# 如何落實網路韌性：Veritas 360 Defense 實戰指南

Siegfried Chen 陳力維

Veritas SE 資深技術顧問

## Downtime

38% 的資深IT主管回報，一次的成功攻擊會導致5天以上的停機時間

## Data Loss

根據研究，多達 20% 的資料可能無法恢復。

* All Data Points from 2023 Data Risk Management Research




VERITAS

# 超越災難還原的韌性

Impact

Complexity

## Cyberattacks

**Malicious Incident**

備份平台是攻擊目標，通常資料已洩露，影響是全範圍的

資料可能無法存取

資料可能無法還原

## Disasters

**Non-Malicious Incident**

備份平台不是目標，
通常資料是完整的，影響也是區域性的

系統中斷

資料可存取

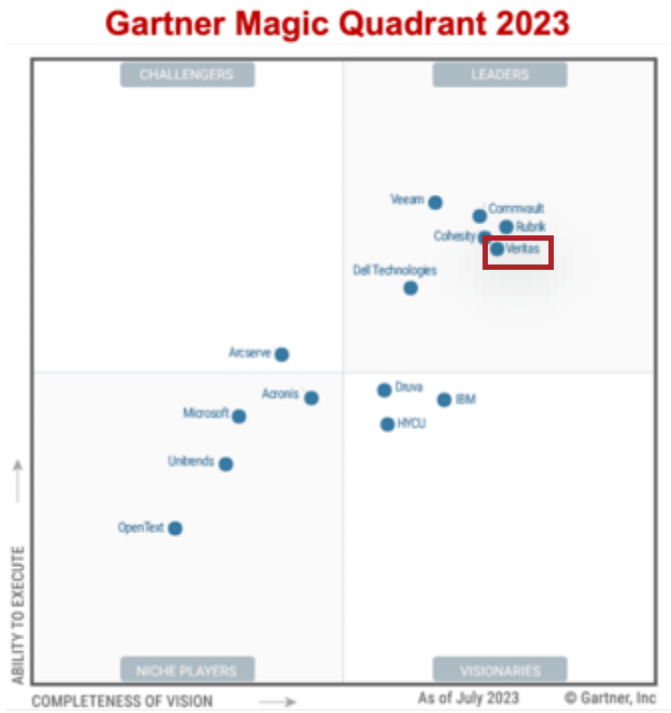
資料可還原




VERITAS

# 從Disaster Recovery到Cyber Recovery

## Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solution 2023

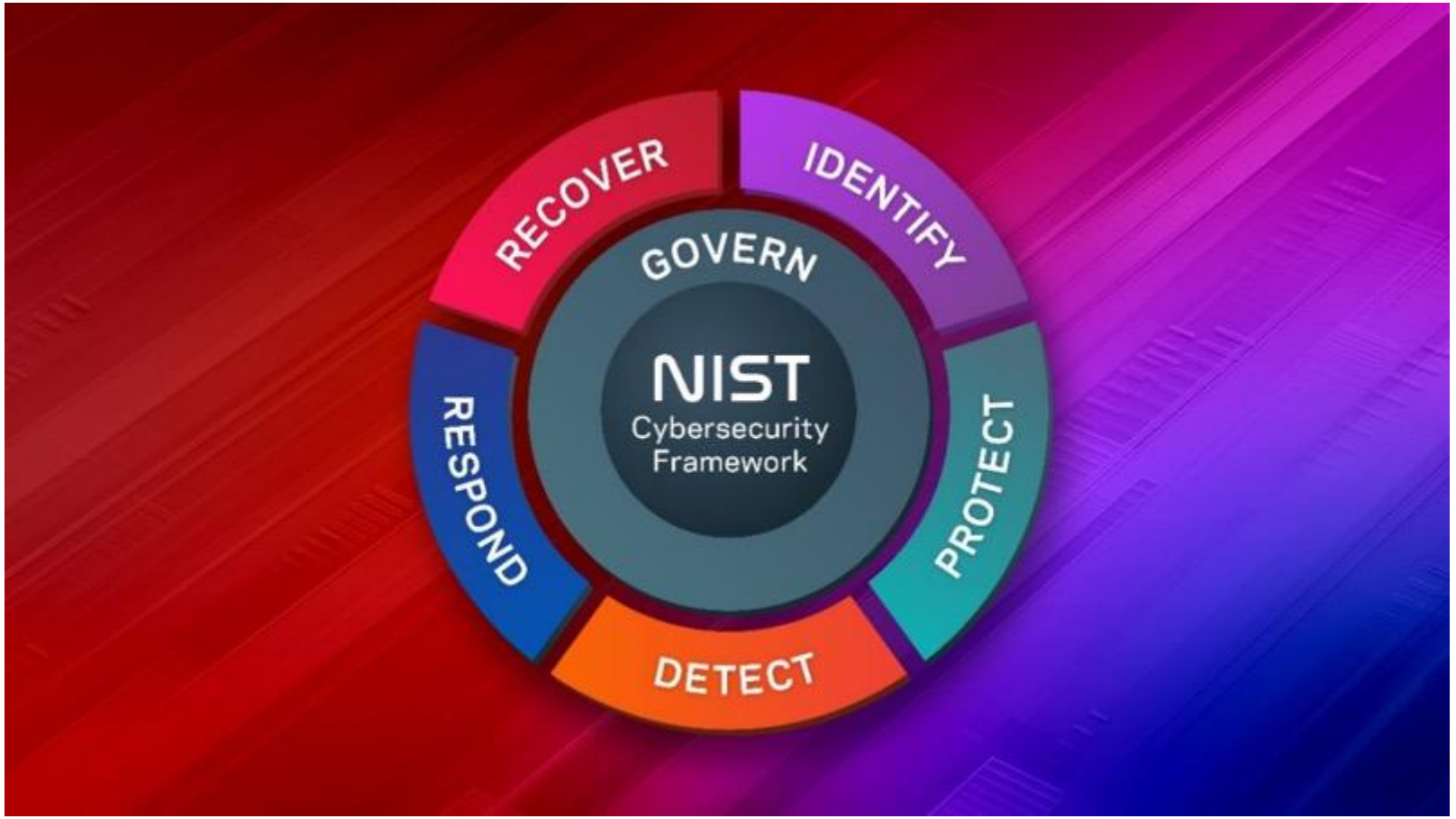



## IDC: Worldwide Cyber-Recovery 2023 Vendor Assessment


IDC：”Veritas may be the best cyber-resilience solution you've never heard of”

# NIST Cybersecurity Framework 2.0

事前預防(Identify/Protect)、事中應變(Detect/Respond)、事後恢復(Recover)



VERITAS REDLab

# 結合一流的方案<br>面對各種真實攻擊

## 惡意軟體實際演練

- 植入惡意軟體
- 驗證韌性
- 確保還原能力

## 安全分析

- 獨立研究
- 識別新的攻擊形態
- 更新防禦機制

## 強化產品

- 測試實際攻擊情境
- 持續強化產品特色與功能



VERITAS

# Veritas 網路安全夥伴生態系統


**Identity Management**

Microsoft · okta · PingIdentity · Shibboleth

**Malware Detection**

McAfee · Microsoft Defender · Symantec by Broadcom

**Security Operations**

HITACHI Inspire the Next · kyndryl

**Data Security**

ANZEN · Calamu

**Security Posture Management**

CROWDSTRIKE · Qualys

**Privileged Access | Active Directory Security**

CYBERARK · semperis

**SIEM/SOAR**

Microsoft Sentinel · securonix · splunk>

**Key Management**

Fortanix · HashiCorp · IBM · THALES · utimaco

**Data Loss Prevention**

Symantec by Broadcom




VERITAS

# Cyber Recovery 30-60-90 檢核清單

落實計劃以確保還原零失誤

30 DAYS | 60 DAYS | 90 DAYS

## PHASE 1

### *基礎建設*

- ❑ 針對所有工作負載建立保護與保留政策
- ❑ 使用不可變儲存
- ❑ 落實3, 2,1 備份策略 (包含一個虛擬和/或實體的Air Gap或SaaS隔離)
- ❑ 套用安全控制(例如MFA, MPA, 網路隔離, RBAC, 加密)
- ❑ 考慮使用強化過後的專屬備份一體機
- ❑ 啟用支援AI的異常分析
- ❑ 啟用惡意軟體偵測和保留規則
- ❑ 更新軟體與安全更新(持續性)

## PHASE 2

### *主動管理風險*

- ❑ 識別"遺漏"的關鍵資產
- ❑ 執行暗資料分析
- ❑ 查找與分類機敏資料
- ❑ 識別與監視高風險的使用者行為
- ❑ 建立一個隔離的還原環境(IRE或clean room)
- ❑ 建立還原執行腳本(recovery runbook)，調整操作順序
- ❑ 整合資安操作(SecOps)並建立事件回應營運手冊(playbooks) (例如SIEM / SOAR / XDR整合)

## PHASE 3

### *精煉、演練、落實*

- ❑ 調整備份政策以達成100%的備份成功率，以符合SLA要求
- ❑ 調整支援AI的異常偵測 (消除誤報false positives/negatives)
- ❑ 執行桌上模擬演習 (包含不中斷的還原演練)
- ❑ 演練還原與驗證結果




VERITAS

# Cyber Recovery 30-60-90 檢核清單

落實計劃以確保還原零失誤

**30 DAYS**

**PHASE 1**

***基礎建設***

- 針對所有工作負載建立保護與保留政策
- 使用不可變儲存
- 落實3, 2,1 備份策略 (包含一個虛擬和/或實體的Air Gap或SaaS隔離)
- 套用安全控制(例如MFA, MPA, 網路隔離, RBAC, 加密)
- 考慮使用強化過後的專屬備份一體機
- 啟用支援AI的異常分析
- 啟用惡意軟體偵測和保留規則
- 更新軟體與安全更新(持續性)

