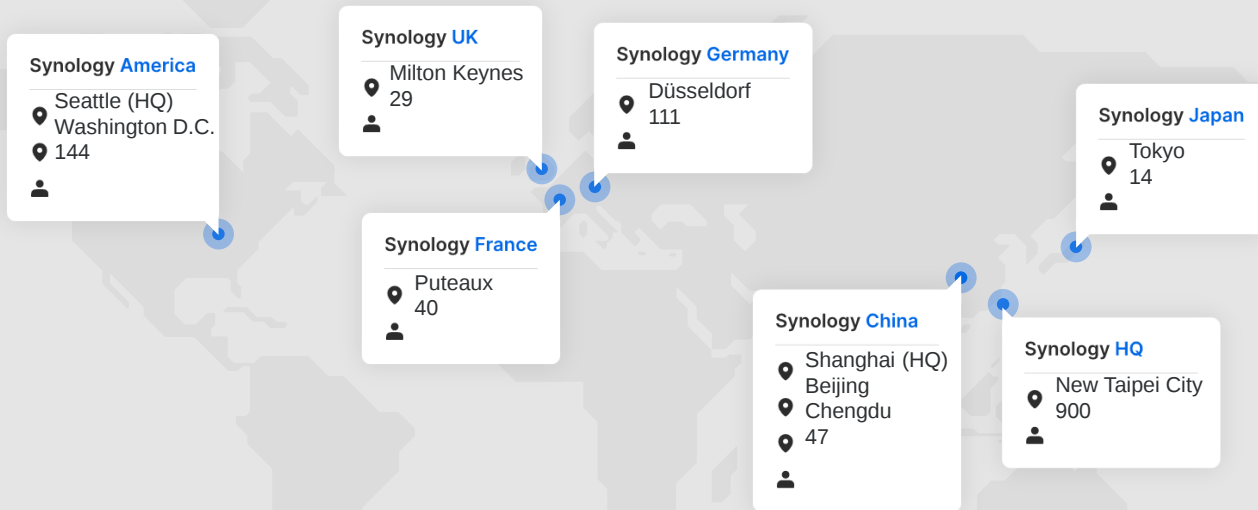


從上市櫃公司到各產業組織， 加速達成 ISO27001 資料安全合規性 之策略解析

Synology 技術客戶經理
Johnny Tung

研發於台灣，銷售至全球 120 個市場

Build a Better World with Data



1300+

全球員工數

10M+

伺服器累積銷售

88EB+

儲存資料量

1M+

生產力工具活躍用戶

30M

保護端點裝置與雲端帳號

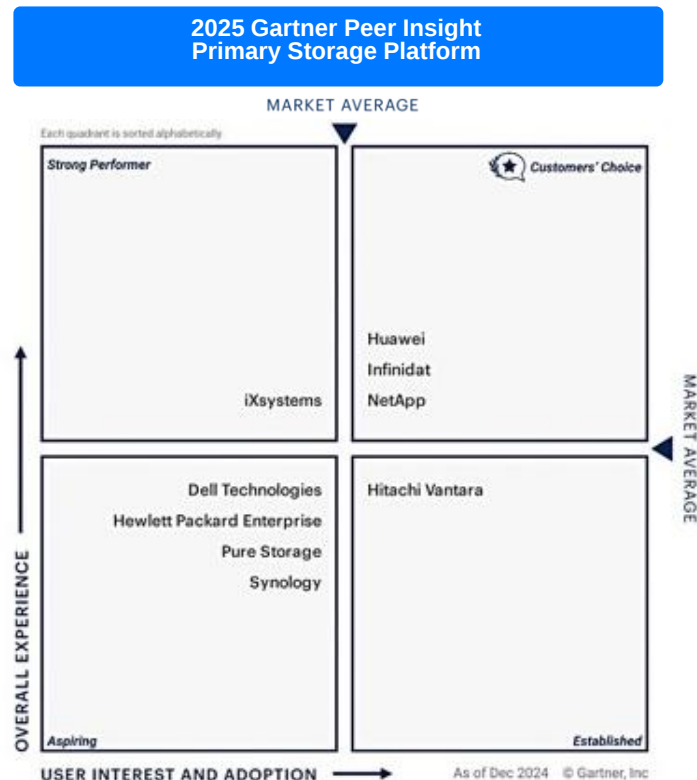
榮獲 Gartner Peer Insights 肯定

99% 客戶推薦

最佳企業級備份與復原解決方案 (Gartner Peer Insights, 2024)

4.7/5 客戶評分

最佳主要儲存平台 (Gartner Peer Insights, 2024)





全方位企業資料管理解決方案

A photograph of a server room with rows of black server racks. The racks are filled with various electronic components, and the perspective is looking down a long aisle.

資料儲存管理

A photograph of a server room, similar to the one on the left, showing rows of server racks from a slightly different angle.

資料備份與
災難復原

A photograph of a modern city skyline at night, featuring several tall skyscrapers with illuminated windows.

企業生產力

A photograph of a person wearing glasses, seen from the side, looking at multiple computer monitors. The screens display various data, including maps and charts. The person is holding a pen near their chin.

智慧影像監控



全方位企業資料管理解決方案

The background for the first section is a dark, close-up photograph of server racks, showing the vertical structure and some internal components.

資料儲存管理

The background for the second section is a dark, high-angle photograph of a city at night, with many lights from buildings and streets visible.

