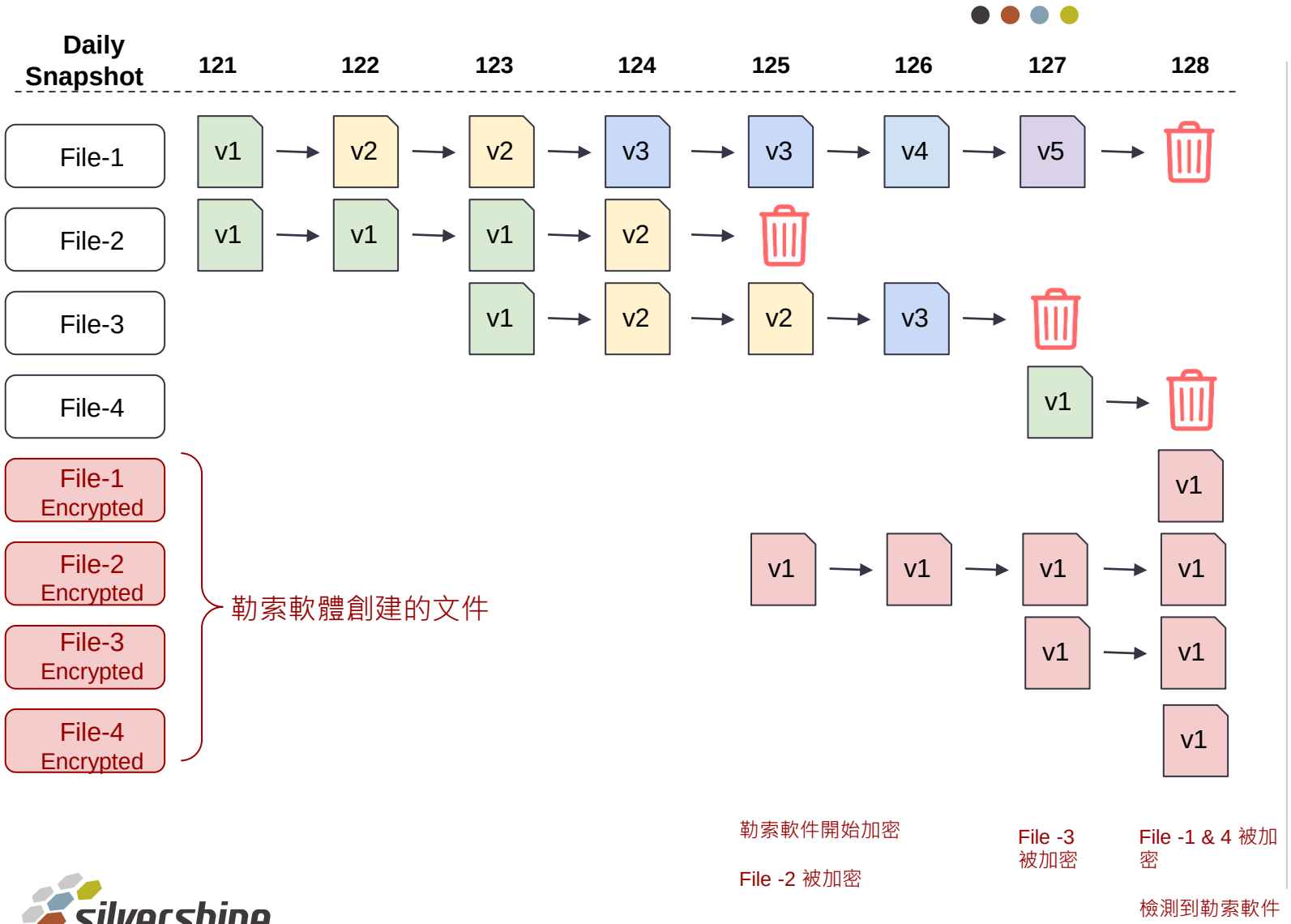
如果我們從檢測到勒索軟體的時間點恢復快照，**資料就會損失**

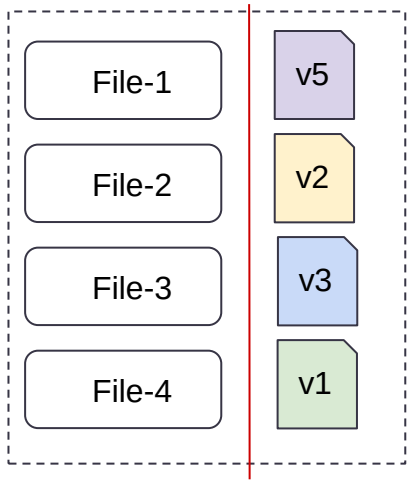
- 快照 124 是沒有被加密文件
- File- 1,3,4 中的數據丟失

我們可以跨快照選擇文件版本嗎？

silvershine

Auto Select Technology™





自動選擇不同快照的最佳文件版本：

- 減少勒索軟體事件造成的數據遺失
- 加快恢復時間

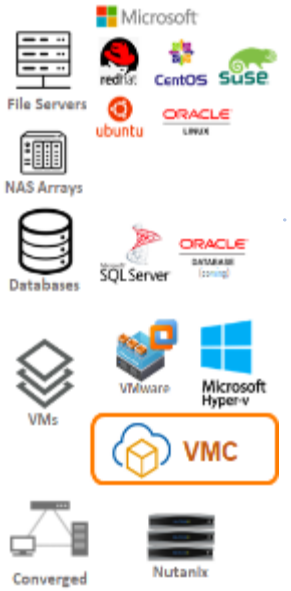
silvershine