# 單一平台管理雲地多資料中心

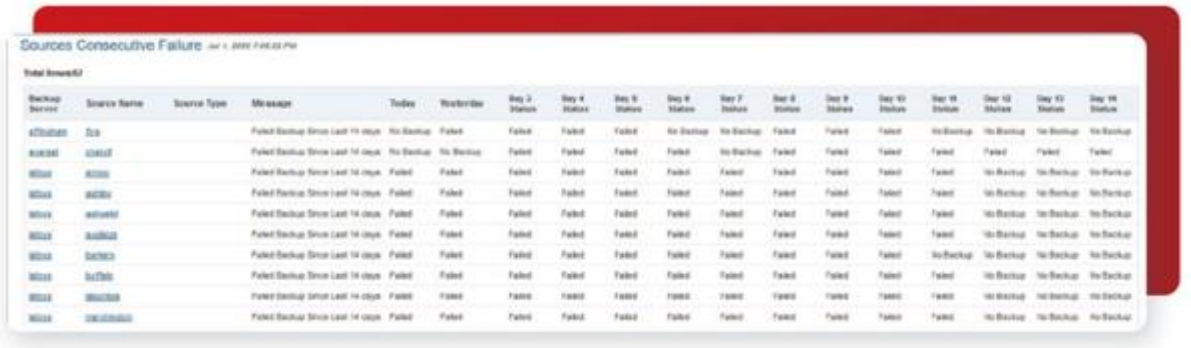


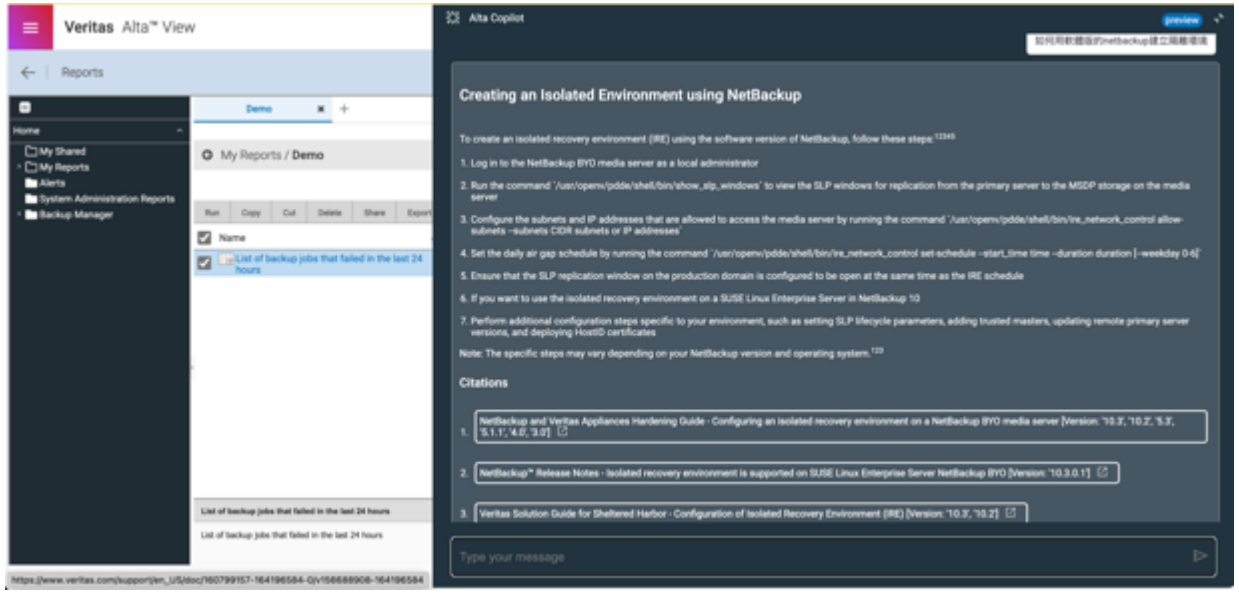
**資產探索：**
查找檔案伺服器、資料庫和其他備份目標

**匯入既有清單：**
利用CMDB, ITAM, CSV, vSphere 來確認備份目標

**善用分析以確保備份覆蓋：**
識別遺漏的備份目標或失敗的備份

**支援自然語言的Alta Copilot**
以自然語言查找問題資產、產生報表



# 利用分析/儀表版/評分表來改善安全性



**勒索軟體就緒評分表：**

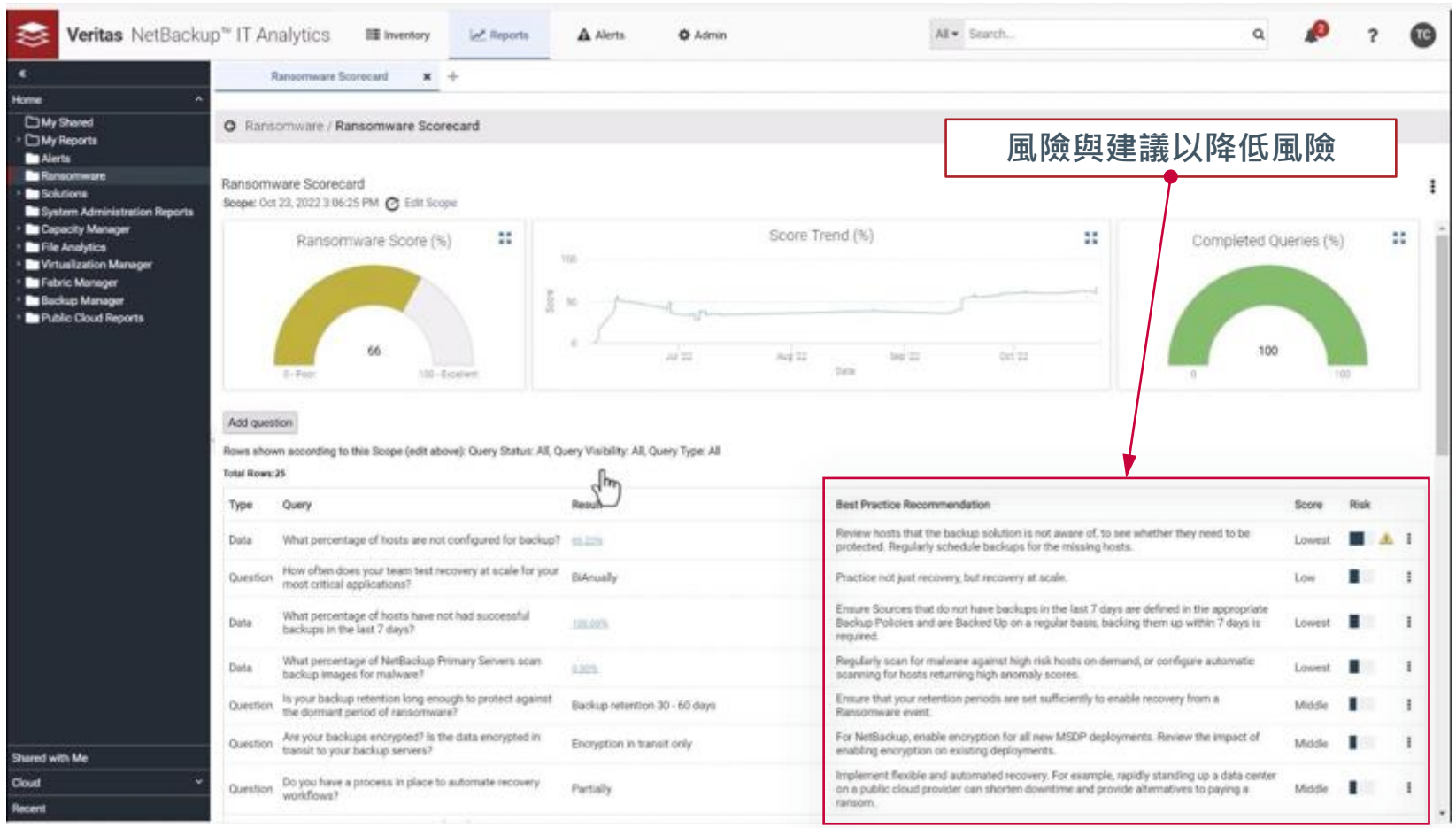
依據標準或客製的KPI(例如備份成功率)，來識別勒索軟體防護狀態是否存在風險

**安全態勢校正：**

追蹤勒索軟體計分卡風險的補救狀況

**社交工程儀表板：**

根據使用者存取權限和易受攻擊的共享來了解風險狀態



# 強化使用者/網路存取控制



**Multi-factor authentication (MFA):**

使用 MFA 阻止密碼破解和帳密偷取，以降低未經授權存取平臺、資料和設置的風險。 可使用 Veritas MFA 或透過SAML使用現有系統

**Multi-person authorization (MPA):**

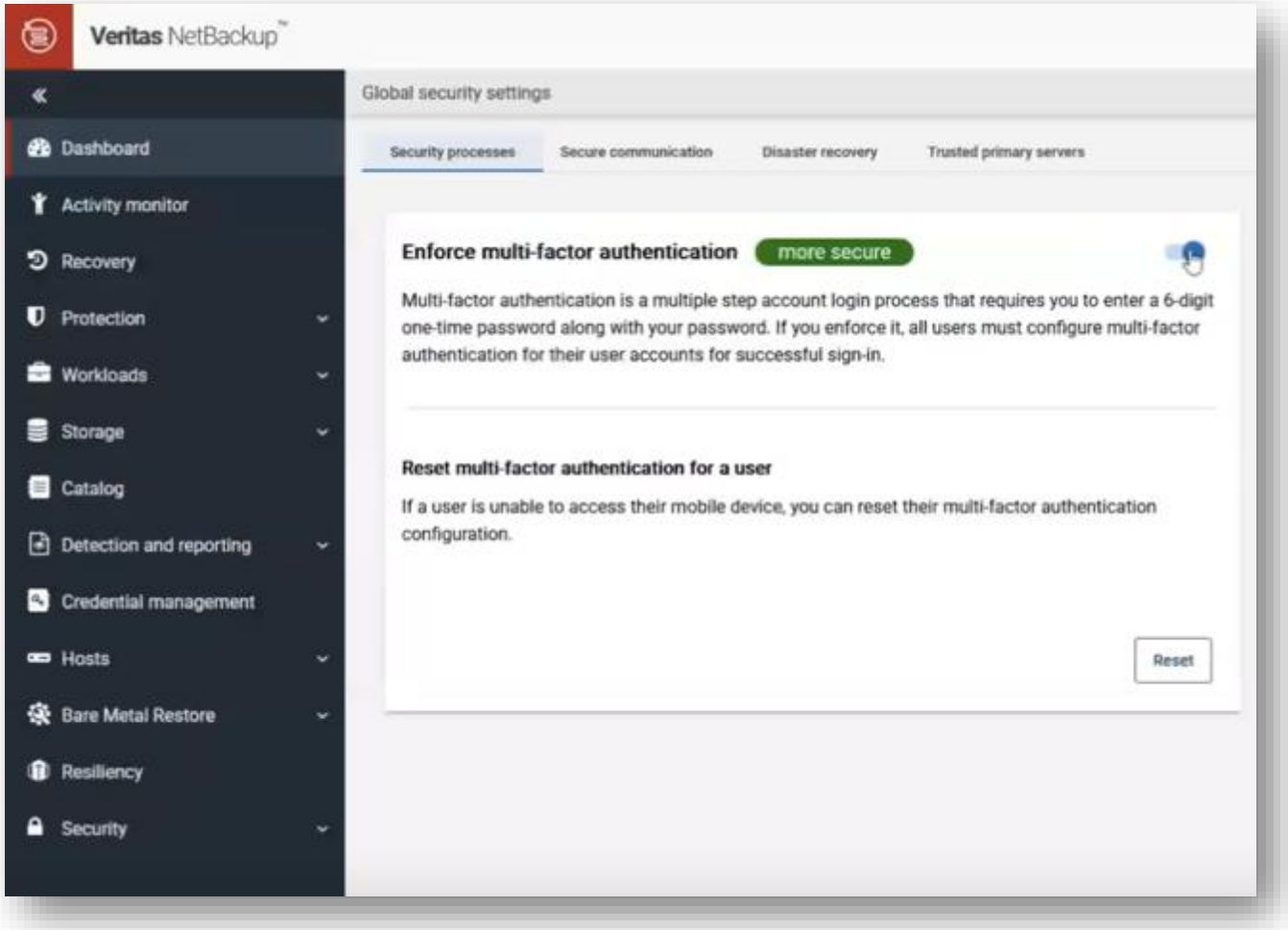
通過要求 2 人或更多人批准更改和存取權限，防止單方面更改和設置，例如將備份刪除、過期和 root存取權限