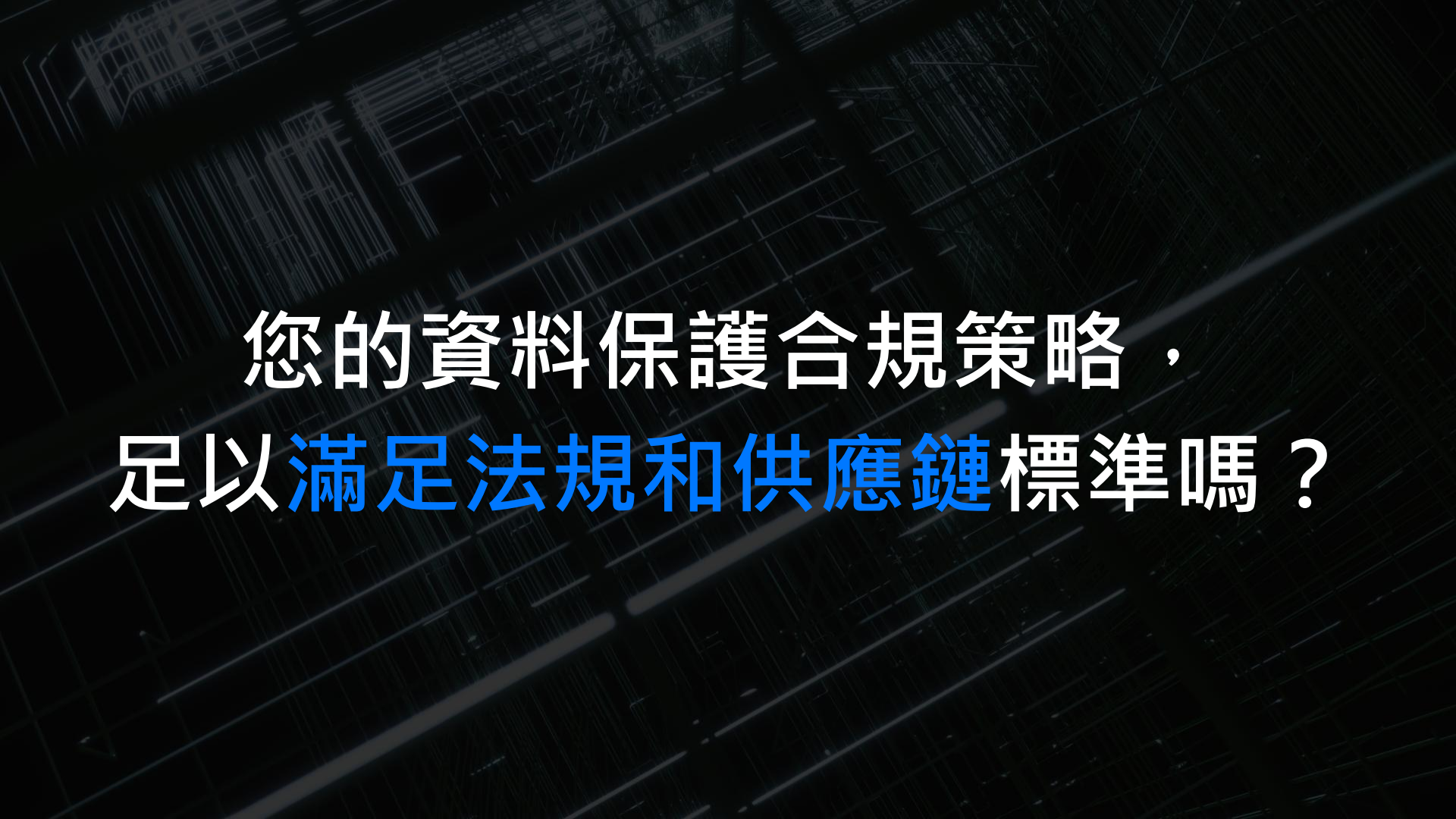
資料備份與
災難復原

The background for the third section is a dark, abstract image featuring a grid pattern, possibly representing data or a network.

企業生產力

The background for the fourth section is a dark, low-key photograph of a person in a dark environment, possibly a security guard or investigator, looking at a screen.

智慧影像監控



您的資料保護合規策略，
足以滿足法規和供應鏈標準嗎？

近年與資通安全相關規範：以上市櫃公司為例

金管會內部控制及
稽核制度實施辦法

110 年 9 月

證券交易所上市上櫃公司
資通安全管控指引

110 年 12 月 27 日

110 年 11 月 20 日

金管會公開發行公司年報應行
記載事項準則部分條文修正

110 年 12 月 28 日

金管會公開發行公司建立
內部控制制度處理準則第 9 條之 1

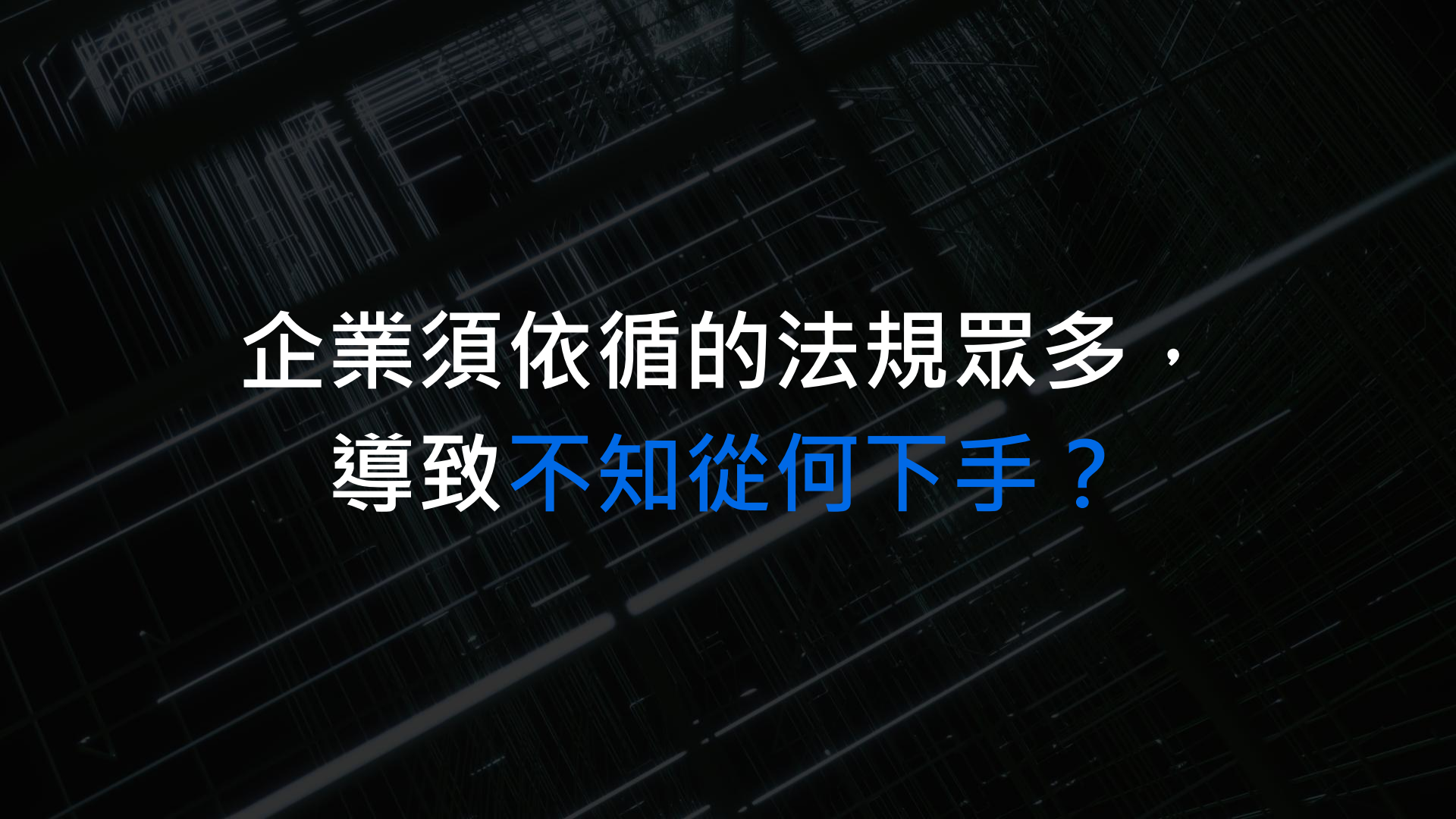
合規性已成營運關鍵

Top 5

2025 年企業 IT 認定主要任務

80%

企業受到法令或產業供應鏈要求



企業須依循的法規眾多，
導致不知從何下手？

產業與領域須符合規範：以上市櫃公司為例

上市上櫃公司資通安全管控指引

- 第七條、鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
- 第八條、鑑別應遵守之法令及契約要求。
- 第九條、鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標（RTO）及資料復原時間點目標（RPO），設置適當之備份機制及備援計畫。
- 第十條、制定核心業務持續運作計畫，定期辦理核心業務持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善