Druva不是一個簡單備份方案，而是一個數據防護平台

exterro okta paloalto NETWORKS splunk>

原生雲 **Cloud Native SaaS** 架構

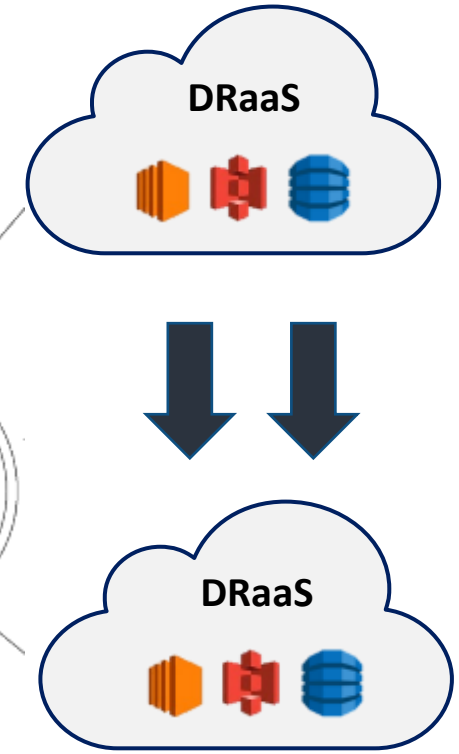
內部數據中心與工作負載

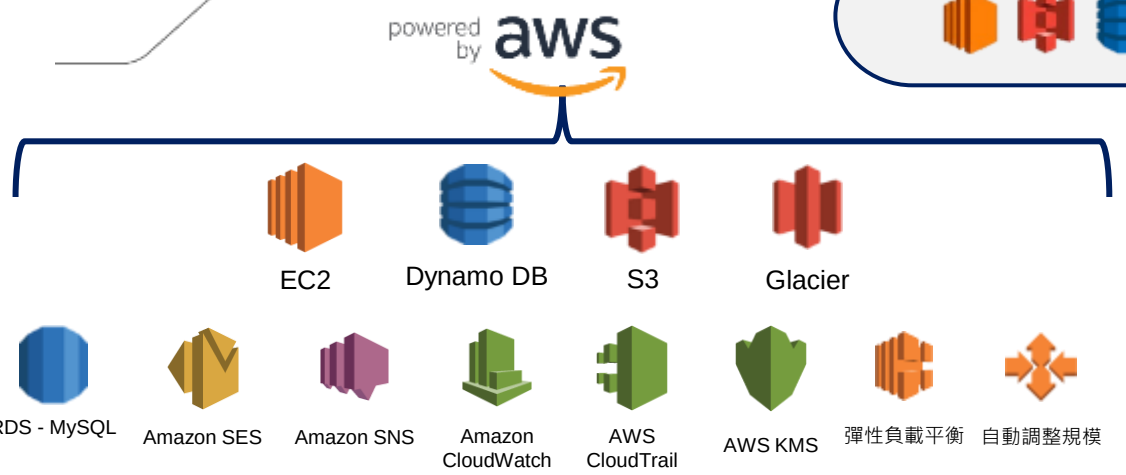


直接操作雲端

零硬體

LAN 速度 RTO/RPO (雲端快取)





silvershine

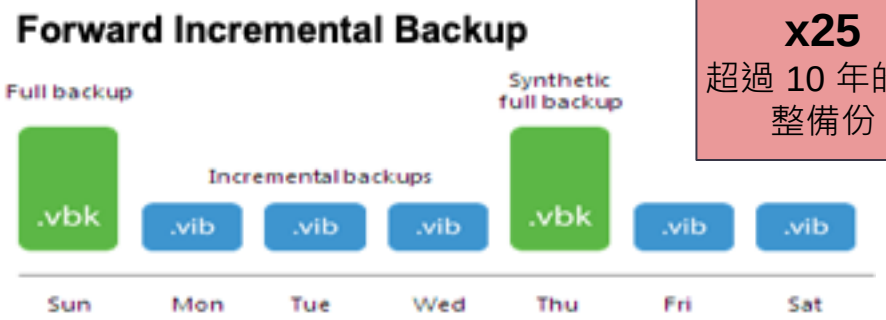
最小化備份空間

混合式雲端方式 (傳統)

內部部署