**Privileged Access Management:**

整合CyberArk 來確保對平臺和設備的特權存取都受到監控和管理

**Key Management System:**

利用現有 KMS 簡化部署或使用 Veritas 原生功能。



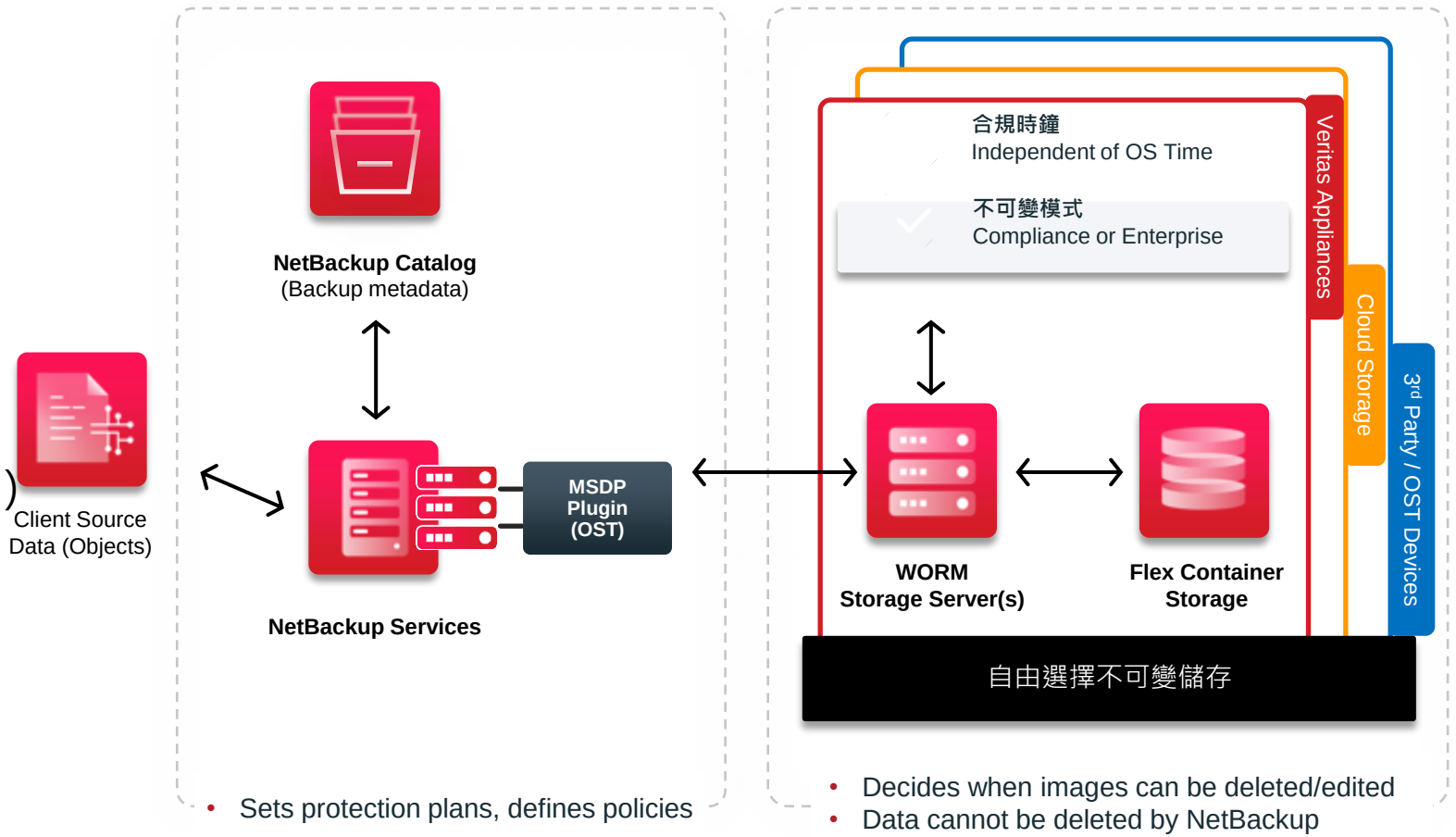
# 確保資料韌性

**多層不可變與保留：**
防止資料破壞，因為無法編輯或修改資料，並且在保留期到期之前不會刪除備份副本

**一體機服務容器化：**
所有服務都是容器化的，因此它們本質上是不可變和安全的

**資料儲存加密：**
以Galois/Counter Mode（GCM）AES-256 bit落實 NIST AES 256加密演算，防止未經授權的資料存取

**資料傳輸加密：**
利用TLS 1.3加密，以防止網路竊聽



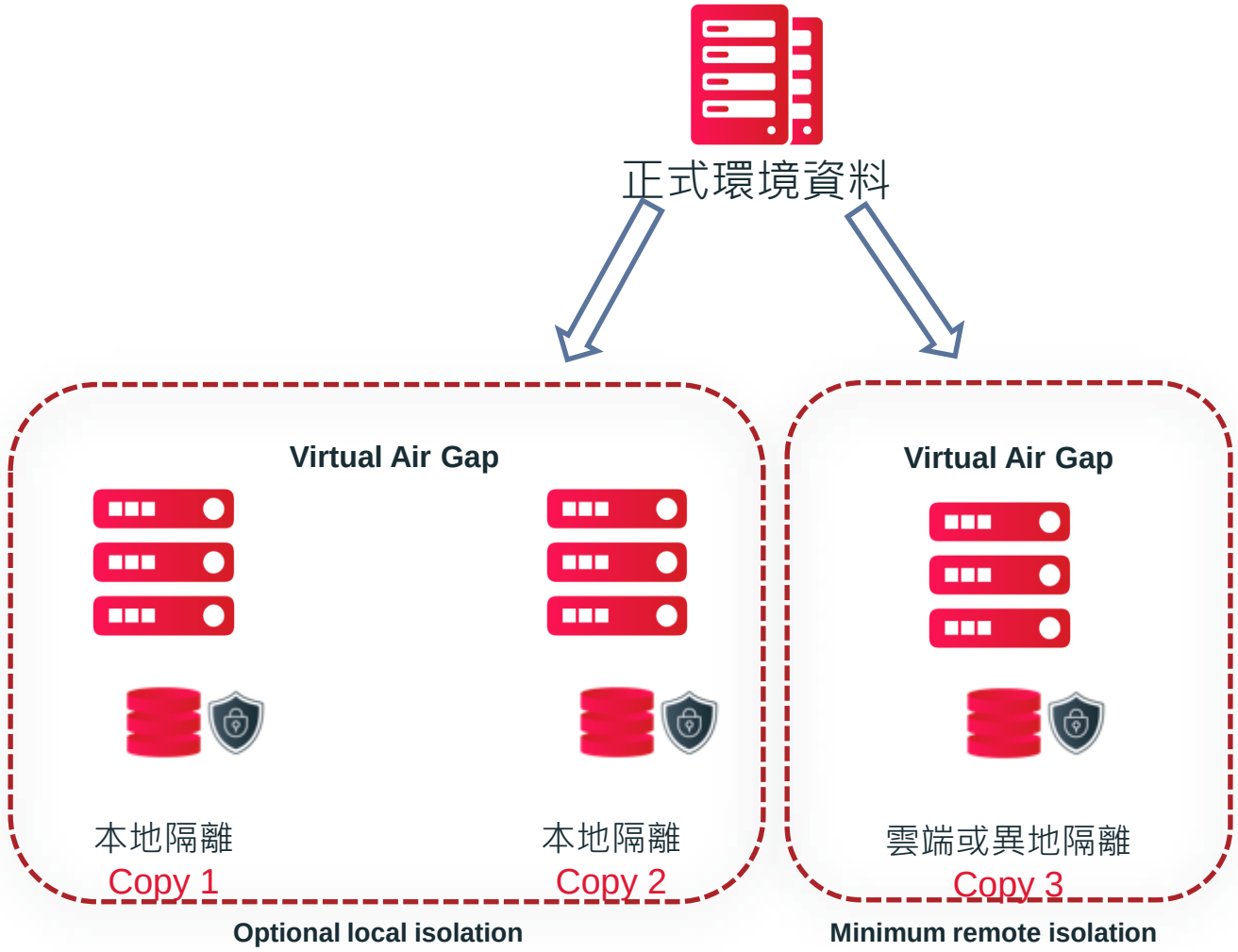
# 隔離

本地、異地、雲端



**依3-2-1原則設計的**
**完整隔離**

- 單一政策
- 3 份複本
- 3 種保留時間
- 3 種不可變選項
- 零信任原則
- AI驅動的安全性







VERITAS

# 利用SaaS達成雲端隔離

彈性的隔離儲存協助混合與多雲的資料保護



**一點即用的隔離：**

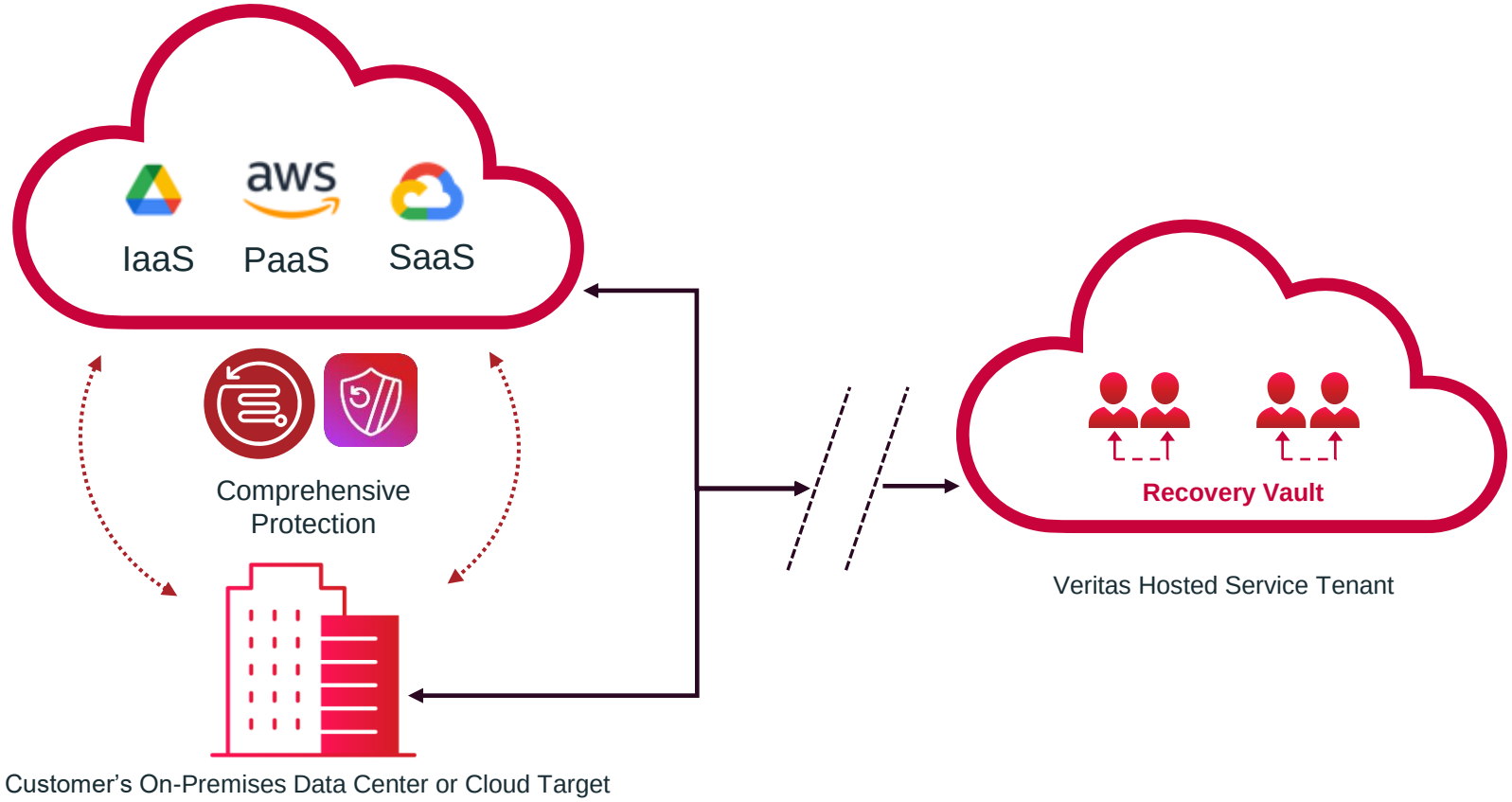
全託管資料隔離服務（SaaS）到雲端

**零信任原則與威脅偵測：**

預設情況下，加密、MFA、RBAC 和特權存取管理與異常檢測相結合，可及早發現新出現的勒索軟體

**資料隔離：**

利用非持續連線來達成動態的AirGap



VERITAS

# 地端隔離

## 本地與異地隔離

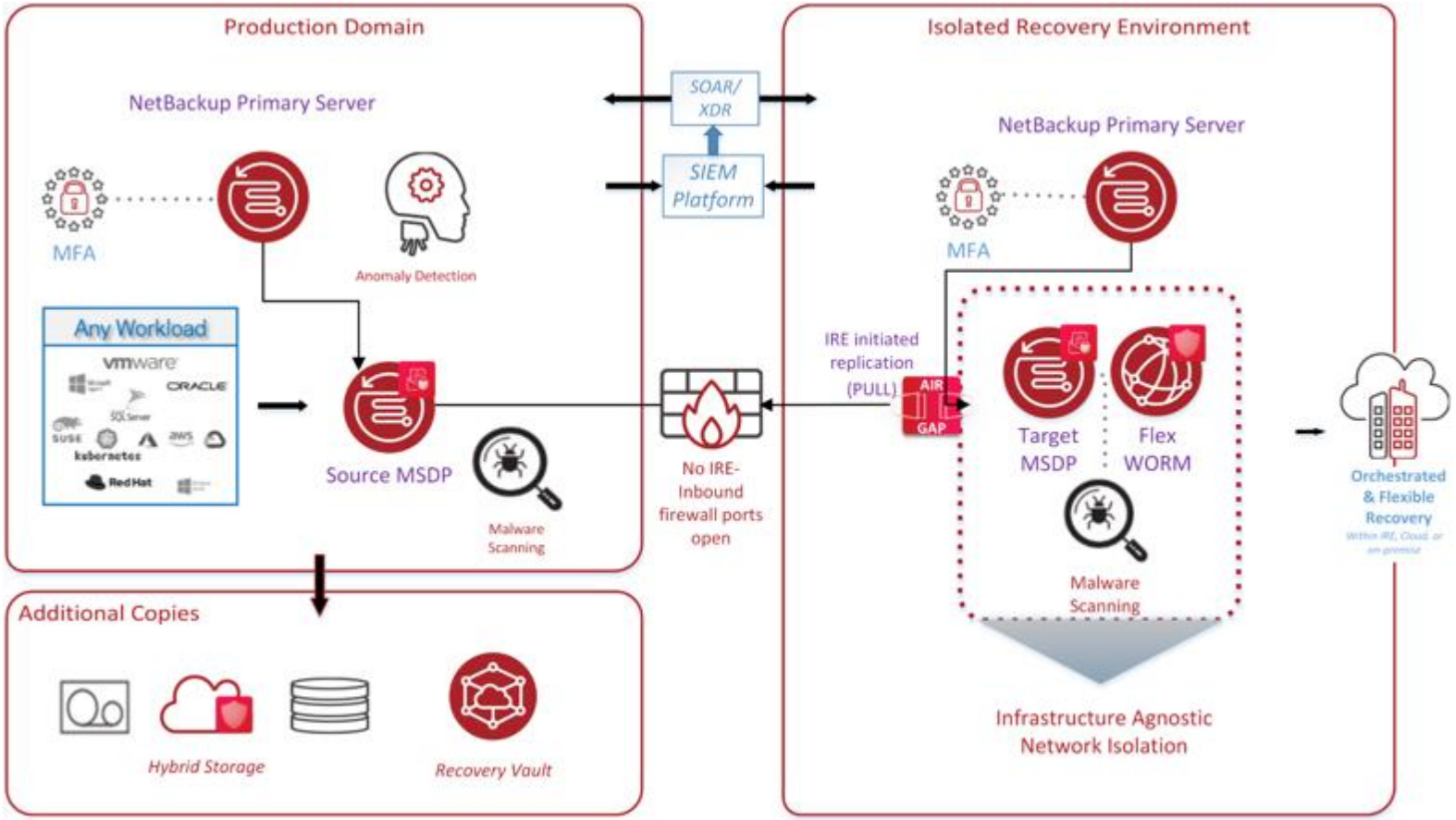


**本地隔離：**

將資料副本儲存在虛擬隔離(air gapped)、不可變和不可刪除的儲存設備中

**異地隔離：**

將遠端副本儲存在虛擬隔離(air gapped)、不可變和不可刪除的儲存設備中







VERITAS

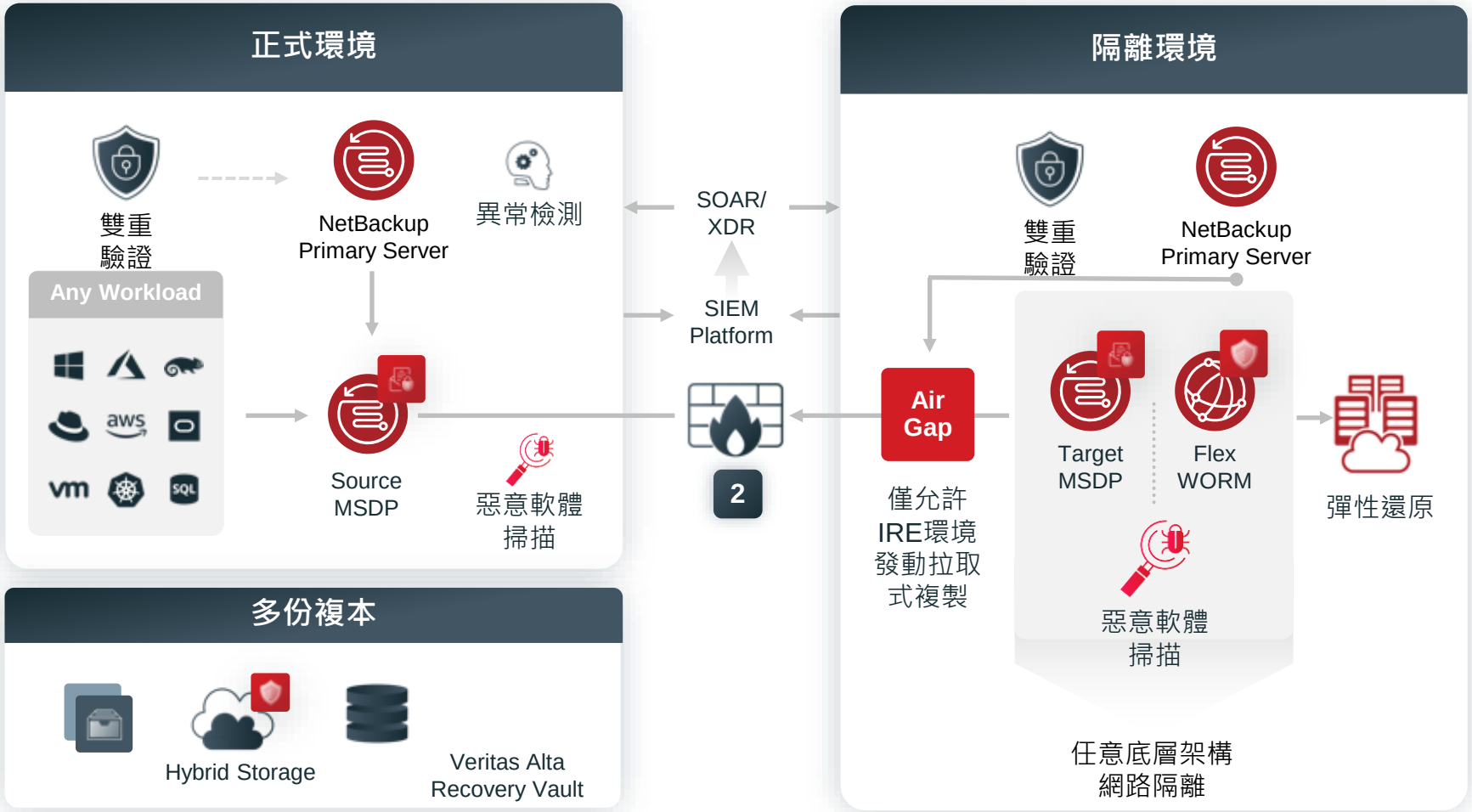
PREVENT DATA DESTRUCTION — ISOLATED RECOVERY ENVIRONMENT

# 地端隔離：建立單向拉取式的隔離環境

本地與異地隔離

使用腳本自動執行將資料連接和配置到 Cleanroom/IRE 的步驟

1. 即時異常檢測和按需惡意軟體掃描
2. 基於PULL方法的可操作Air Gap進行資料隔離
3. 基於多租戶 WORM 儲存和 BYOS 選項，確保資料完整性
4. 大規模恢復到上次已知的良好狀態







