

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



超越災難還原的韌性



從Disaster Recovery到Cyber Recovery

Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solution 2023



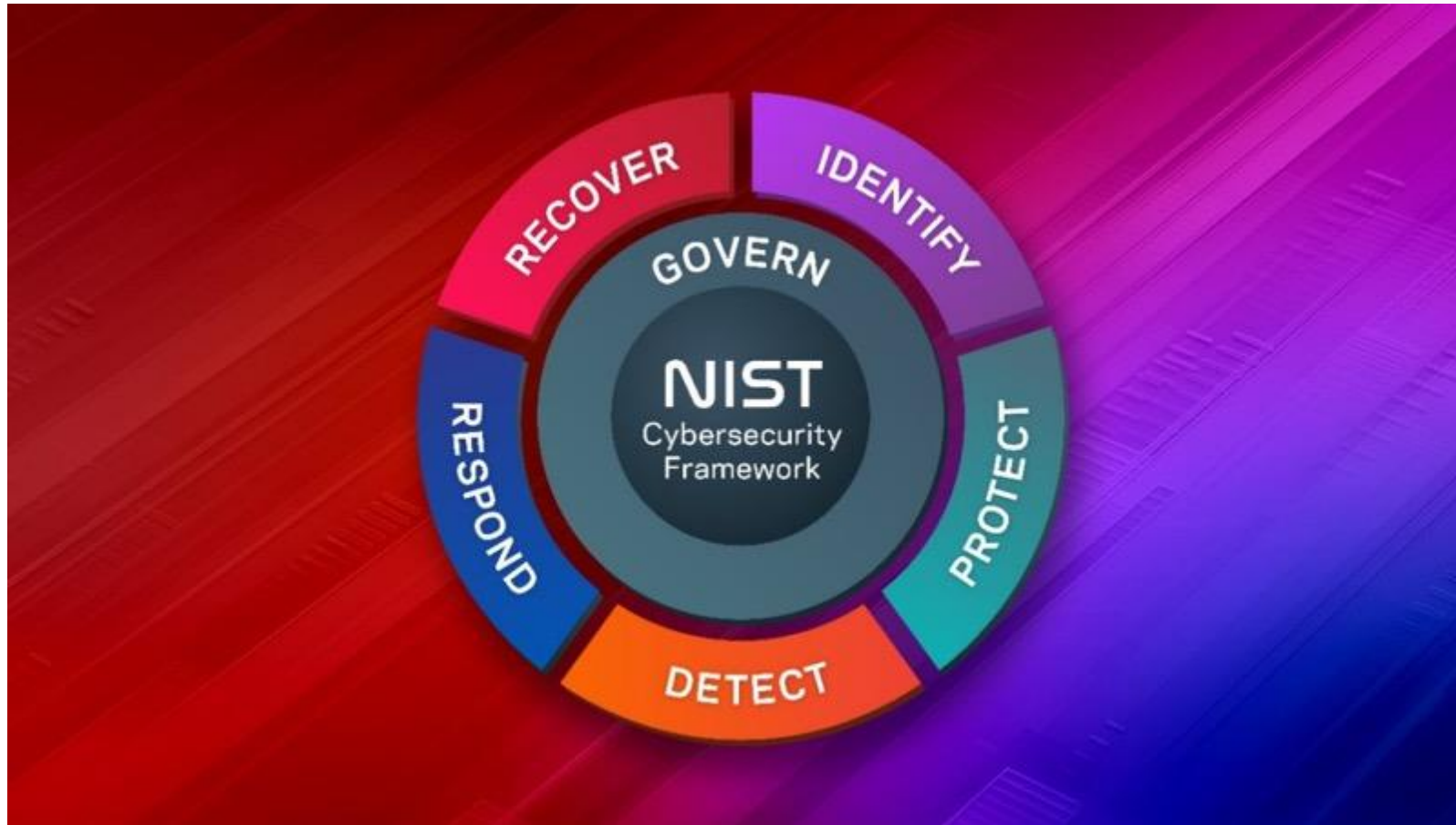
IDC: Worldwide Cyber-Recovery 2023 Vendor Assessment



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)





結合一流的方案
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 網路安全夥伴生態系統



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)

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)

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

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)