證券暨期貨市場各服務事業資訊作業韌性參考指引

- 第 7 條（營運衝擊分析）
組織應每年定期執行營運衝擊分析，評估核心業務中斷所造成之衝擊程度，並產出下列分析結果，以利評估核心系統復原策略：二、組織應訂定核心系統之復原時間目標（RTO）、資料復原點目標（RPO），以作為備份備援規劃及執行復原作業之依據。
- 第 8 條（備份備援機制）
二、組織於制定資料備份機制時，宜考量「3-2-1 備份原則」
- 第 12 條（營運持續計畫演練）
一、組織應針對已辨識可能造成核心業務中斷之風險情境（包含天然災害、人為災害與資通訊安全事件）設計演練情境

合規法條之間存有不少共通點

上市上櫃公司資通安全管控指引

- 第七條、鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
- 第八條、鑑別應遵守之法令及契約要求。
- 第九條、鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標（RTO）及資料復原時間點目標（RPO），設置適當之備份機制及備援計畫。
- 第十條、制定核心業務持續運作計畫，定期辦理核心業務

持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討

證券暨期貨市場各服務事業資訊作業韌性參考指引

- 第 7 條（營運衝擊分析）
組織應每年定期執行營運衝擊分析，評估核心業務中斷所造成之衝擊程度，並產出下列分析結果，以利評估核心系統復原策略：一、組織應訂定核心系統之復原時間目標（RTO）、資料復原點目標（RPO），以作為備份備援規劃及執行復原作業之依據。
- 第 8 條（備份備援機制）
二、組織於制定資料備份機制時，宜考量「3-2-1 備份

原則」，並應定期執行資料備份與恢復測試（營運持續計畫演練）。組織應針對已辨識可能造成核心業務中斷之風險情境（包含天然災害、人為災害與資通訊安全事件）設計演練情境。

明訂 RTO 與 RPO

合規法條之間存有不少共通點

上市上櫃公司資通安全管控指引

- 第七條、鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
- 第八條、鑑別應遵守之法令及契約要求。
- 第九條、鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標（RTO）及資料復原時間點目標（RPO），設置適當之備份機制。
- 第十條、制定核心業務持續運作計畫，定期辦理核心業務

持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善

證券暨期貨市場各服務事業資訊作業韌性參考指引

- 第 7 條（營運衝擊分析）
組織應每年定期執行營運衝擊分析，評估核心業務中斷所造成之衝擊程度，並產出下列分析結果，以利評估核心系統復原策略：二、組織應訂定核心系統之復原時間目標（RTO）、資料復原點目標（RPO），以作為備份備援規復原作業之依據。
（備份備援機制）
- 二、組織於制定資料備份機制時，宜考量「3-2-1 備份

原則」

- 第 12 條（營運持續計畫演練）
一、組織應針對已辨識可能造成核心業務中斷之風險情境（包含天然災害、人為災害與資通訊安全事件）設計演練情境

制定還原演練計畫

...卻也有各自不同的規範

上市上櫃公司資通安全管控指引

- 第七條、鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
- 第八條、鑑別應遵守之法令及契約要求。
- 第九條、鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標（RTO）及資料復原時間點目標（RPO），設置適當之備份機制及備援計畫。
- 第十條、制定核心業務持續運作計畫，定期辦理核心業務持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善

證券暨期貨市場各服務事業資訊作業韌性參考指引

- 第 7 條（營運衝擊分析）
組織應每年定期執行營運衝擊分析，評估核心業務中斷所造成之衝擊程度，並產出下列分析結果，以利評估核心系統復原策略：二、組織應訂定核心系統之復原時間目標（RTO）、資料復原點目標（RPO），以作為備份備援規劃及執行
- 第 8 條
二、組織於制定資料備份機制時，宜考量「3-2-1 備份原則」
- 第 12 條（營運持續計畫演練）
一、組織應針對已辨識可能造成核心業務中斷之風險情境（包含天然災害、人為災害與資通訊安全事件）設計演練情境

僅其一指引提及

有沒有更加便利、
一體適用的合規策略？

ISO27001 是最佳解法



機密性

完整性

可用性

從 ISO27001 著手，同步滿足其餘安全規範

ISO 27001:2022, Control 8.13

1. 概述清楚且具體的還原程序，還原範圍涵蓋所有相關關鍵系統和服務。
2. 產出任何系統、資料或應用程式的可用副本，這些項目涵蓋在備份作業中。
3. 符合組織獨特的商業和營運要求（例如復原時間目標、備份類型、備份頻率）（請參閱 Control 5.30）。
4. 將備份儲存在適當的位置，此位置的環境應予以妥善保護，且為不同於來源資料的實體位置，以防止資料盡失，並確保可安全存取以進行維護（請參閱 Control 8.1）。
5. 強制定期測試備份與還原，保證資料可用性以便在需要時，能立即還原檔案、系統或應用程式。
6. 備份測試應根據組織需要的復原時間進行衡量.....
7. 根據風險等級，對已備份的資料進行加密。
8. 先檢查是否有資料遺失，再執行所有備份作業。
9. 確保通知維護人員備份作業的狀態，以便在完全或部分失敗時採取補救措施。
10. 應包括未直接由組織管理的基於雲端平台的數據。