用於 14 天資料時，儲存空間至少要符合下列工作需求：

- 2 次完整備份 (目前的備份，加上即將建立的最新完整備份)
- 14 天的增量備份

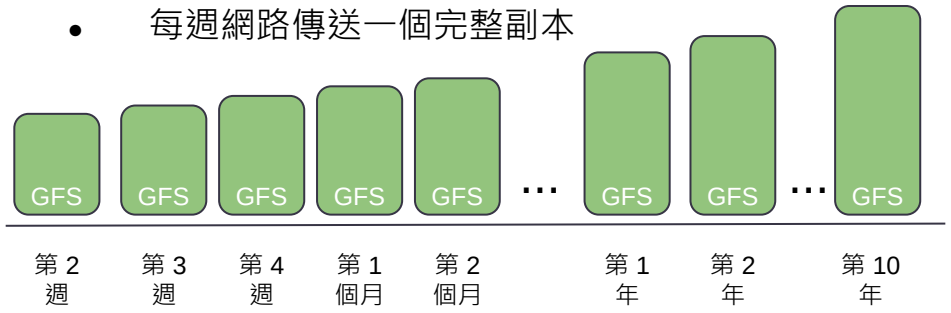


最多
x25
超過 10 年的完整備份

雲端

用於 4-d、12-w、10-y 原則時，必須使用雲端儲存進行：

- ~23 份雲端完整備份。
- 每週網路傳送一個完整副本

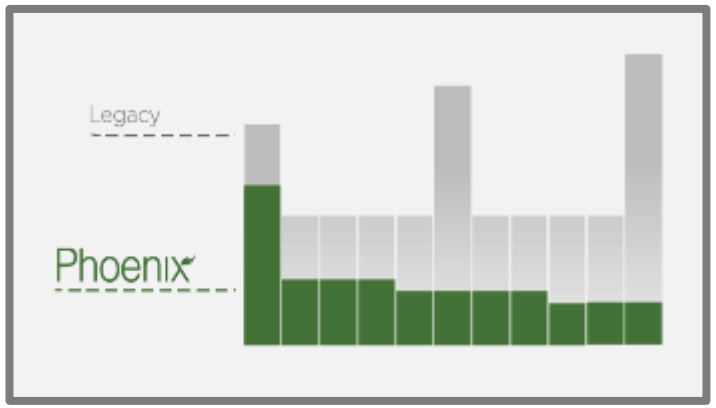


Druva 雲端

一次完整備份，後續全部增量備份

+ 全域重複資料刪除 + 自動分層

1 個副本 + 增量型 (已刪除重複資料)