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

Sources Consecutive Failure Jul 1, 2024 4:46:03 PM

Total Rows: 12

Backup Source	Source Name	Source Type	Message	Today	Yesterday	Day 3 Status	Day 4 Status	Day 5 Status	Day 6 Status	Day 7 Status	Day 8 Status	Day 9 Status	Day 10 Status	Day 11 Status	Day 12 Status	Day 13 Status	Day 14 Status
17000000	17000000	File	Failed Backup Since Last 14 days	No Backup	Failed	Failed	Failed	Failed	No Backup	No Backup	Failed	Failed	Failed	No Backup	No Backup	No Backup	No Backup
17000001	17000001	File	Failed Backup Since Last 14 days	No Backup	Failed	Failed	Failed	Failed	No Backup	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed
17000002	17000002	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000003	17000003	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000004	17000004	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000005	17000005	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000006	17000006	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000007	17000007	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000008	17000008	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000009	17000009	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000010	17000010	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000011	17000011	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
17000012	17000012	File	Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup

Veritas Alta™ View

← Reports

Home

My Shared

My Reports

Alerts

System Administration Reports

Backup Manager

Demo

My Reports / Demo

Run Copy Cut Delete Share Export

☒ Name

☒ List of backup jobs that failed in the last 24 hours

List of backup jobs that failed in the last 24 hours

List of backup jobs that failed in the last 24 hours

https://www.veritas.com/support/en_US/doc/160799157-164196584-qv156688906-164196584

Alta Copilot

如何用最簡單的NetBackup建立隔離環境

Creating an Isolated Environment using NetBackup

To create an isolated recovery environment (IRE) using the software version of NetBackup, follow these steps.¹²³⁴⁵

1. Log in to the NetBackup BYO media server as a local administrator
2. Run the command `/usr/openw/pdbs/shell/bin/show_slp_windows` to view the SLP windows for replication from the primary server to the MSDP storage on the media server
3. Configure the subnets and IP addresses that are allowed to access the media server by running the command `/usr/openw/pdbs/shell/bin/ire_network_control allow-subnets --subnets CSR subnets or IP addresses`
4. Set the daily air gap schedule by running the command `/usr/openw/pdbs/shell/bin/ire_network_control set-schedule --start-time time --duration duration --weekday 0-6`
5. Ensure that the SLP replication window on the production domain is configured to be open at the same time as the IRE schedule
6. If you want to use the isolated recovery environment on a SUSE Linux Enterprise Server NetBackup 10
7. Perform additional configuration steps specific to your environment, such as setting SLP lifecycle parameters, adding trusted masters, updating remote primary server versions, and deploying Hovos certificates

Note: The specific steps may vary depending on your NetBackup version and operating system.¹²³

Citations

1. NetBackup and Veritas Appliances Hardening Guide - Configuring an isolated recovery environment on a NetBackup BYO media server [Version: 10.3, 10.2, 9.3, 5.1.1, 4.0, 3.0] [\[Link\]](#)
2. NetBackup® Release Notes - Isolated recovery environment is supported on SUSE Linux Enterprise Server NetBackup BYO [Version: 10.3.0.1] [\[Link\]](#)
3. Veritas Solution Guide for Sheltered Harbor - Configuration of Isolated Recovery Environment (IRE) [Version: 10.3, 10.2] [\[Link\]](#)