備份 3-2-1

制定還原演練計畫

明訂 RTO 與 RPO



Synology 資料保護解決方案 協助企業達成 ISO27001

達成 ISO27001 的四大要素



保護來源
資料

確保備份
可用性

建構備份
可還原性

多元還原
隨需取回

Synology ActiveProtect 備份專用一體機

一站式軟硬整合，企業級資料安全一次到位



如何達成 ISO27001 ？

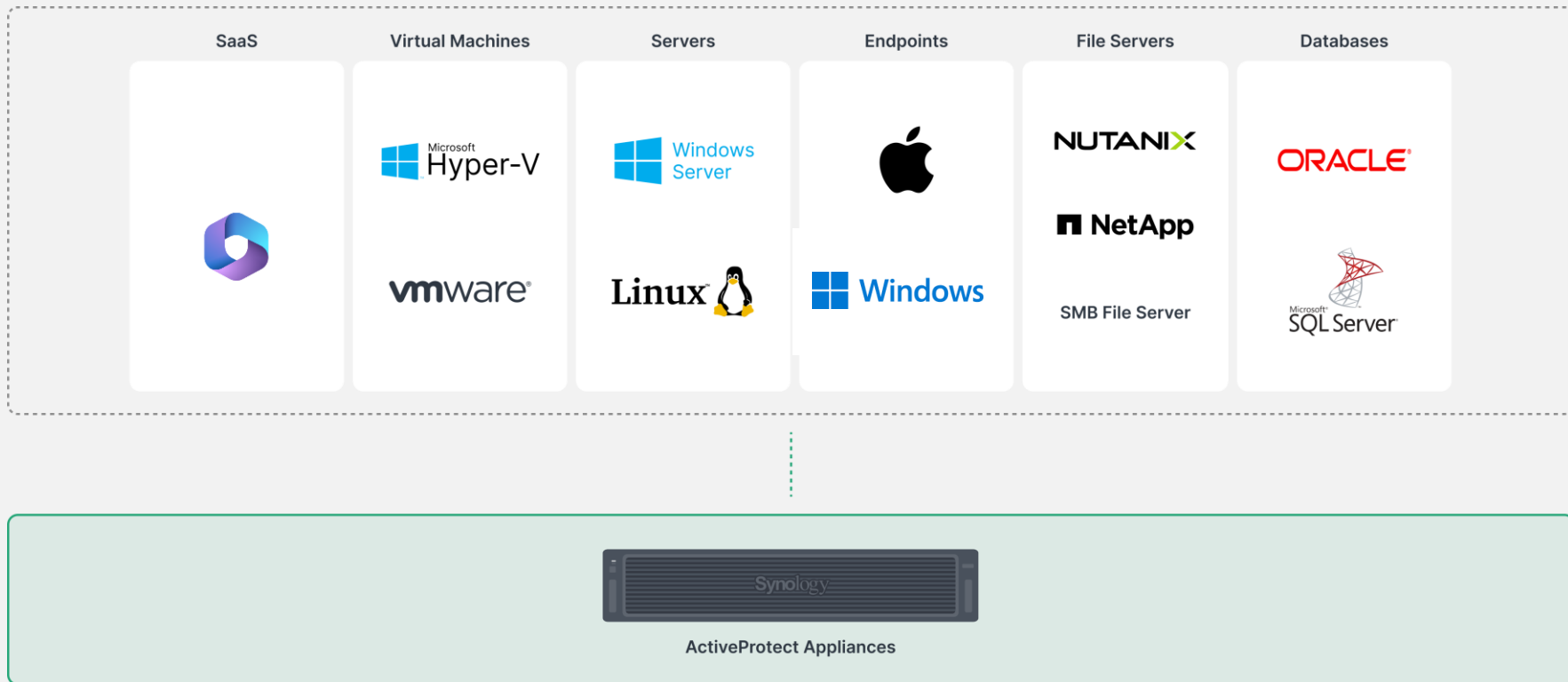


保護來源
資料

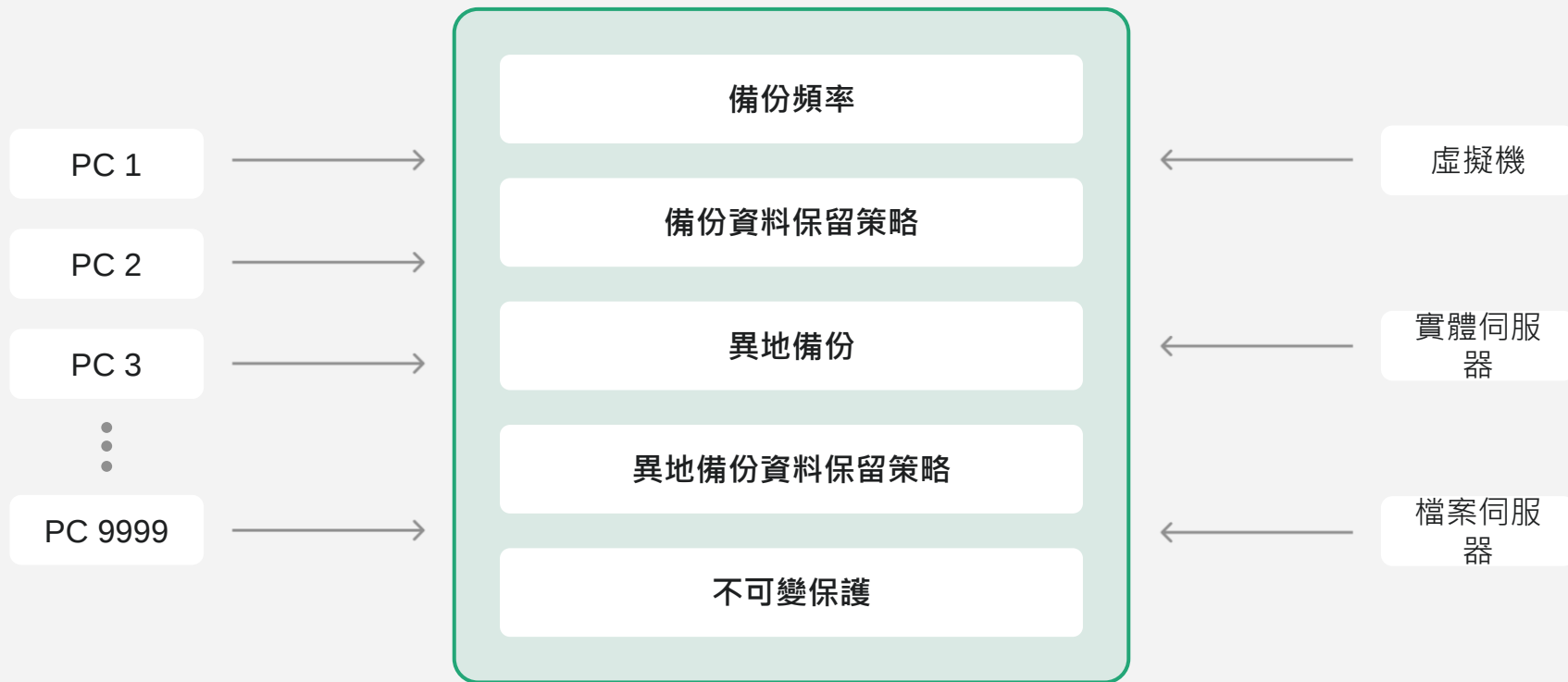
ISO27001 規範

- 針對任何系統、資料或應用程式，**產出可用副本**
- 應包括未直接由組織管理的基於**雲端平台**的資料
- 確保滿足組織的特定商業和營運需求（例如，**恢復時間目標、備份類型、備份頻率**）
- 確保備份資料根據其性質特定保留政策進行儲存