VERITAS

STRENGTHEN CYBER DEFENSE – DETECT

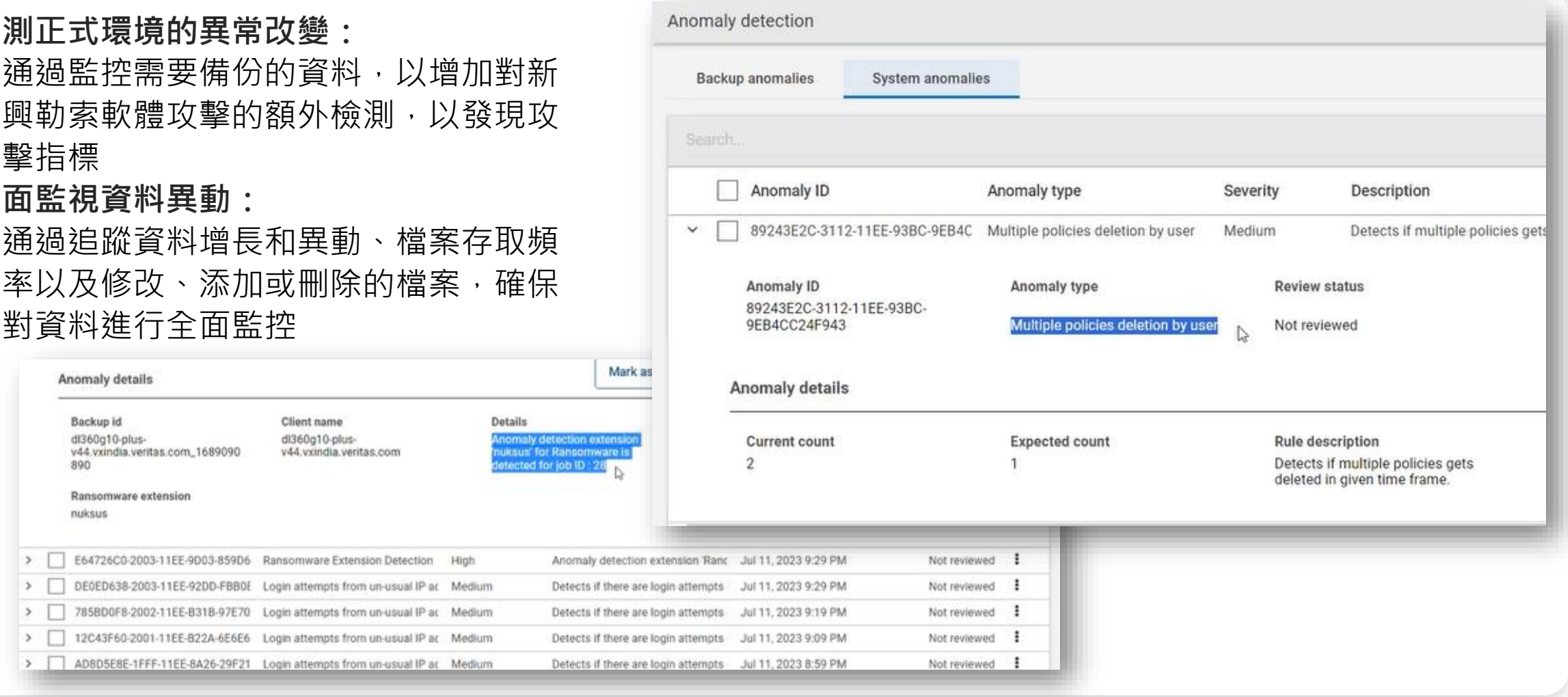
# AI/ML驅動的異常偵測

**偵測正式環境的異常改變：**

通過監控需要備份的資料，以增加對新興勒索軟體攻擊的額外檢測，以發現攻擊指標

**全面監視資料異動：**

通過追蹤資料增長和異動、檔案存取頻率以及修改、添加或刪除的檔案，確保對資料進行全面監控







VERITAS

# 惡意軟體與弱點偵測



**惡意軟體掃描：**

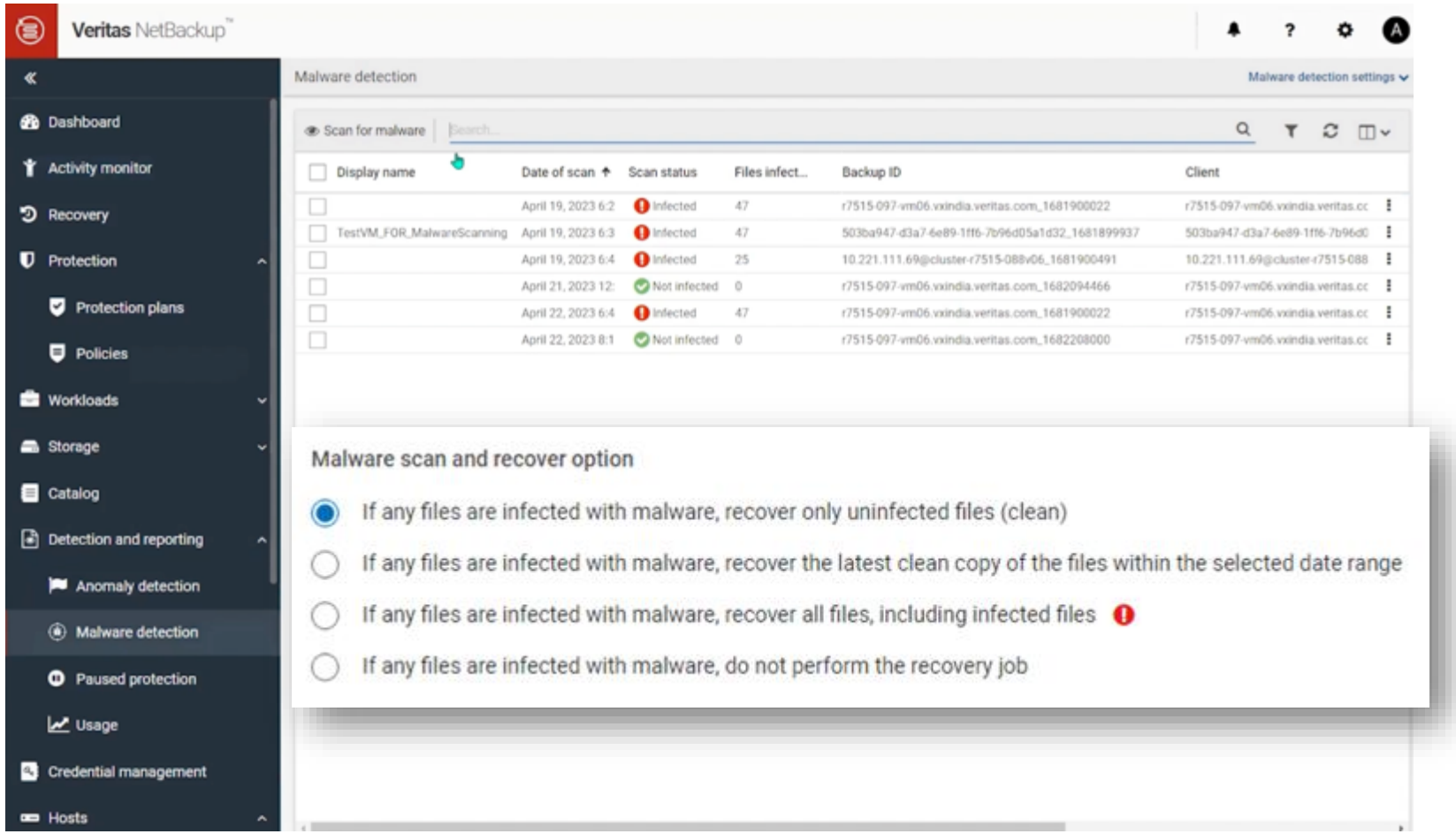
使用領先的惡意軟體工具掃描和分析備份中的非結構化資料以查找惡意軟體。

**支援的資料來源：**

Backup 影像, VMs, Windows, NetBackup Universal Shares, cloud, K8s, DNAS 與 OST

**弱點掃描：**

結合 Qualys Vulnerability and Configuration Management從備份資料中檢測資料、虛擬機和系統的漏洞。



# Cyber Recovery 30-60-90 檢核清單

落實計劃以確保還原零失誤

60 DAYS

PHASE 2

***主動管理風險***

- 識別”遺漏”的關鍵資產
- 執行暗資料分析
- 查找與分類機敏資料
- 識別與監視高風險的使用者行為
- 建立一個隔離的還原環境(IRE或clean room)
- 建立還原執行腳本(recovery runbook)，調整操作順序
- 整合資安操作(SecOps)並建立事件回應營運手冊(playbooks)(例如SIEM / SOAR / XDR整合)