Type your message



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：

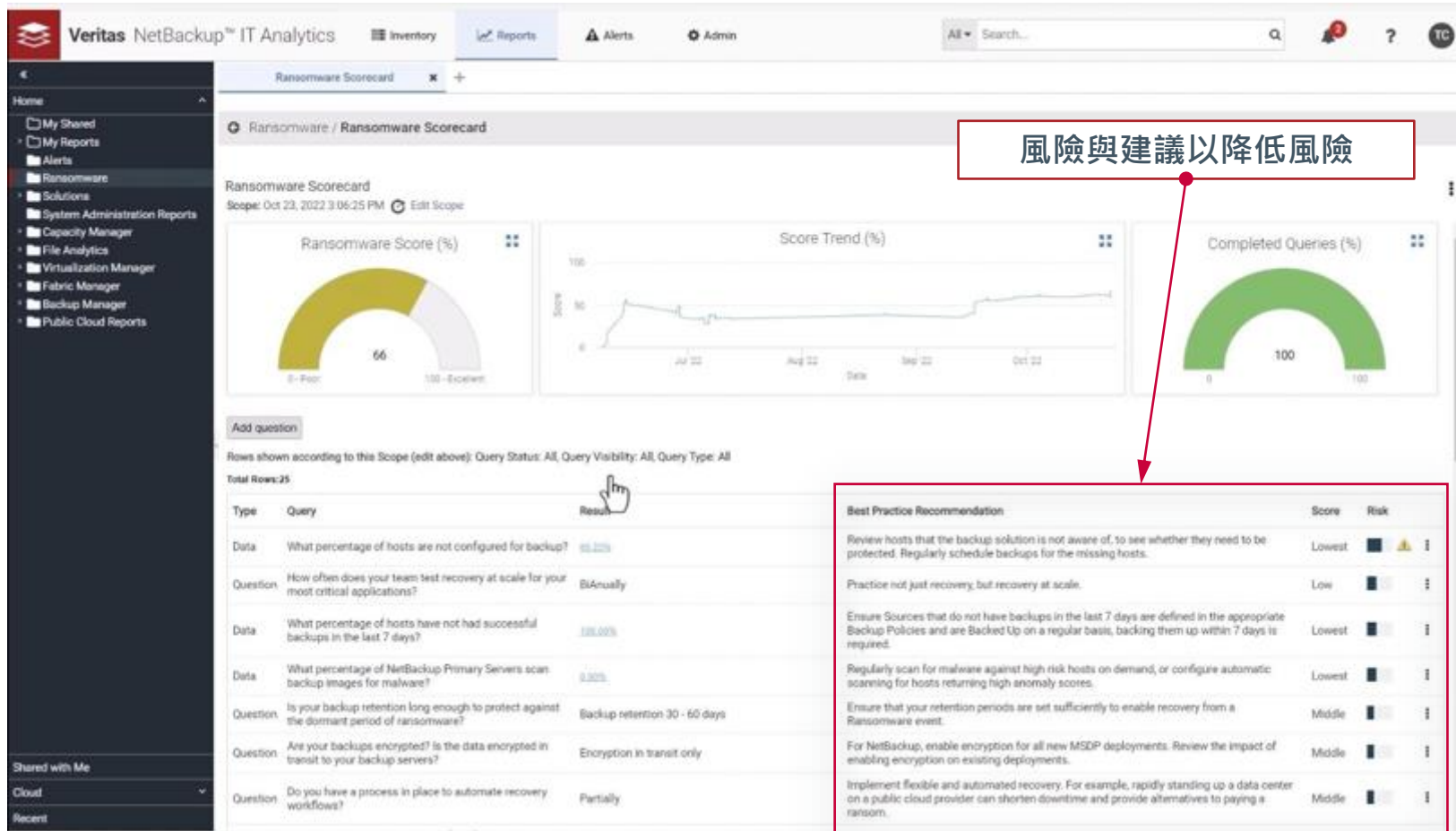
依據標準或客製的KPI(例如備份成功率)，來識別勒索軟體防護狀態是否存在風險

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