Synology ActiveProtect 跨平台集中保護



單一保護原則，涵蓋所有備份設定



自動完整保護

虛擬裝置

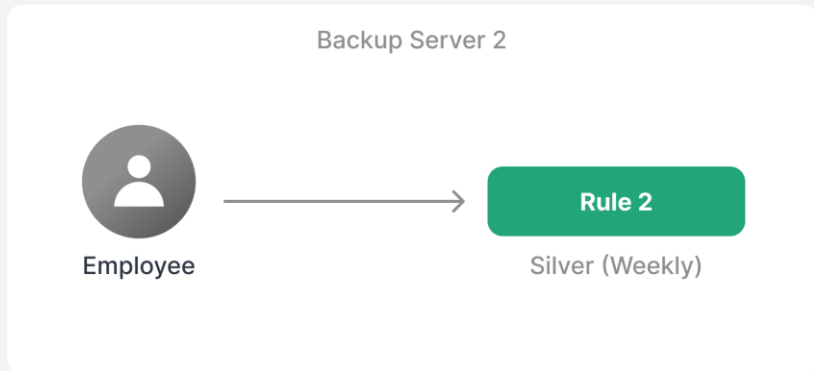
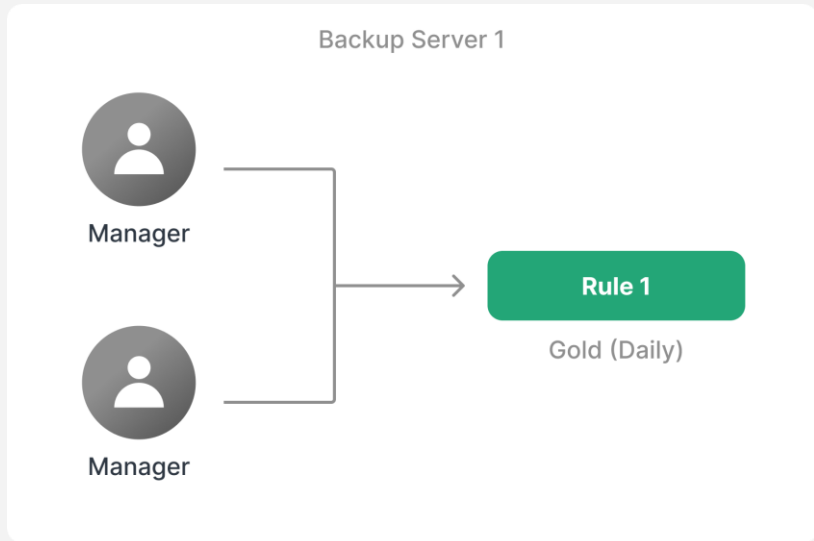
依據 虛擬機所在的 **host/cluster/folder** 自動套用保護原則

雲端服務

依據 帳號所屬的群組 自動套用保護原則

實體裝置

部署時帶入 **Connect Key** 以連線並自動套用保護原則



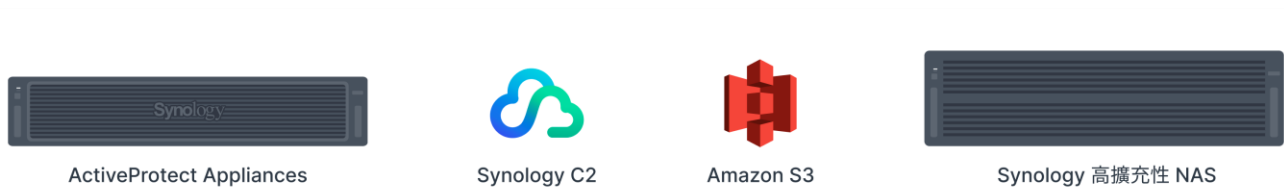
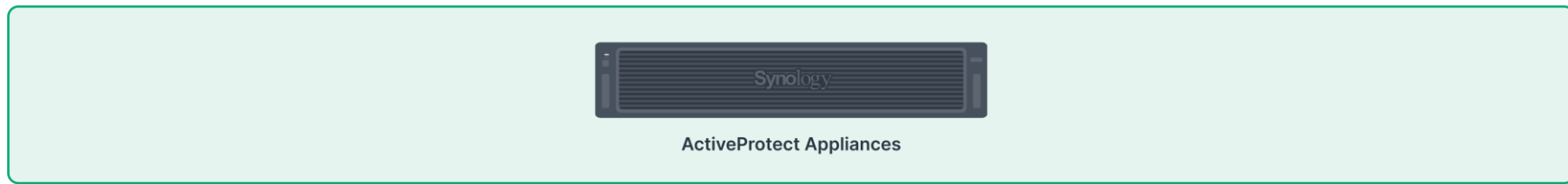
如何達成 ISO27001 ？

確保備份
可用性

ISO27001 規範

- 先檢查是否有資料遺失，再執行所有備份作業
- 根據風險等級，對已備份的資料進行加密
- 將備份儲存在適當的位置，此位置的環境應予以妥善保護、且為不同於來源資料的實體位置

原生異地備份能力



原生整合不可變保護，確保一致的資料保護原則

市售備份軟體

🔒 固定的硬體資料鎖定時間



Synology ActiveProtect

🔄 硬體資料鎖定時間自動同步資料留存設定



離線備份 (Air-gap)

- 隔離排程設定
- 彈性隔離選項
 - 防火牆封鎖
 - 網路埠關閉
 - 硬體關機

Air-gapped schedule

☐ Not apply

☒ Logical air-gap (Deny all connections) ⚙️

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun																								
Mon																								
Tue																								
Wed																								
Thu																								
Fri																								
Sat																								

Offline settings

☐ Logical air-gap (Deny all connections)

Deny all inbound connections through data interfaces during the air-gap period.

☒ Physical air-gap (Disable NICs)

Deny all inbound and outbound connections through data interfaces by turning off the NICs.

☐ Physical air-gap (Power off)

Power off the entire appliance. It is recommended to apply this to appliances used solely as backup copy destinations.