VERITAS

# 資料的搜查與分類



**AI 驅動的資料搜查:**

提高準確性，減少漏報/誤報

**支援各種資料來源(Microsoft, Dell/EMC, CIFS/NFS, NetApp, S3, Box):**

支援異質環境

**1,200以上的規則/ 275以上的分類政策:**

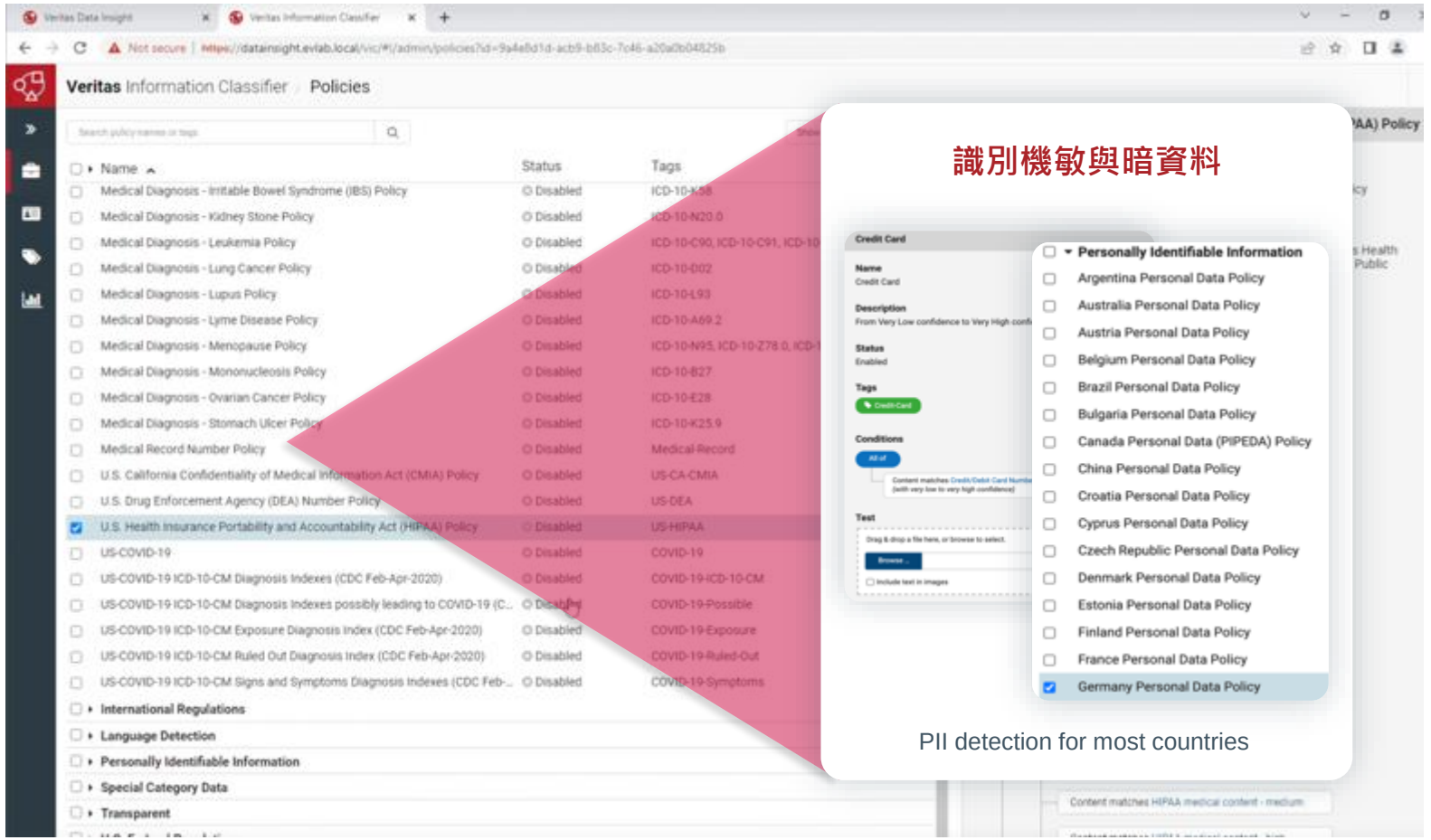
支援全球各地的個資政策、金融和醫療相關法規

**匯入即有的分類規則:**

利用以前的 DLP Discovery為企業環境提供單一分類來源

**支援OCR:**

全面、快速地發現圖像和掃描文檔中的敏感資料







VERITAS

# 管理資料風險

識別與監視風險



**識別使用者風險：**

在規劃存取政策時，根據角色和敏感要求分析使用者的風險狀況

**使用者行為：**

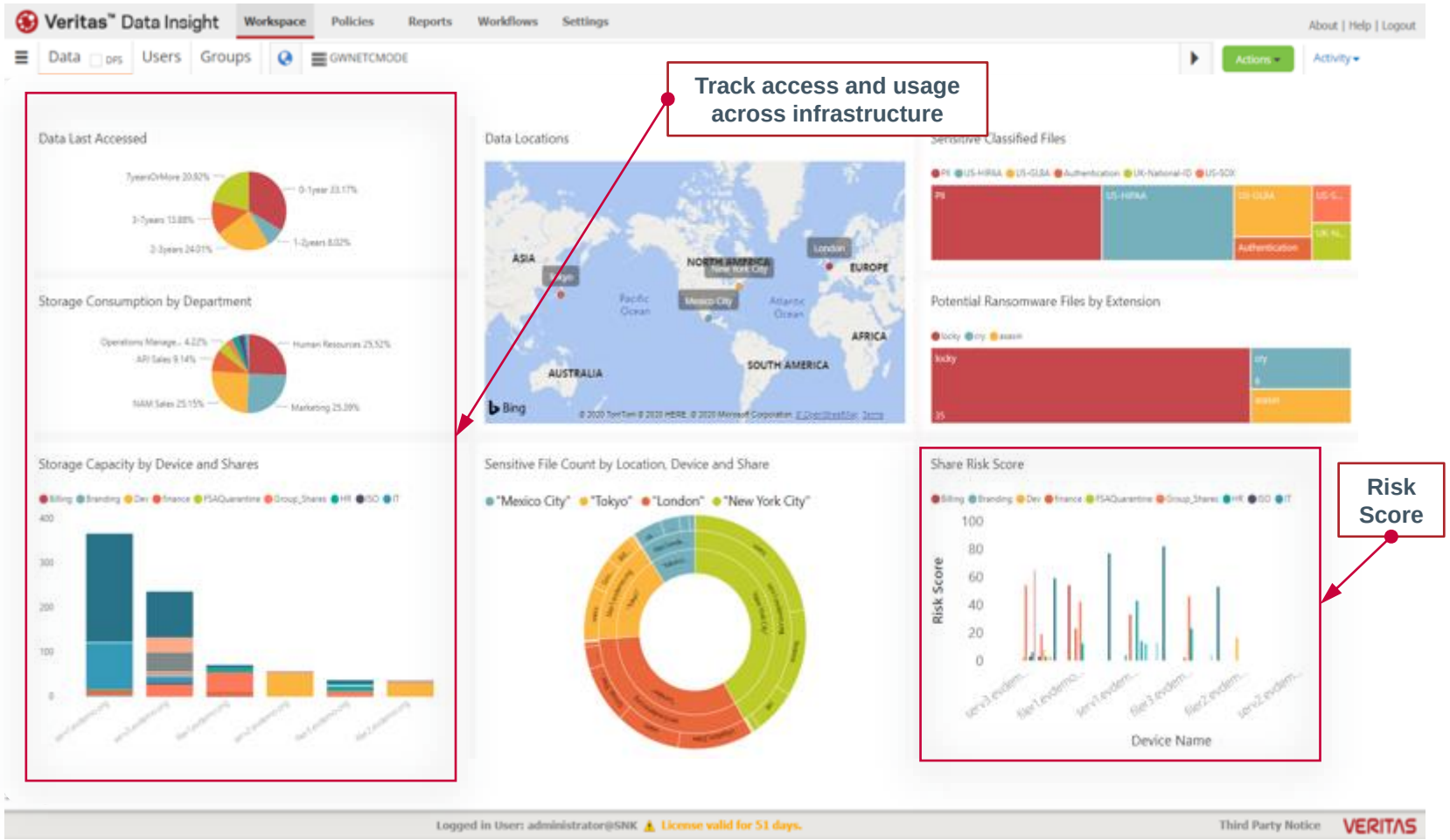
根據用戶風險和資料敏感度為異常使用者存取建立警報

**持續監視資料勢態：**

確保現有和新的資料具有對應的策略和控制措施，以滿足組織的安全要求

**依風險發出警示：**

釐清資料保護、資料安全和資料治理方面的落差



VERITAS

# 優化資料保護平台與備份資料



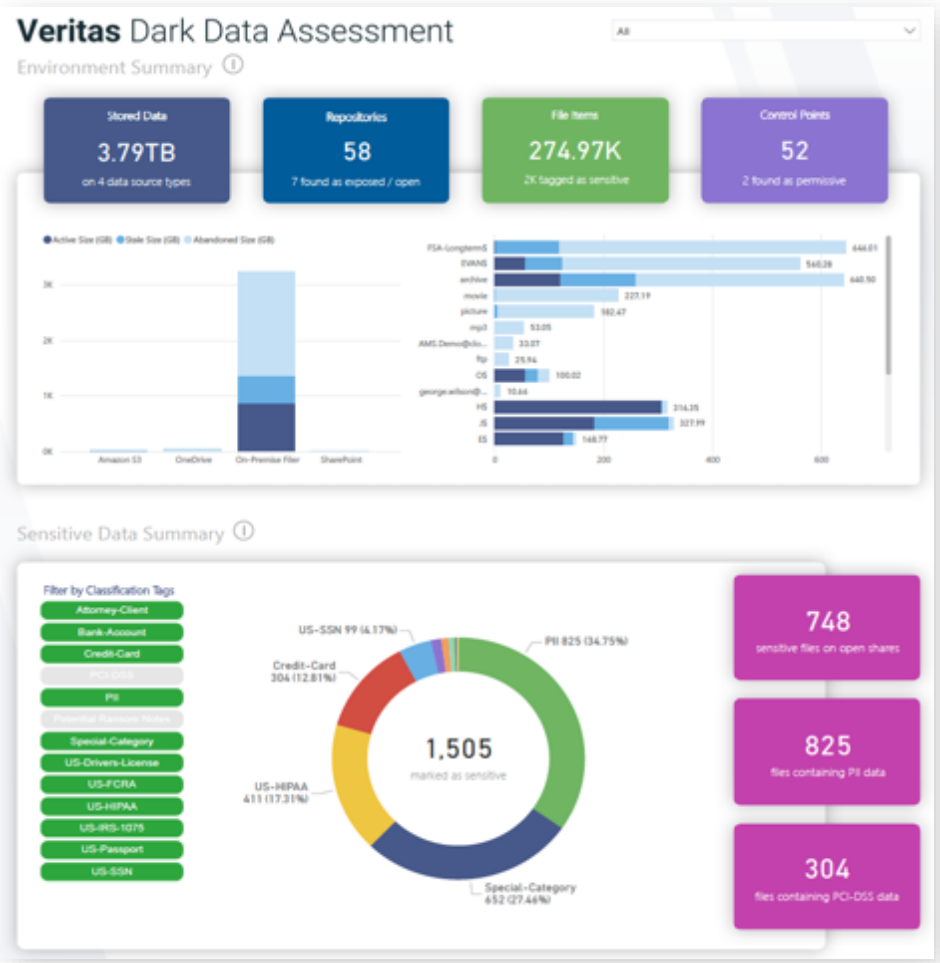
**識別暗資料：**

利用保護報告和分析來識別要歸檔或刪除的資料

**優化資料儲存：**

通過靈活和動態的儲存選擇（縱向擴展、橫向擴展、混合、雲）確保成本和性能要求滿足業務需求。

- DDA Shares and File Groups
- DDA User Group and Department Summary
- DDA PSTs Videos and Very Large Files
- DDA Disabled Users Summary
- DDA Sensitive And Permissive
- DDA M365 Summary
- DDA AmazonS3 Summary
- DDA Send Files To Classify
- DDA File Extension Summary