風險與建議以降低風險



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):

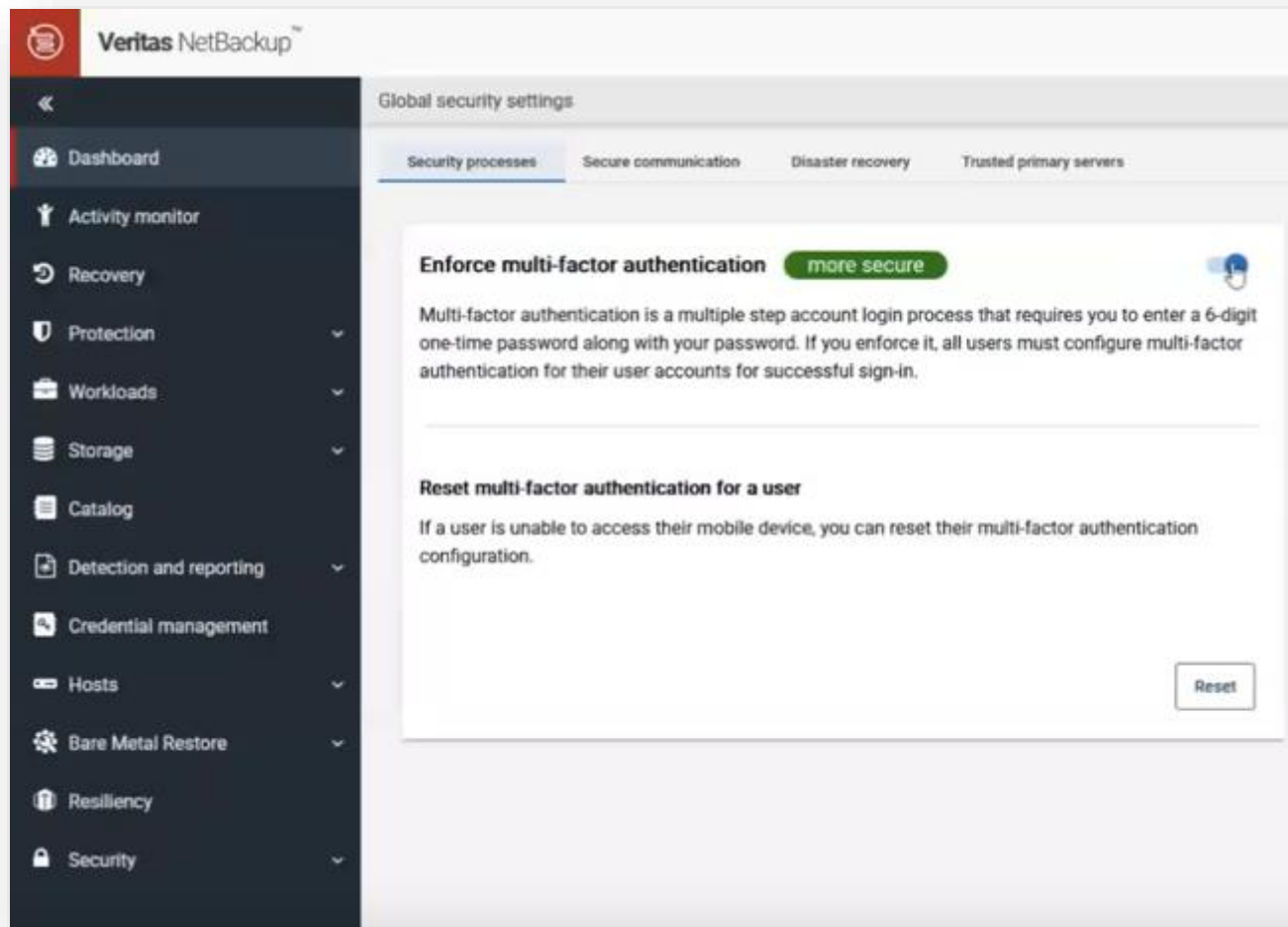
通過要求 2 人或更多人批准更改和存取權限，防止單方面更改和設置，例如將備份刪除、過期和 root 存取權限