Note:

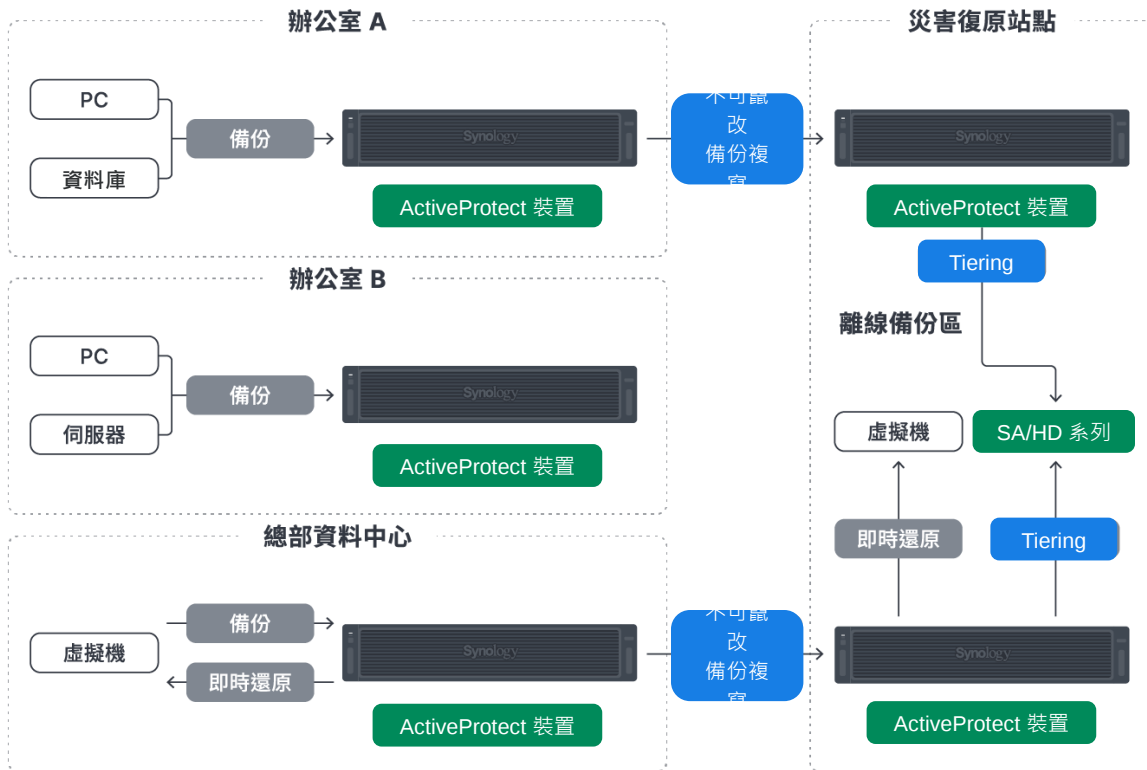
- The schedule will be run on the local time of this server.
- Tasks that have not started execution after going offline will start in the next online session.
- Tasks that have already started running will be queued and retried for 72 hours.

Cancel

Save

ActiveProtect

一站式規劃部署多層次防護架構



「要求建立一個資料儲存庫（Data Vault），讓金融業成員在遭受攻擊有一個
隔離的、離線的、不受感染的備份副本可立即被存取並還原系統的運作。」

- 美國避風港計畫 -

如何達成 ISO27001 ？

建構備份
可還原性

ISO27001 規範

- 強制**定期測試**備份與還原，保證資料可用性以便在需要時，能**立即還原**檔案、系統或應用程式
- 備份測試應根據組織需要的復原時間進行衡量，以確保在資料遺失或系統故障時能夠依此回復

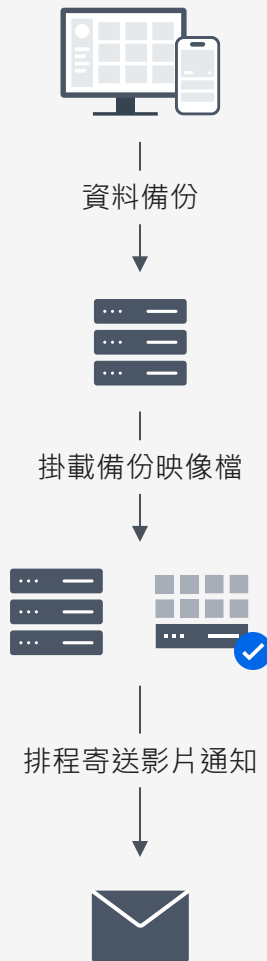
內建主、被動備份驗證， 確保資料可還原性

- 自動修復備份資料

主動偵測錯誤或損壞的資料，並透過自動修復功能修復毀損資料

- 自動驗證備份資料

搭配 Synology 內建虛擬機運行，匯入備份影像與運行時拍攝影片



內建主、被動備份驗證， 確保資料可還原性

- 自動修復備份資料

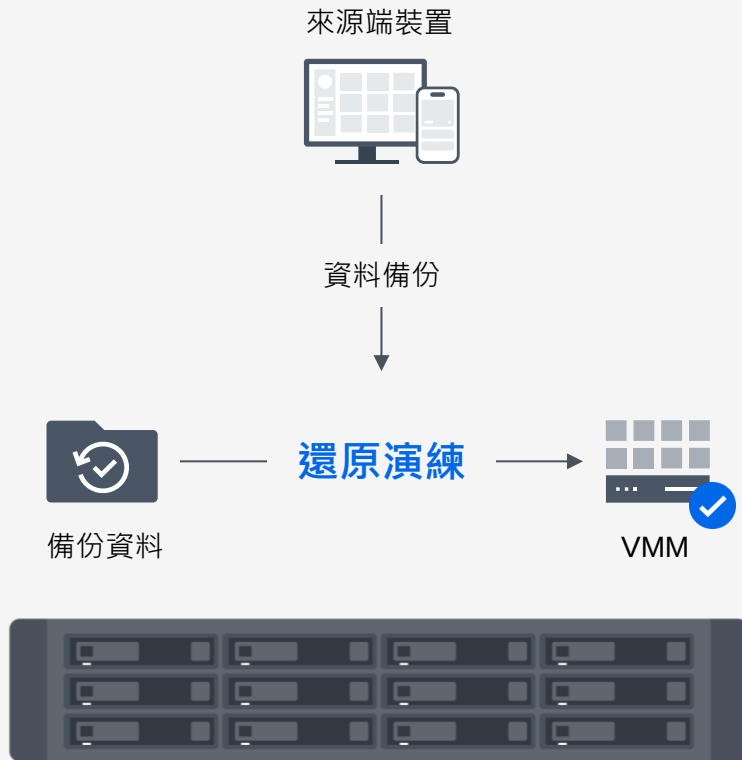
主動偵測錯誤或損壞的資料，並透過自動修復功能修復毀損資料

- 自動驗證備份資料

搭配 Synology 內建虛擬機運行，匯入備份影像與運行時拍攝影片

- 沙盒環境備份演練

透過 Synology 內建虛擬機定期還原演練，不影響正式營運環境



如何達成 ISO27001 ?