Druva Phoenix 能使儲存裝置效能達到最佳化

- 僅在第一次使用完整備份
- 即使在第一次備份時也會先實施全域重複資料刪除，再送入雲端
- 在該次備份之後，永遠實施增量型備份 (沒有限制)
- Druva 會自動為 AWS 中的儲存進行分層

大幅減少備份管理員的工作

- 一般日常例行活動
  - RPO/RTO 報告
  - 更多成功/更少失敗
  - ~~儲存/容量管理~~
  - 回應：更快回應新要求
  - 更少疑難排解
- 每週一次
  - ~~安全性修補~~
  - ~~儲存容量規劃~~
  - 更多復原測試
- 每季一次
  - ~~軟體/硬體修補~~
  - ~~軟體/硬體重新整理週期~~
  - 更簡單的風險/合規性報告
  - ~~遠端辦公室、取得、新硬體~~
  - ~~過度規劃的容量與高成本~~

您的時間很寶貴

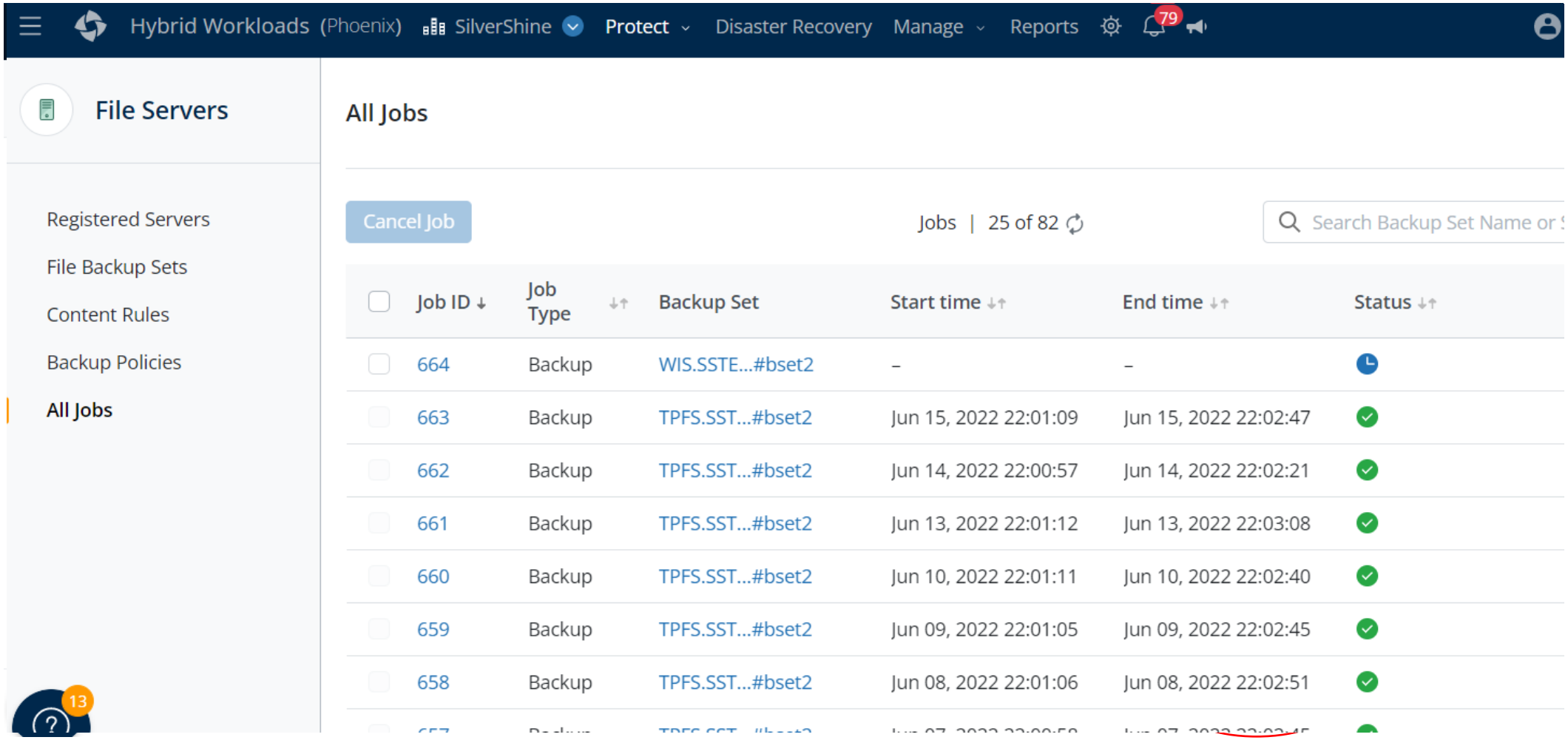
RelyOn Nutec
360° Safety

「這讓我們在每月備份工作上節省了超過 30 個小時的工作時數，相較於過去我們總覺得十分麻煩的系統，像是 NetBackup，這個差別真的非常大。」

— Gavin Bell，全球 IT 專案經理

silvershine

Druva 設定範例


Hybrid Workloads (Phoenix)
SilverShine
Protect
Disaster Recovery
Manage
Reports
79
File Servers
Registered Servers
File Backup Sets
Content Rules
Backup Policies
All Jobs
All Jobs
Cancel Job
Jobs | 25 of 82
Search Backup Set Name or
Job ID
Job Type
Backup Set
Start time
End time
Status
664 Backup WIS.SSTE...#bset2 – –
663 Backup TPFS.SST...#bset2 Jun 15, 2022 22:01:09 Jun 15, 2022 22:02:47
662 Backup TPFS.SST...#bset2 Jun 14, 2022 22:00:57 Jun 14, 2022 22:02:21
661 Backup TPFS.SST...#bset2 Jun 13, 2022 22:01:12 Jun 13, 2022 22:03:08
660 Backup TPFS.SST...#bset2 Jun 10, 2022 22:01:11 Jun 10, 2022 22:02:40
659 Backup TPFS.SST...#bset2 Jun 09, 2022 22:01:05 Jun 09, 2022 22:02:45
658 Backup TPFS.SST...#bset2 Jun 08, 2022 22:01:06 Jun 08, 2022 22:02:51
13