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。





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：

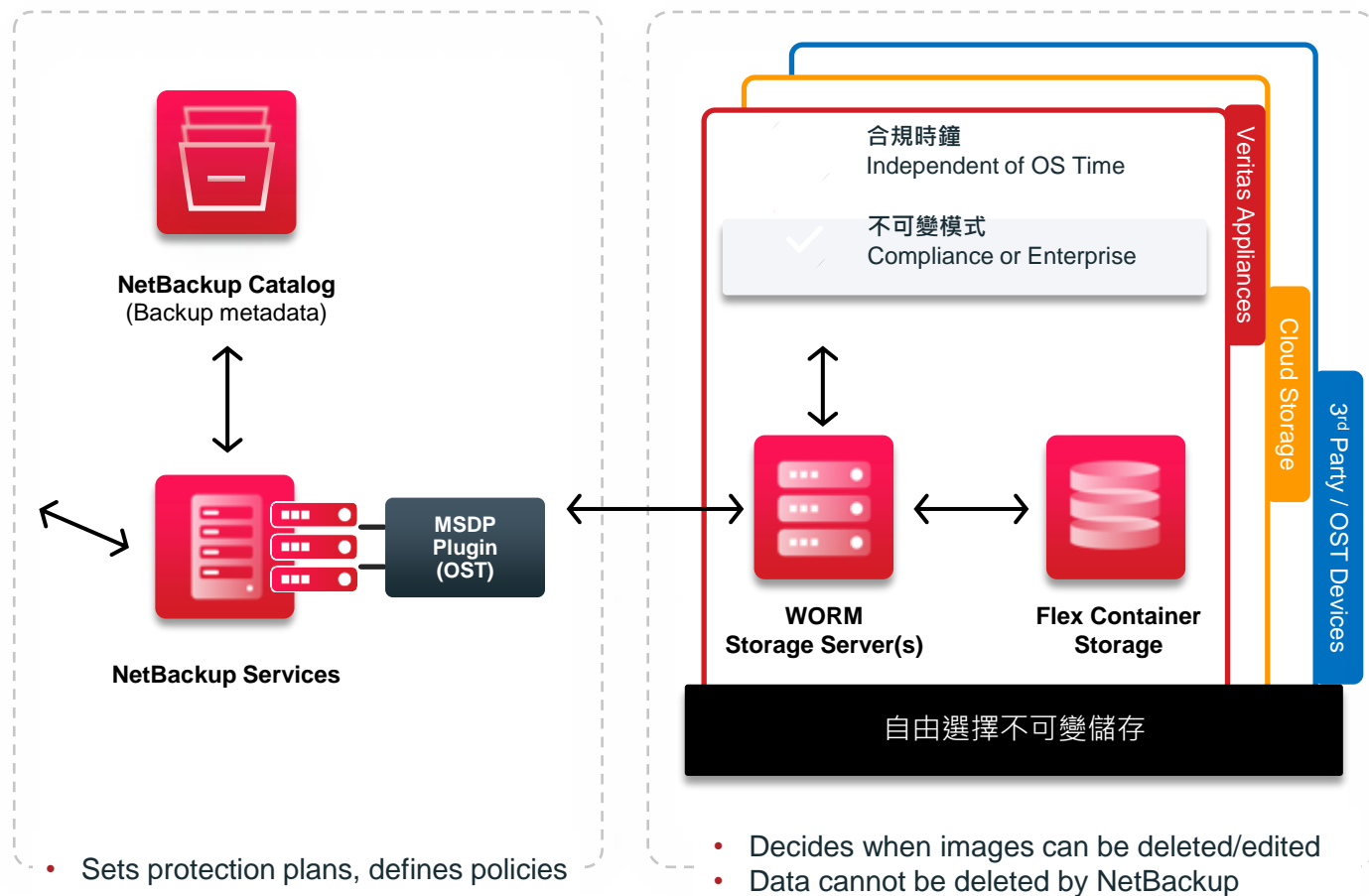
以Galois/Counter Mode (GCM) AES-256 bit落實 NIST AES 256 加密演算，防止未經授權的資料存取