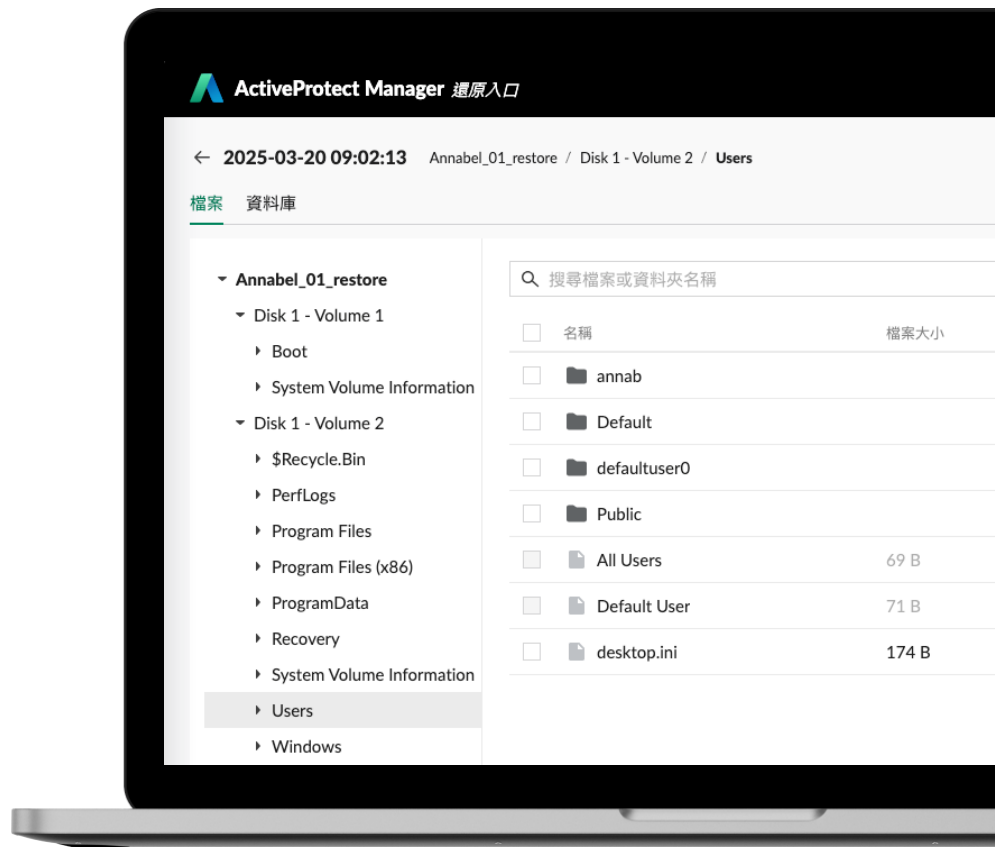
多元還原
隨需取回

ISO27001 規範

- 概述清楚且具體的還原程序，還原範圍涵蓋所有相關關鍵系統和服務。

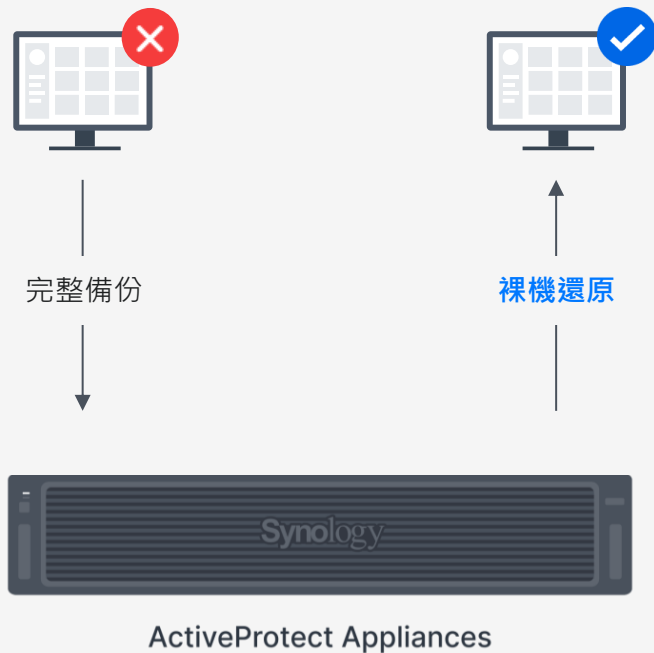
多元還原，依實際需求 恢復關鍵資料

- 精細檔案層級還原



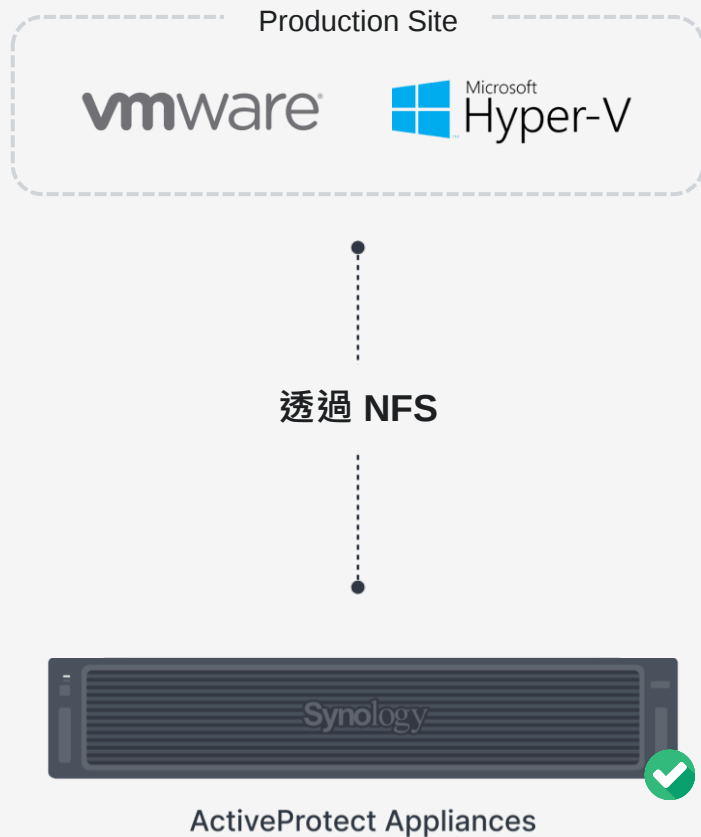
多元還原，依實際需求 恢復關鍵資料

- 精細檔案層級還原
- 系統裸機還原

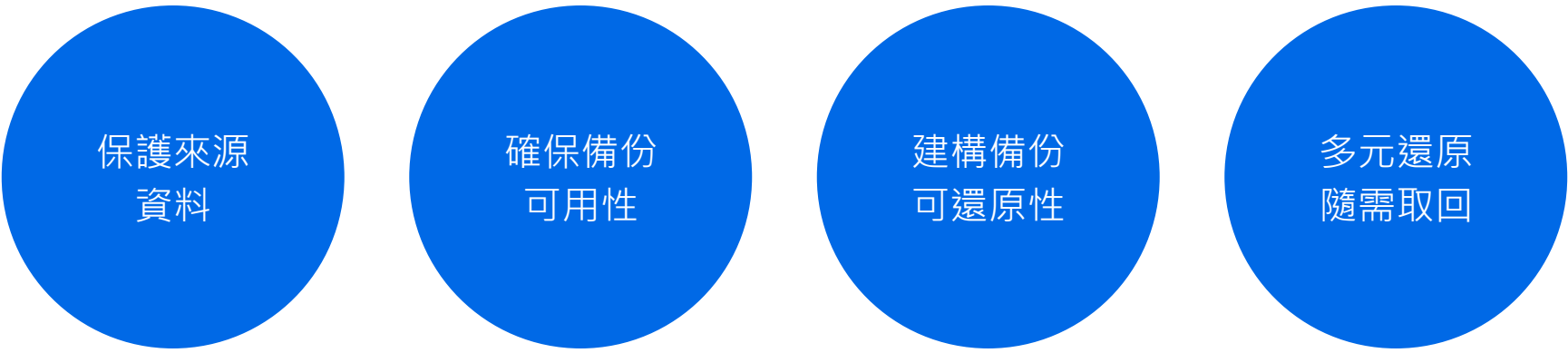


多元還原，依實際需求 恢復關鍵資料

- 精細檔案層級還原
- 系統裸機還原
- 即時還原
 - P2V, V2V 還原
 - 跨 Hypervisor 還原



依循 ISO27001 的四大要素



保護來源
資料

確保備份
可用性

建構備份
可還原性

多元還原
隨需取回



Synology ActiveProtect 備份專用一體機，
如何幫企業完善資料保護策略？

杰鑫國際物流

透過備份專用一體機 ActiveProtect，
快速部署異地備份並
集中管理 10+ 台的分點備份伺服器

挑戰

- 既有佈署超過 10 台以上 Synology 備份伺服器，需要各別查看分點伺服器狀況
- 因應稽核規需要針對單一伺服器甚至是工作負載分別設定保護規則，資料保護規則設定與管理流程繁雜且耗時
- 產業特性特殊，相當注重資安合規性，其中針對異地備份便需要部署距離 20 公里以上的保護措施



杰鑫國際物流

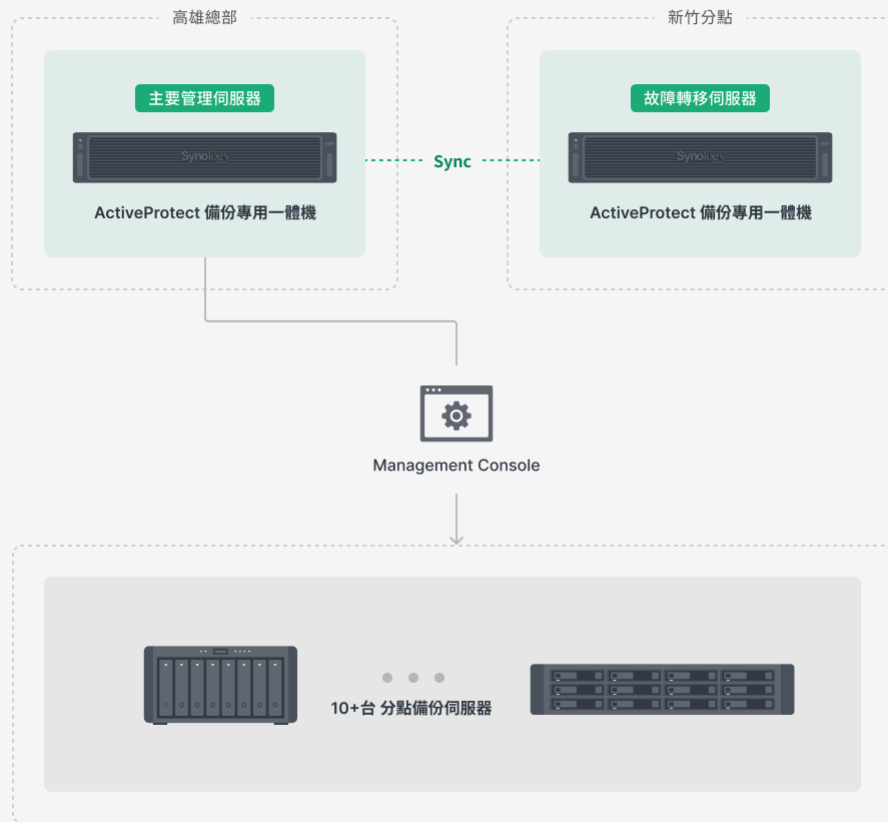
透過備份專用一體機 ActiveProtect，
快速部署異地備份並
集中管理 10+ 台的分點備份伺服器

挑戰

- 既有佈署超過 10 台以上 Synology 備份伺服器，需要各別查看分點伺服器狀況
- 因應稽核規需要針對單一伺服器甚至是工作負載分別設定保護規則，資料保護規則設定與管理流程繁雜且耗時
- 產業特性特殊，相當注重資安合規性，其中針對異地備份便需要部署距離 20 公里以上的保護措施

導入成效