- DDA Sensitive File Extension Summary
- DDA Sensitive Data Aging (Last Modified and Last Accessed)
- DDA Permissive Control Point
- DDA User Activity Detail
- DDA Top 10 Activity
- DDA User Risk Score
- DDA Circular Groups
- DDA Data Aging (Last Modified and Last Accessed)
- DDA Classification Summary
- DDA Possible Duplicates
- DDA Potential Ransomware



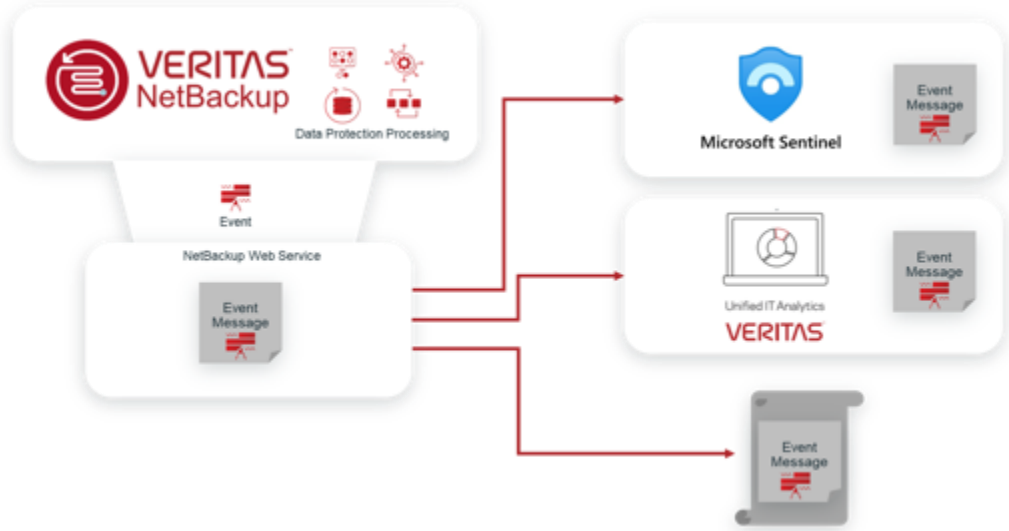
VERITAS

# 安全操作

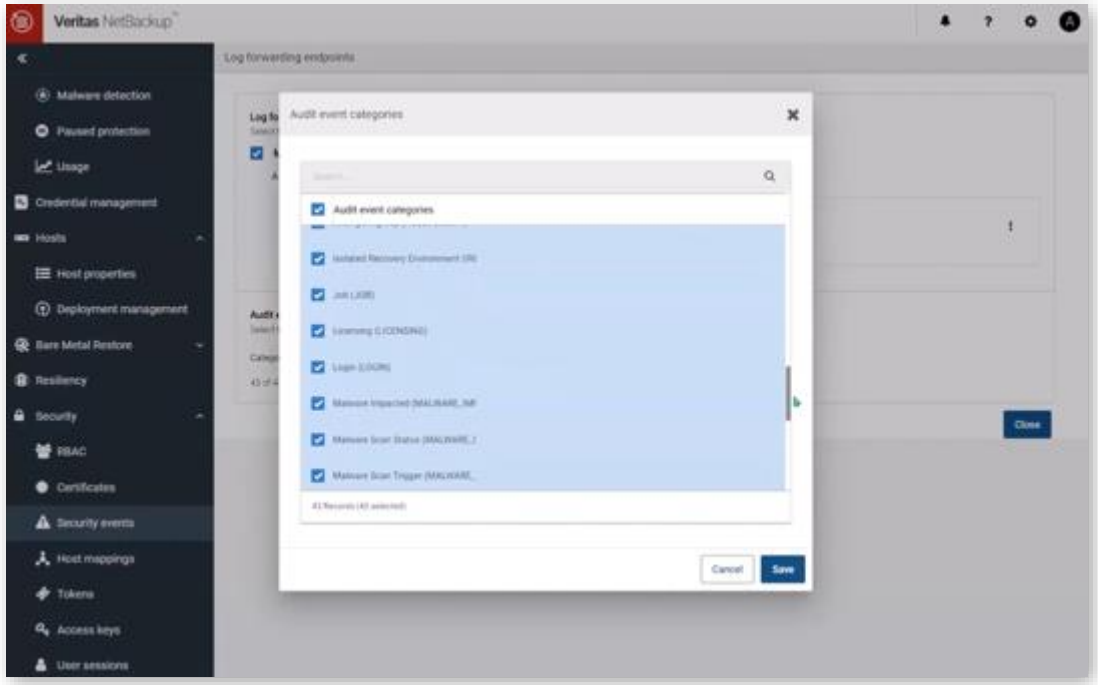


**發現異常時觸發事件回應：**

將警報轉送到 SIEM/SOAR 平臺，以觸發事件回應手冊，以針對在資料備份期間檢測到的潛在勒索軟體




Flexible SIEM/SOAR/XDR integration options with API controls







VERITAS

# Cyber Recovery 30-60-90 檢核清單

落實計劃以確保還原零失誤

90 DAYS

PHASE 3

***精煉、演練、落實***

- 調整備份政策以達成100%的備份成功率，以符合SLA要求
- 調整支援AI的異常偵測 (消除誤報false positives/negatives)
- 執行桌上模擬演習 (包含不中斷的還原演練)
- 演練還原與驗證結果




VERITAS

# 建立協同運作的恢復計劃

為災難還原和資安事件建立協同運作的恢復計劃



**運行執行腳本：**

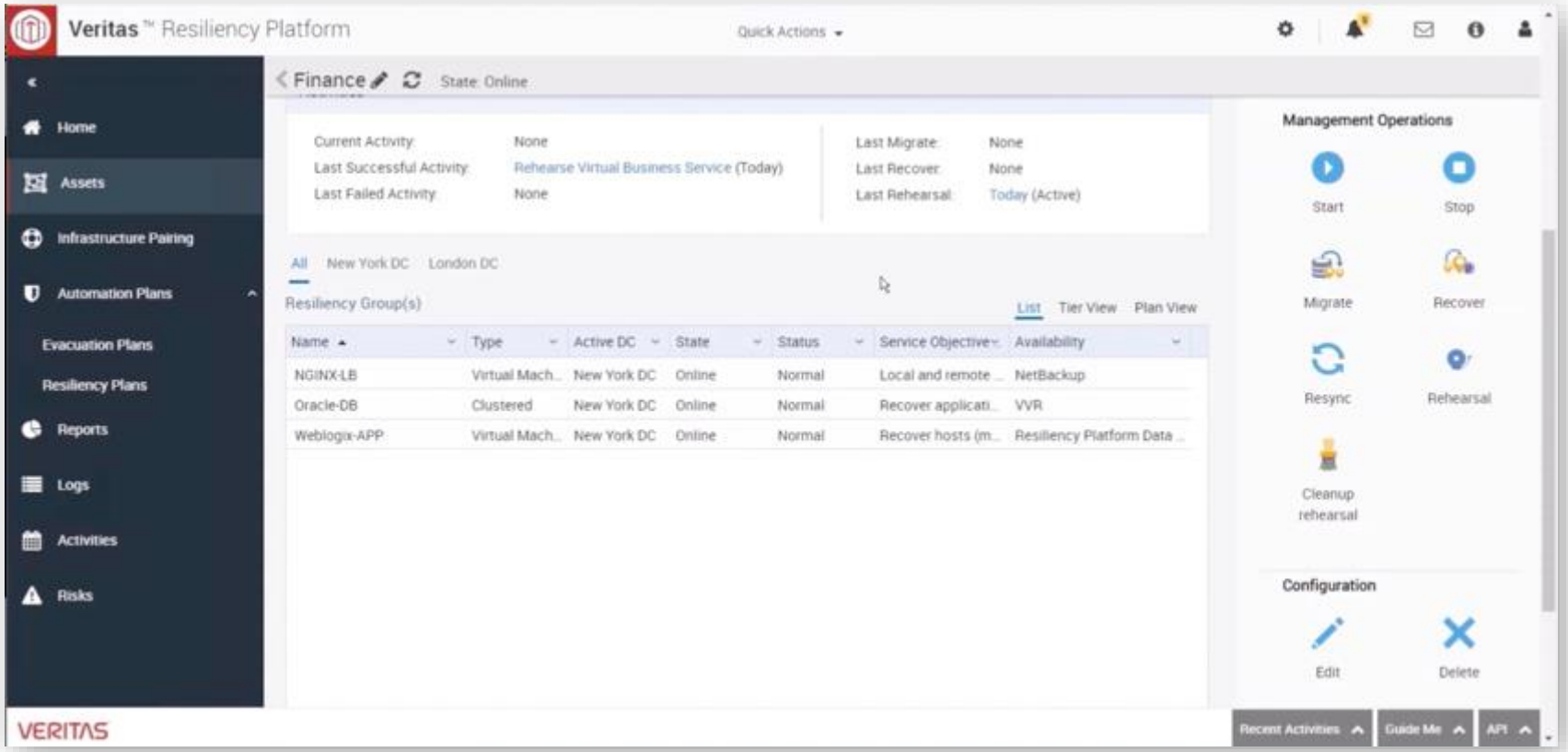
以程式設計方式定義獨特的 執行腳本/工作流，以自動執行災難和網路恢復的恢復過程和任務