TCO view : SaaS模式備份 VS 傳統備份

不僅看花了多少錢？看整體擁有成本

希望備份

To increase BCM confident

To reduce TCO

To reduce Capex & Complexity

1

硬體成本 – 備份伺服器，儲存設備，網路，Dedupe appliance，。。

2

軟體成本 – 備份主軟體，各種模組軟體附加。。

3

硬體維護成本 – 硬體維修，保固延申委外人力，硬體淘汰更換。。

4

軟體維護成本 – 軟體升級，延申保固。。

5

空間費用 – 擺放硬體空間的租金，電力消耗費用。。（要求淨零碳排的趨勢）

6

雲端費用 – 是否另外需付雲端容量的費用?是否需額外端頻寬費用？

7

人力成本 – 維護備份軟硬體人員的支出。是否有差異？

8

時間成本 – 要花多少時間在處理備份這個工作？Restore要花多少時間完成？。。

9

附加的功能 – 未來不需額外付費。。

10

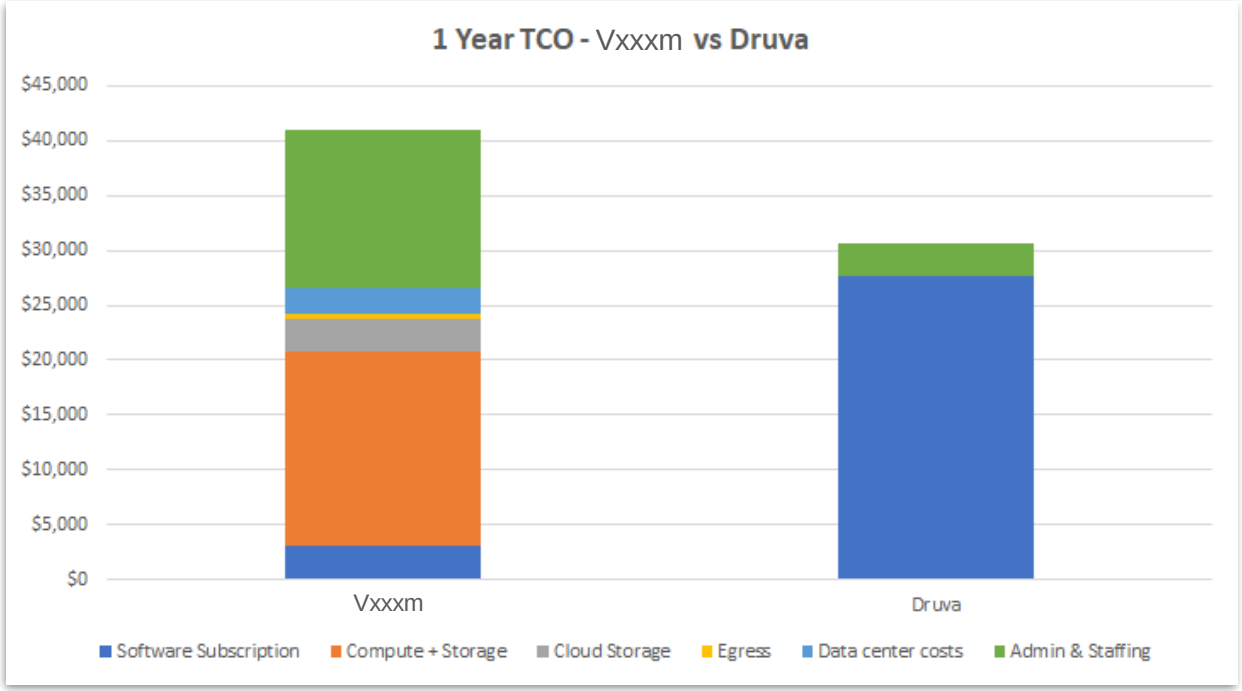
節省的儲存空間費用 – 要幾倍的容量做備份？Dedupe重刪的效果？

11

勒索病毒 – 選擇的備份方案，被勒索病毒攻擊的機率，高 or 低，有否因應方案？

TCO view : SaaS模式備份 VS 傳統備份

- **應用範例**:
  - 10 TB source data - VMware (20 VMs)
  - Cloud tiering (every 7 days)
- **成本計算:**
  - 備份軟體及授權
  - 伺服器及儲存設備(DAS)
  - 租用雲端空間
  - 機房維護
  - 管理人力及時間