- 透過**集中管理單一介面**即可查看所有備份運行狀況，大幅減少 IT 管理人員每日維運時間
- 透過**保護原則管理備份一次設定**，輕鬆滿足規範
- **重複資料刪除率逾 80%**
- 每年定期舉辦還原演練，**滿足 ISO27001 的合規要求**





Synology 資料保護解決方案 如何助杰鑫國際物流滿足 ISO27001 ?

Synology 助杰鑫國際物流滿足 ISO27001 要求



RTO

< 30 mins

RPO

完全合規



杰鑫國際物流股份有限公司

杰鑫國際物流如何實際執行還原演練？

杰鑫國際物流如何運用 Synology 實作備份演練 確保資料可還原性？



導入成效

- 只需要短短幾分鐘即可完成
- 演練作業完全隔絕於 production site 的環境，有效避免影響組織正常營運
- 確實掌握備份資料的可還原性，提升營運韌性



" 台灣光罩以 Synology 完善 3 PB
巨量資料備份，達成備份 3-2-1 及
ISO27001 落實合規性 "

" 春源鋼鐵攜手 Synology 完整
守護全台 11 廠區資料，打造 5 分
鐘即可回復的營運持續計畫 "



廣受全球 企業使用者信賴

150K+

全球企業用戶

50%+

台灣百大企業均採用 Synology



台灣光華



春源鋼鐵
CHUN YUAN STEEL



NAR Labs 財團法人國家實驗研究院

國家高速網路與計算中心
National Center for High-performance Computing



AI Labs.tw
台灣人工智慧實驗室

SHISEIDO



SK shipping



Interasia



台新金控
Taishin Holdings



W
UNIVERSITY of
WASHINGTON



AMBASSADOR
Hotels & Restaurants
國賓大飯店



TOYOTA



JetstarPacific
Jetstar

從上市櫃公司到各產業組織， 加速達成 ISO27001 資料安全合規性 之策略解析

免費填表諮詢 Synology 專家
讓我們為您規劃資安合規策略