**資源協同運作：**

可分配、排序和存取資源，以支援跨多個資料資源和資料目標來運行執行腳本

**整合惡意軟體掃描工具：**

惡意軟體檢測自動化







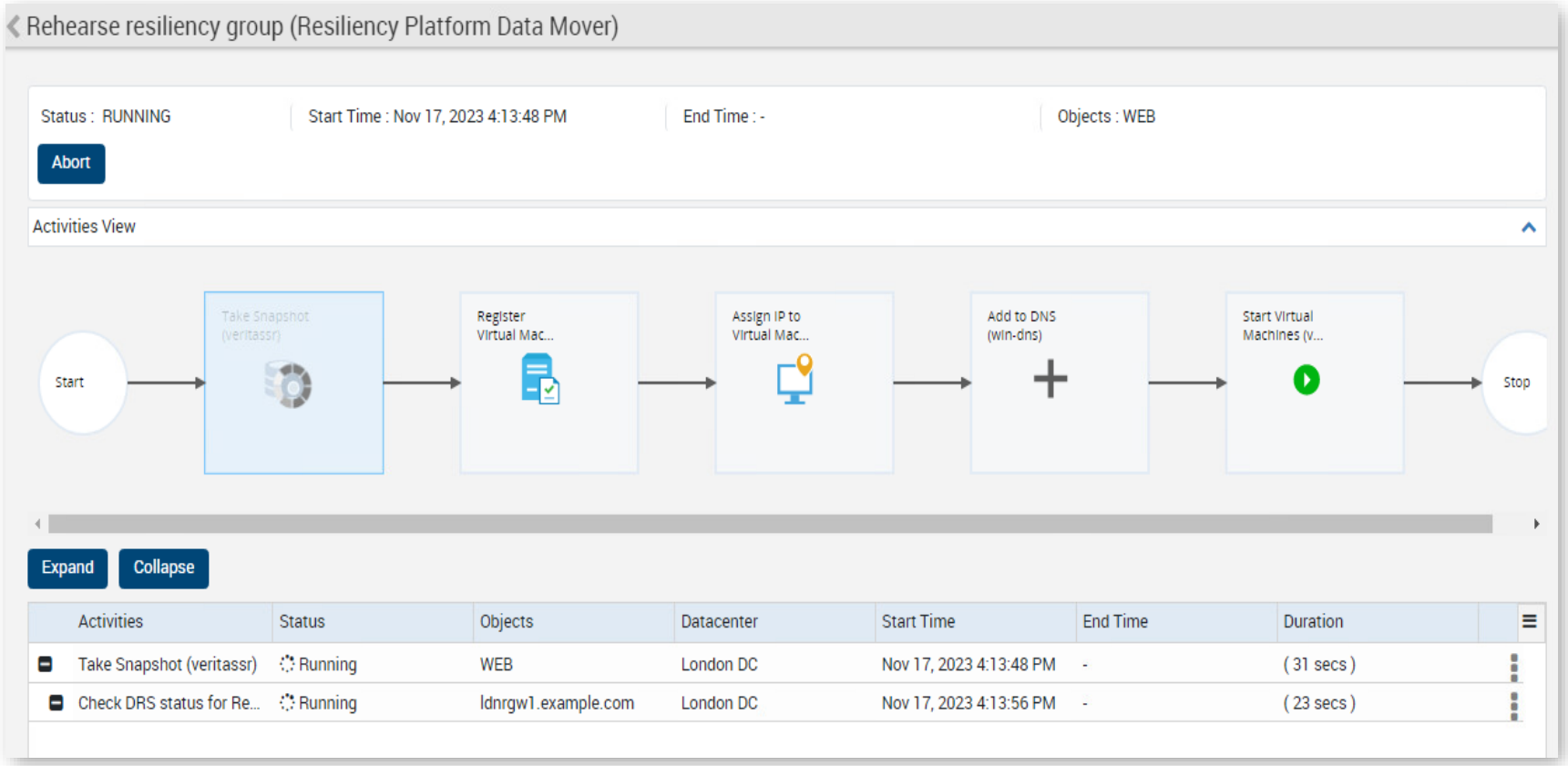
VERITAS

# 不中斷的執行腳本驗證



**運行不中斷的演練：**

可動態連接至Web、資料和應用程式資源，利用生產資料快照來驗證恢復執行腳本







VERITAS

# 了解可能的資料外洩

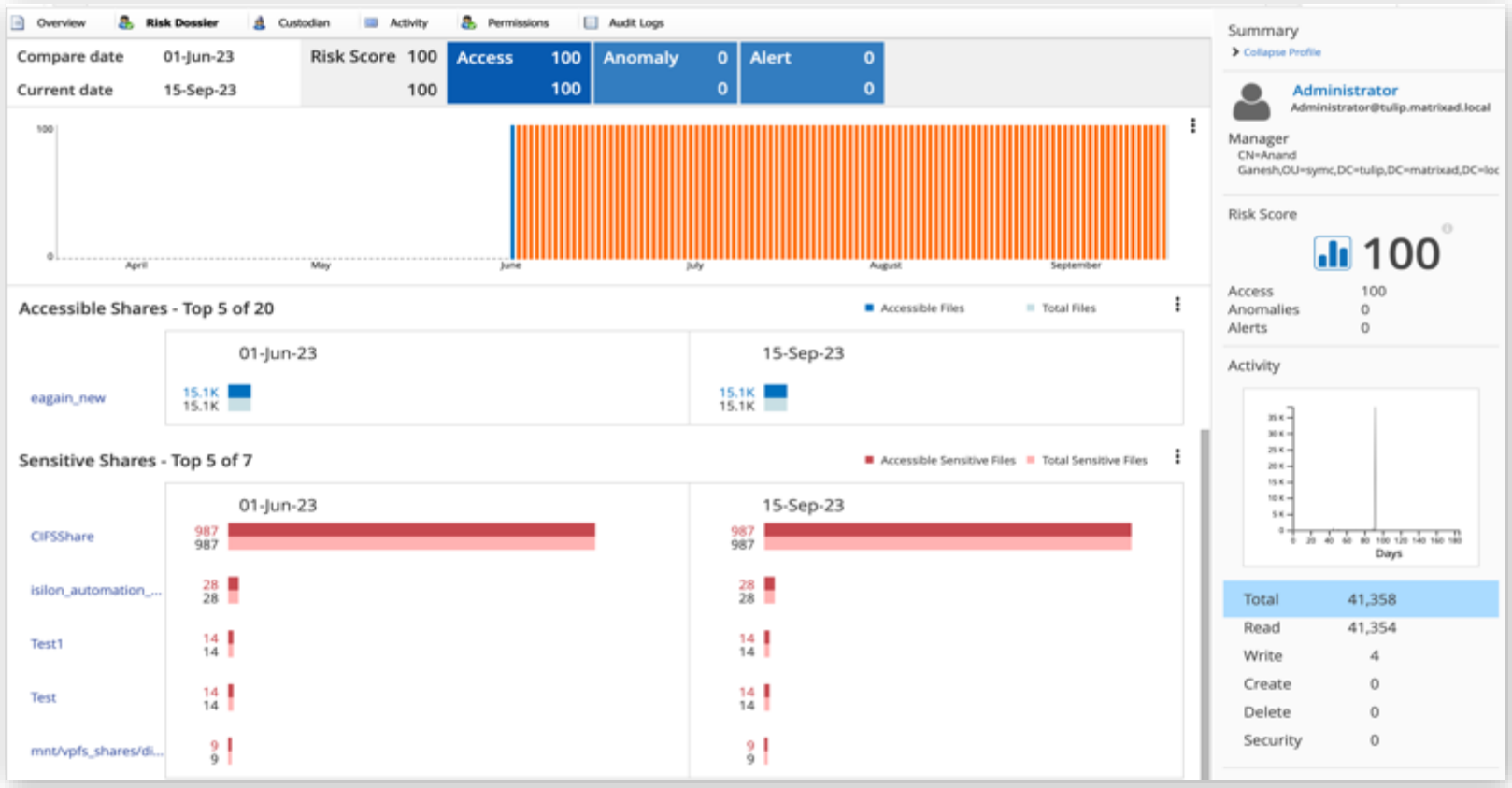


**影響分析：**

發現異常活動的資料，以確定哪些敏感資料可能受到事件的影響

**識別/調查異常的使用者行為：**

針對使用者行為發出警報，例如存取的檔案、下載的資料偏離正常活動的基線



# 對備份資料的影響

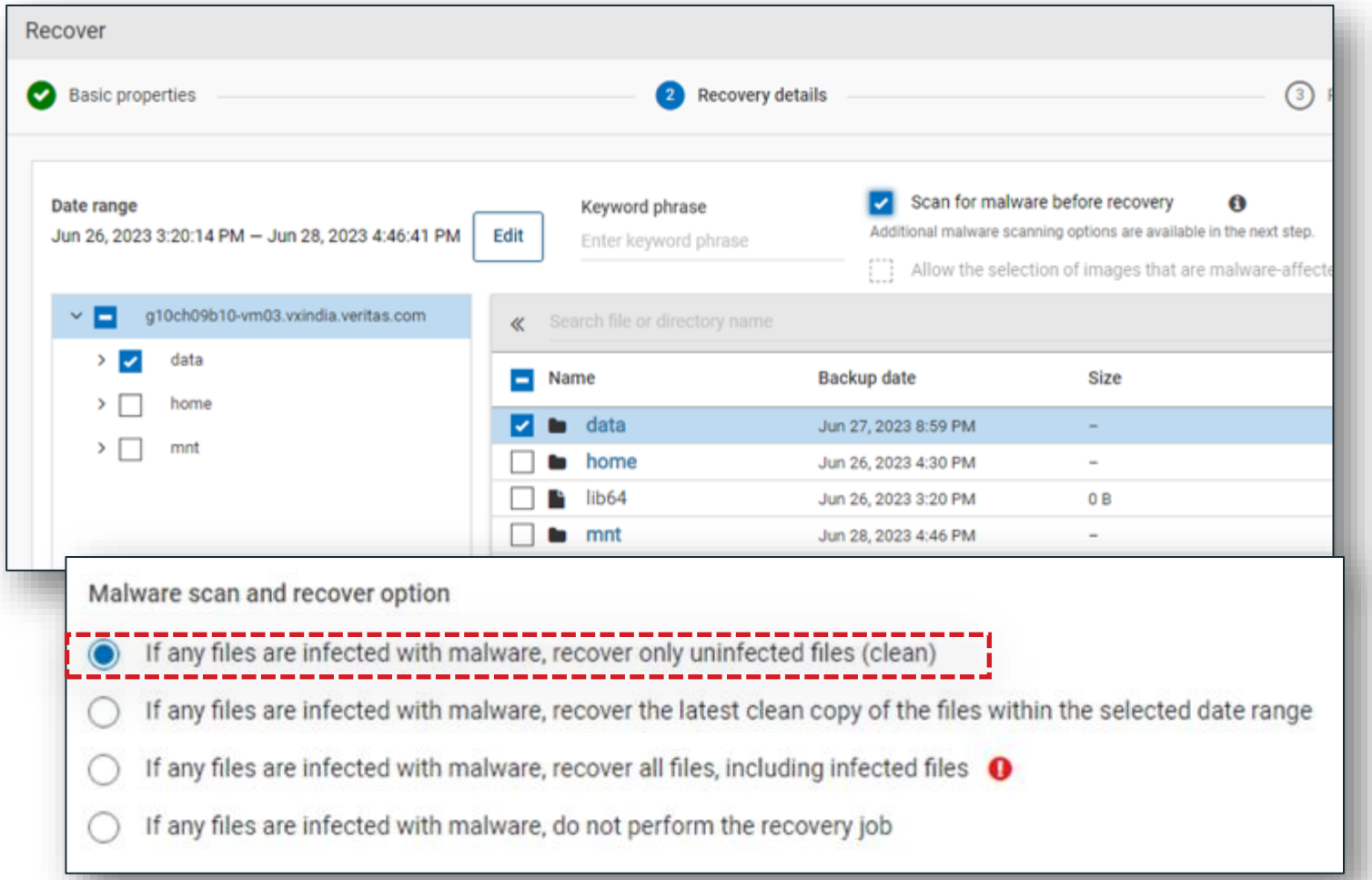


**最後已知良好的恢復點：**

通過在勒索軟體事件開始之前提供最後一個已知的良好備份點來支持取證分析

**縮時檢視：**

使用備份副本來分析和識別攻擊歷程和進展



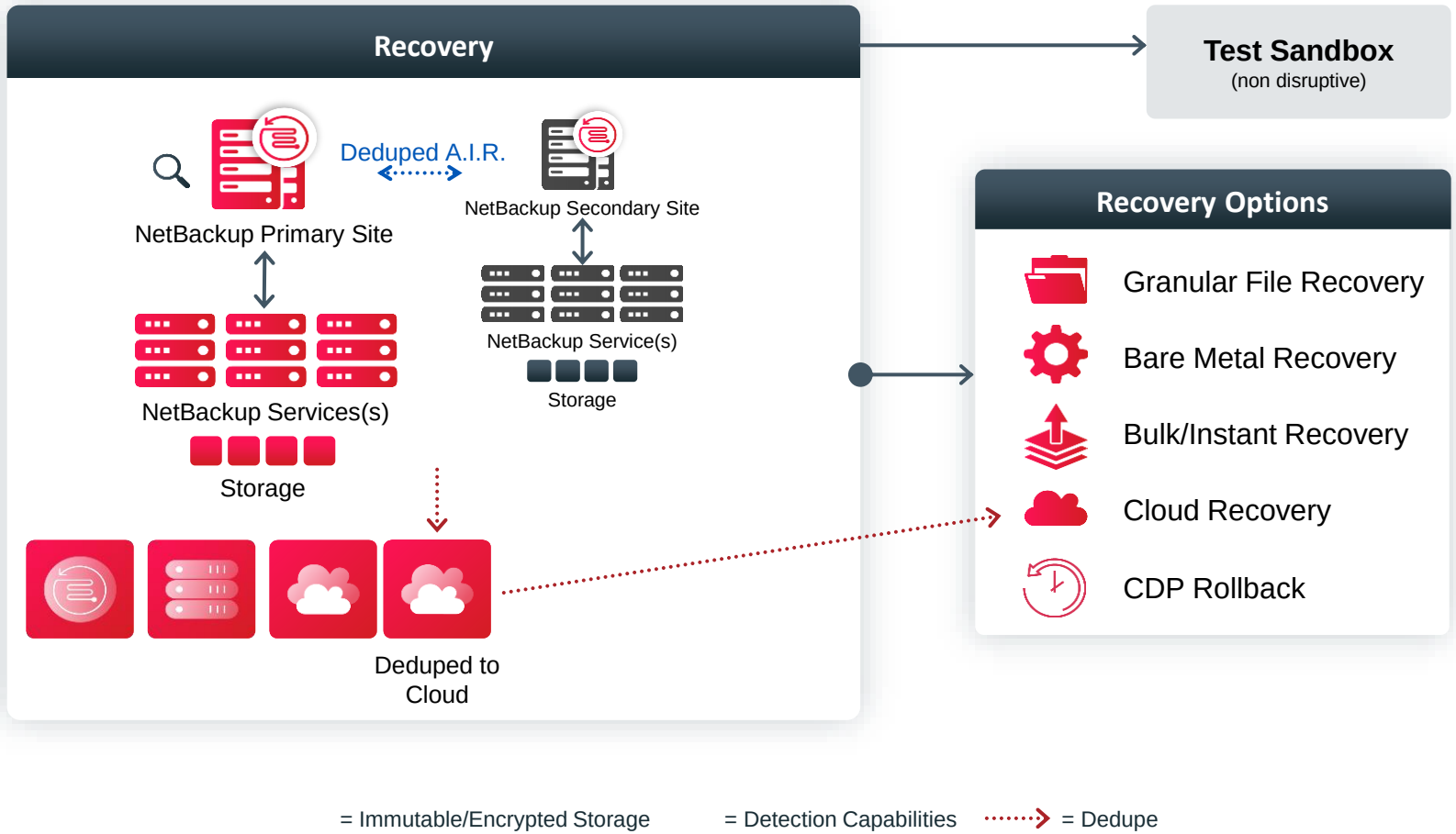
# 優先恢復關鍵應用進行網路恢復(Cyber Recovery)



**協同運作恢復：**

對關鍵業務流程進行腳本恢復，並啟動以下即時恢復：

-Files
-Files systems
-VMs
-DBs
-Cloud



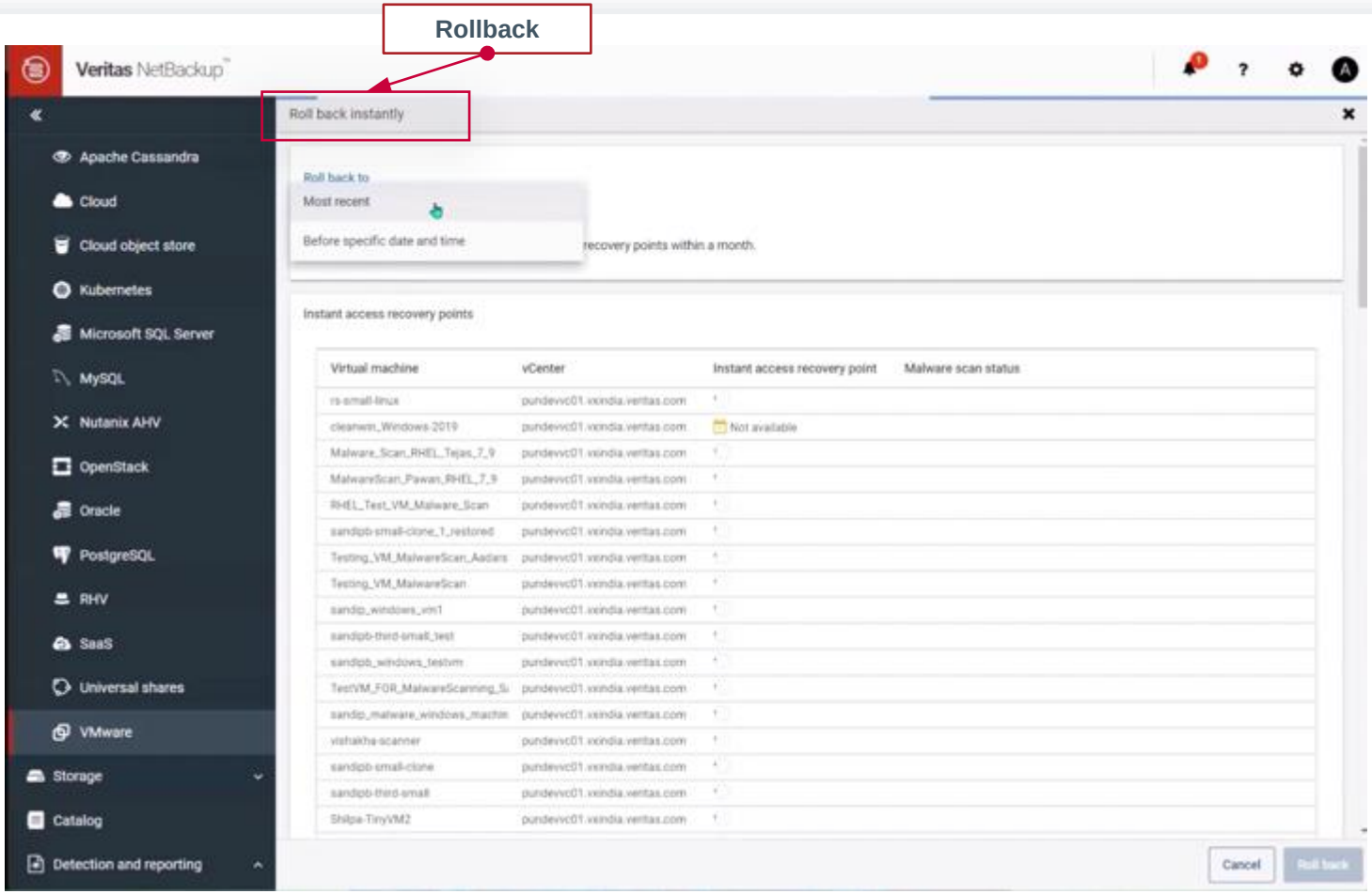
# 啟動災難還原流程



**為關鍵應用建立高可用性架構：**
使用高可用性恢復關鍵應用