Druva 是北斗星的意思 – 數據保護的北斗星

根據最後一次投資，市場估值在 2 Billion美元

領先業界的SaaS雲端數據保護解決方案

2.5B+
備份 / 年

50%
YoY 同比增長

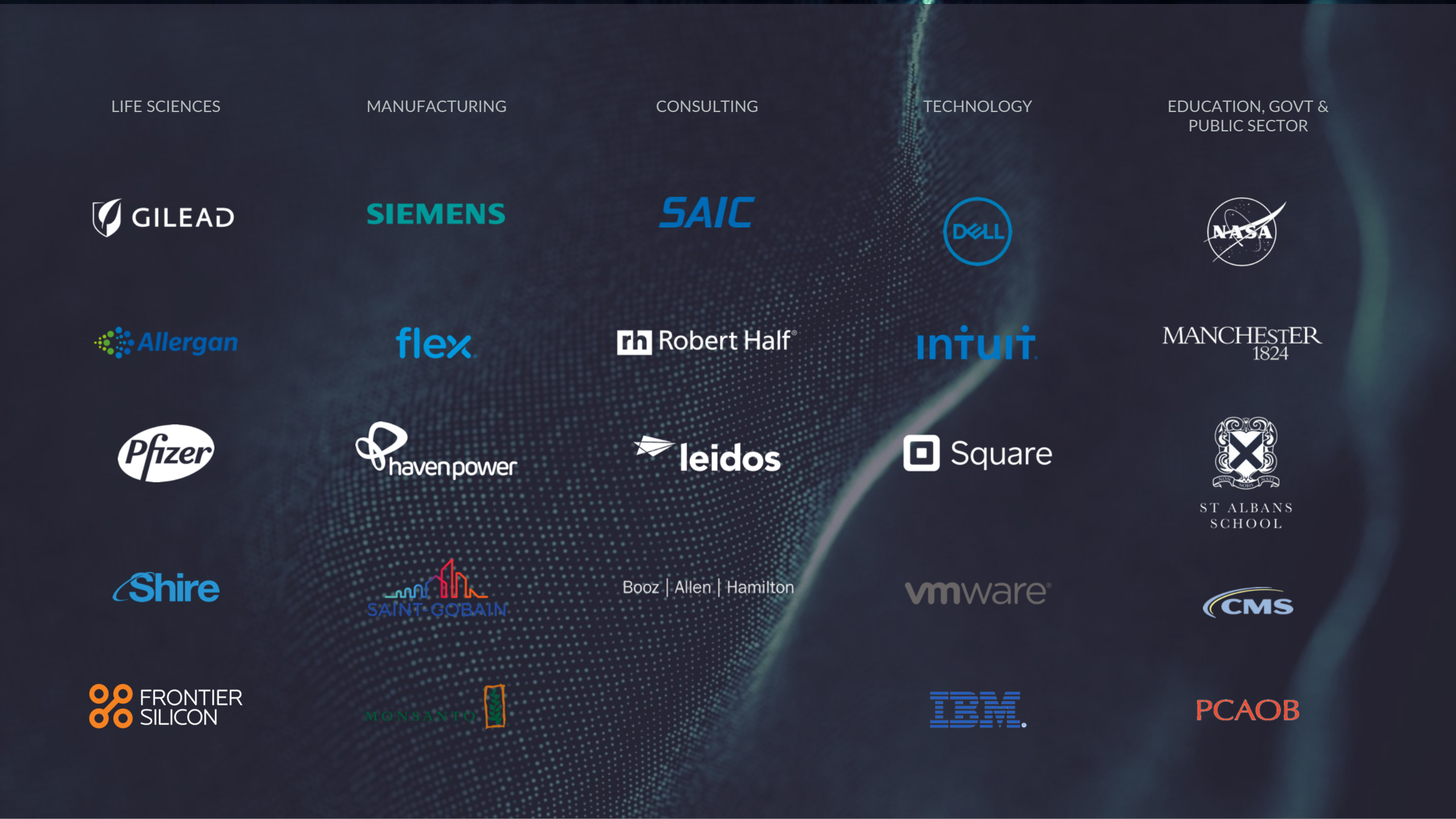
89
NPS 用戶評比

60+ Fortune 500

16
區域

200 PB+
管理數據

A.C.MOORE ARTS & CRAFTS
AMOREPACIFIC
ANDRITZ
ANGLO-EASTERN
APPTUS
BECKMAN COULTER
BROWN-FORMAN
CLEVELAND BROWNS
DHL
DHS HUMAN SERVICES
EGAN
FOREVER 21
Gap International Partners In Exceptional Growth
HITACHI Inspire the Next
IMMEDIATE MEDIA Co
jamf
NASA
OHEL
REGENERON
SAMSUNG SEMICONDUCTORS
Spirent
STARZ
The Pokémon Company INTERNATIONAL
UMBRAGROUP