資料傳輸加密：

利用TLS 1.3加密，以防止網路竊聽



Client Source Data (Objects)





依3-2-1原則設計的 完整隔離

單一政策

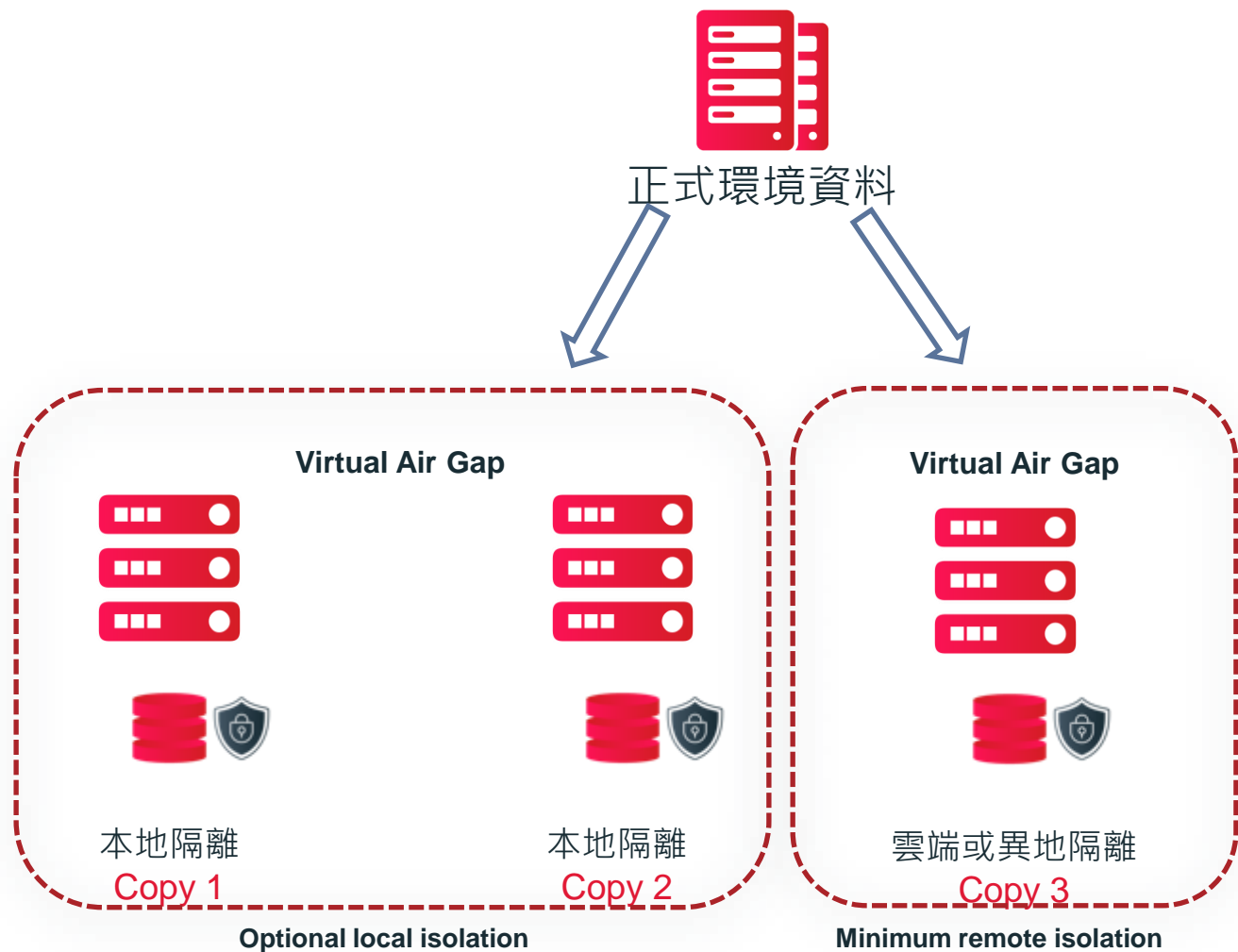
3 份複本

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





PREVENT DATA DESTRUCTION — ISOLATE

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：

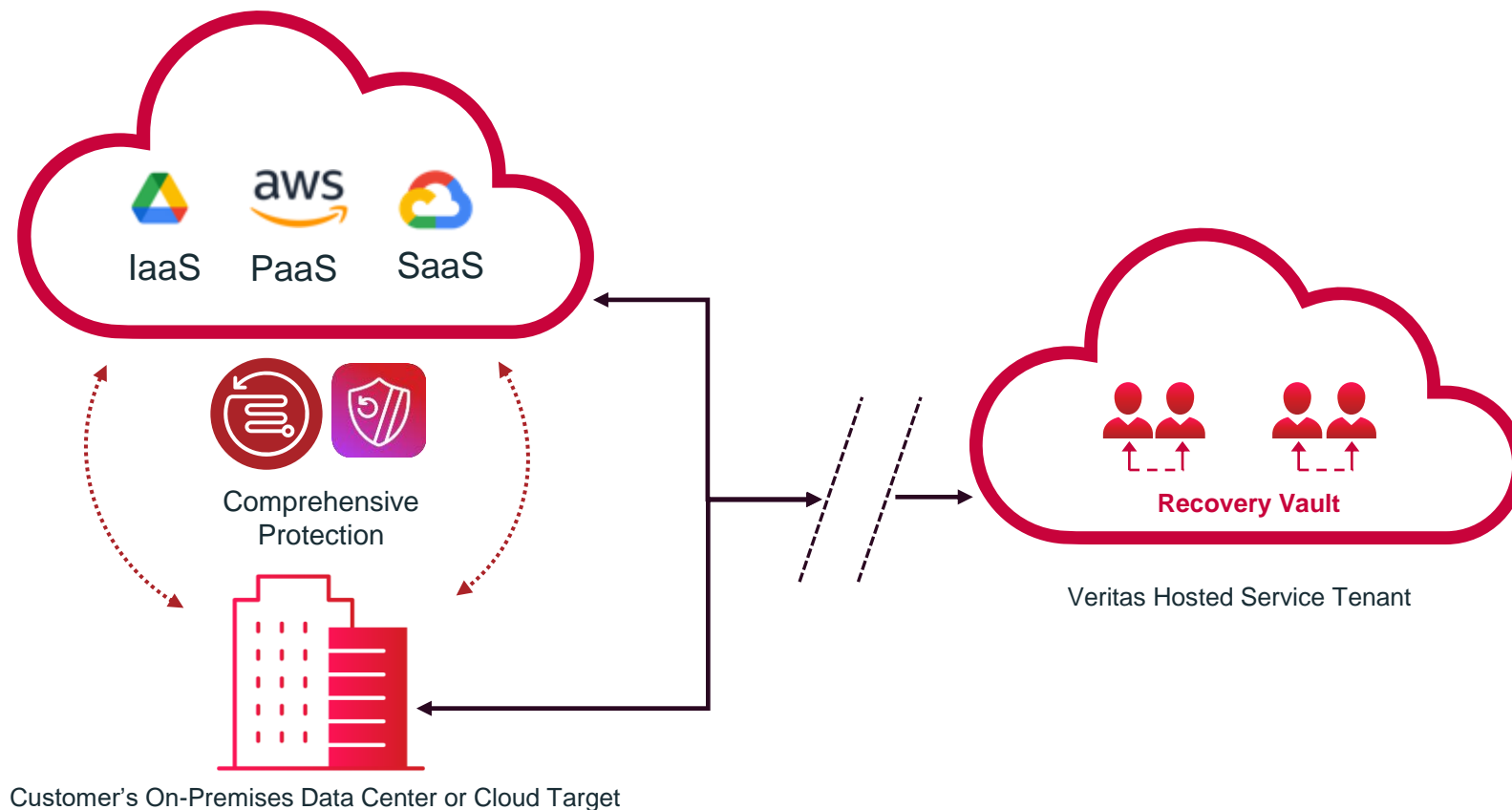
全託管資料隔離服務（SaaS）
到雲端

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