**確認災難影響範圍：**
確定要利用哪些資料來源進行恢復

**啟動還原計劃：**
使用協同運作的還原配置來還原企業資料與應用



# Cyber Recovery 30-60-90 檢核清單

落實計劃以確保還原零失誤

30 DAYS | 60 DAYS | 90 DAYS

## PHASE 1

### *基礎建設*

- ❑ 針對所有工作負載建立保護與保留政策
- ❑ 使用不可變儲存
- ❑ 落實3, 2,1 備份策略 (包含一個虛擬和/或實體的Air Gap或SaaS隔離)
- ❑ 套用安全控制(例如MFA, MPA, 網路隔離, RBAC, 加密)
- ❑ 考慮使用強化過後的專屬備份一體機
- ❑ 啟用支援AI的異常分析
- ❑ 啟用惡意軟體偵測和保留規則
- ❑ 更新軟體與安全更新(持續性)

## PHASE 2

### *主動管理風險*

- ❑ 識別"遺漏"的關鍵資產
- ❑ 執行暗資料分析
- ❑ 查找與分類機敏資料
- ❑ 識別與監視高風險的使用者行為
- ❑ 建立一個隔離的還原環境(IRE或clean room)
- ❑ 建立還原執行腳本(recovery runbook)，調整操作順序
- ❑ 整合資安操作(SecOps)並建立事件回應營運手冊(playbooks) (例如SIEM / SOAR / XDR整合)

## PHASE 3

### *精煉、演練、落實*

- ❑ 調整備份政策以達成100%的備份成功率，以符合SLA要求
- ❑ 調整支援AI的異常偵測 (消除誤報false positives/negatives)
- ❑ 執行桌上模擬演習 (包含不中斷的還原演練)
- ❑ 演練還原與驗證結果




VERITAS


Thank You
VERITAS