LIFE SCIENCES
MANUFACTURING
CONSULTING
TECHNOLOGY
EDUCATION, GOVT & PUBLIC SECTOR
GILEAD
SIEMENS
SAIC
DELL
NASA
Allergan
flex
Robert Half
intuit
MANCHESTER 1824
Pfizer
haven power
leidos
Square
ST ALBANS SCHOOL
Shire
SAINT-GOBAIN
Booz | Allen | Hamilton
vmware
CMS
FRONTIER SILICON
MONSANTO
IBM
PCAOB

客戸認可

Gartner peerinsights™

Druva **4.7**/5

Top 50 IT Management Products BEST SOFTWARE AWARDS 2020

Top 50 Mid-Market Products BEST SOFTWARE AWARDS 2020

Top 50 Highest Satisfaction Products BEST SOFTWARE AWARDS 2020

Druva **4.5**/5

Top Rated 2020

TRUE 2020

Druva **8.7**/10

業界認可

FORRESTER®

Strong Performer for Data Resiliency Solutions

Cyber Catalyst by Marsh

Cyber Catalyst Solution 2020

THE STEVIES

THE CHANNEL CO. CRN STORAGE 100 2020

CYBERSECURITY BREAKTHROUGH AWARD 2020

Data Management Company of the Year

GIGAOM

Leader in GigaOm Unstructured Data Management Radar 2020

NorthFace ScoreBoard Award

Best-in-class certified NPS score of 88

獲得Gartner肯定

2021 Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Gartner®

Druva is the ONLY at-scale SaaS vendor in the report

silvershine

面對勒索病毒，你的備份是助力?還是所託非人?

【8/31 線上Webinar 直播 Q&A 回顧 】

Q&A	直播提問	Silvershine 回答
1	請問規劃異地備份是否可以防止勒索病毒呢?	是有機會防止的，但要看您備份的時間點是否已受到感染？ 只能回復至感染時間點之前的檔案，RPO及RTO之問題。
2	請教貴司系統能否提供遠端連線應用?	可以向銀興申請POC測試，對於您所需要了解的功能會更詳細； Druva操作介面是透過瀏覽器加密連線，有網路的地方皆可連線使用。
3	若使用者缺乏教育訓練(如技術人員)， 此時是否不適合應用貴司系統	Druva GUI 操作介面非常友善簡單操作，銀興可以協助設定及教學， 完成貴司備份方案。
4	請問貴司備份模式是否可以用代理方式集中管理備份?	Druva無須專用的硬體設備，需備份之設備首先要安裝Druva代理程式， 即可套用規則來執行集中管理備份行為。
5	支援離線備份嗎?	因是備份至Druva雲端空間，故需連線才可備份。
6	所以網路中斷就不能備份了嗎?	是的，連上線後會自動接續備份。
7	有斷線異地備份功能或機制嗎?	因是備份至Druva雲端空間，斷線基本上是無法提供備份。

面對勒索病毒，你的備份是助力?還是所託非人?

【8/31 線上Webinar 直播 Q&A 回顧 】

8	備份硬體容量也是隨時可更動訂閱的嗎?	備份容量可隨需求來訂閱增加。
9	請問備份的每個功能都能自行選擇訂閱嗎?	Druva提供套裝套件，可依您需要的備份需求來選擇備份方案， 提供資料中心、SaaS應用程式、終端設備，可供選擇。
10	請問防火牆前後都可以備份嗎?	可以，防火牆內需要建立通過規則即可； 防火牆外可以連上網際網路直接可以備份。
11	請問資料需要回存，速度如何? 有較佳方案嗎?	依貴司的網速而定，此外Druva提供地端cloud cache的服務， 可以快速回復30天內的資料。
12	請問主要是針對機房、本地機嗎? 是否也可備份aws、azure上的資料?	訂閱資料中心套件來備份本地及雲端上主機內的服務及資料。
13	請問，連網頻寬需求如何評估?	備份上傳至Druva的頻寬是可以設定限制傳輸速度，如需要瞭解使用效能， 可以申請POC於您的環境實際測試。
14	請問這個介面可以中文化嗎?	目前只支援英文語系，無中文介面。

Thank You

運行不止

歡迎填問卷
與我們聯繫!

影片連結

silvershine