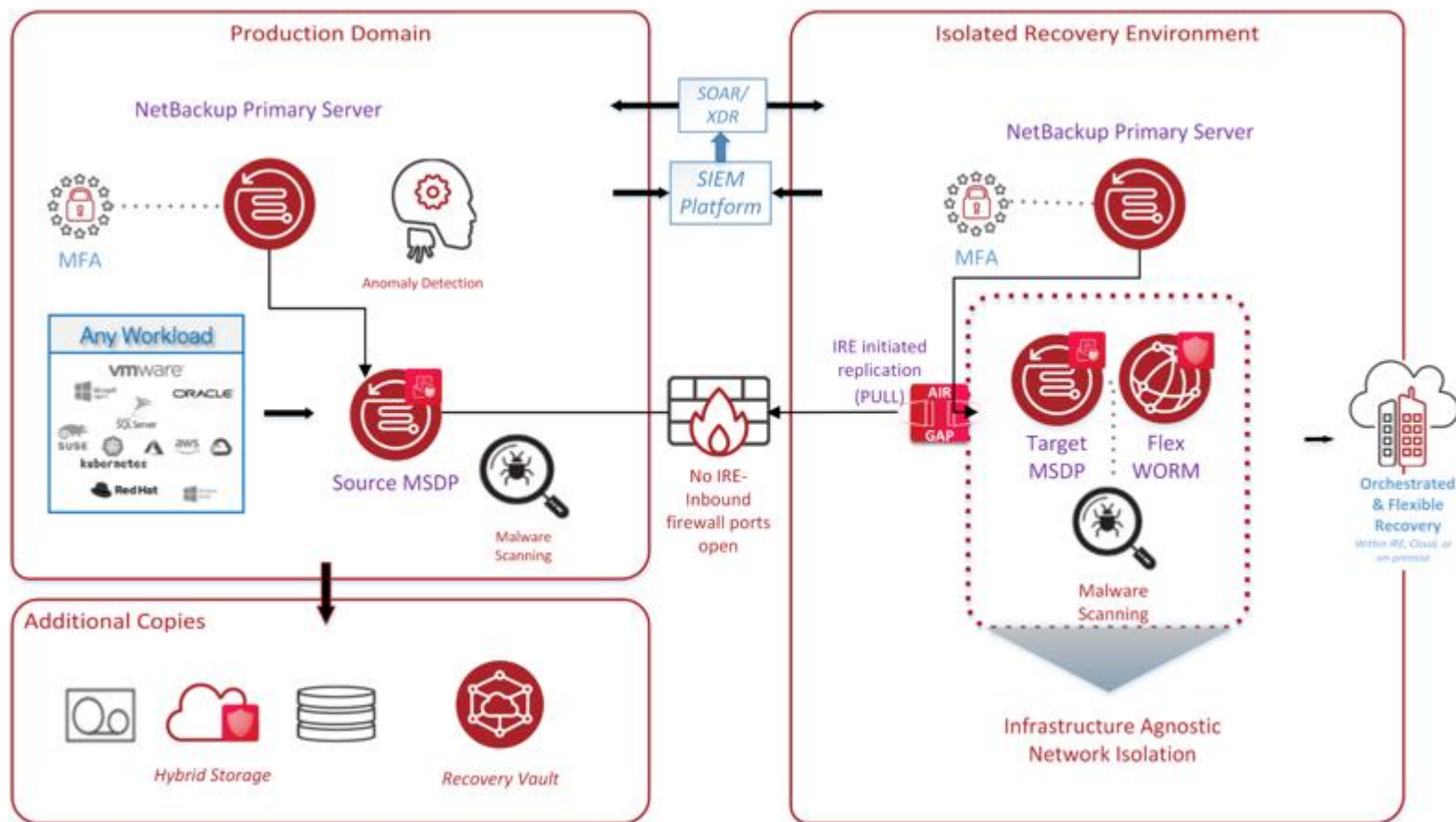


本地隔離：

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



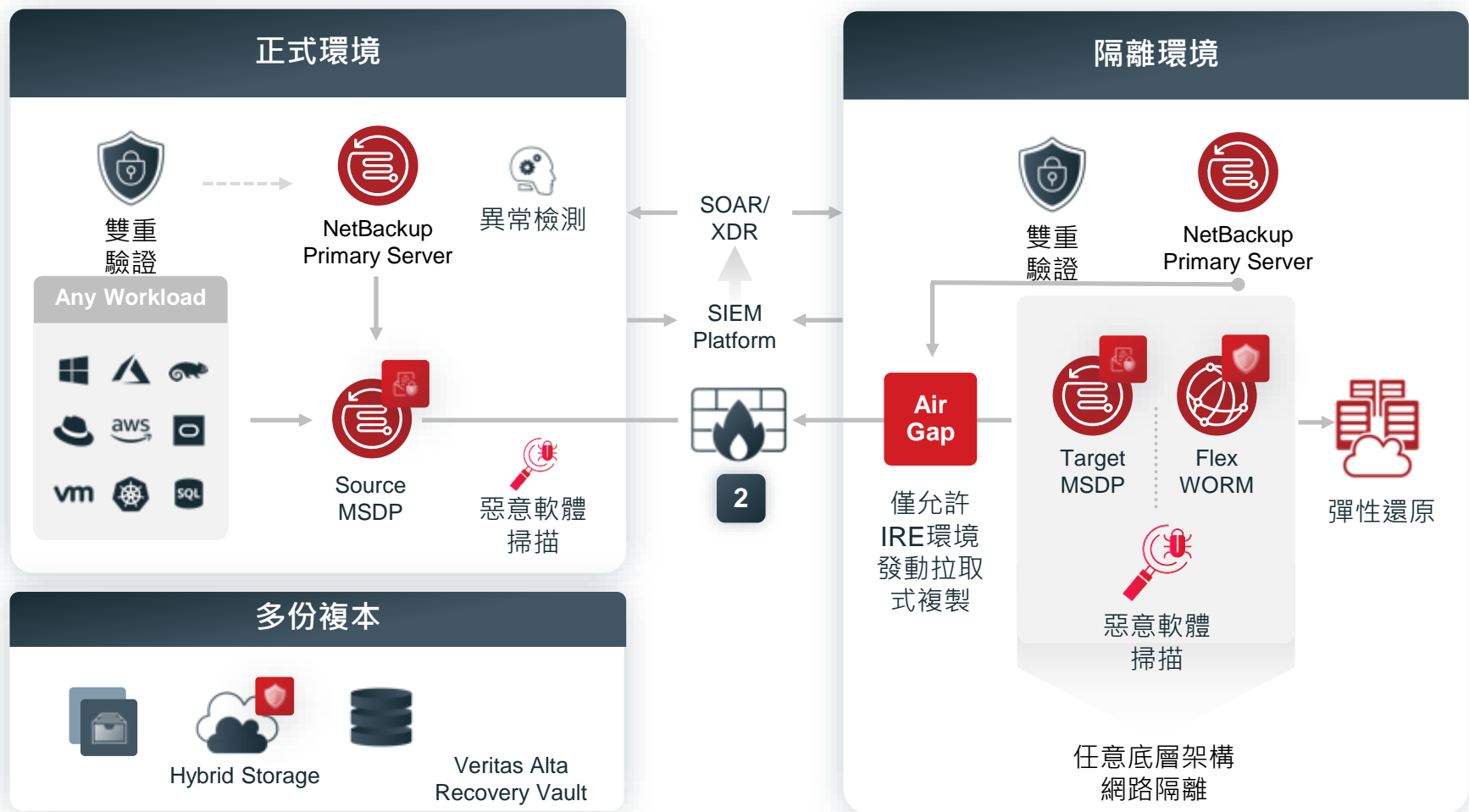


地端隔離：建立單向拉取式的隔離環境

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





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

Anomaly details

Backup id
dl360g10-plus-v44.vxindia.veritas.com_1689090890

Client name
dl360g10-plus-v44.vxindia.veritas.com

Details
Anomaly detection extension 'nuksus' for Ransomware is detected for job ID : 28

Ransomware extension
nuksus

>	<input type="checkbox"/>	E64726C0-2003-11EE-9D03-859D6	Ransomware Extension Detection	High	Anomaly detection extension 'Ranc	Jul 11, 2023 9:29 PM	Not reviewed	⋮
>	<input type="checkbox"/>	DE0ED638-2003-11EE-92DD-FBB0E	Login attempts from un-usual IP at	Medium	Detects if there are login attempts	Jul 11, 2023 9:29 PM	Not reviewed	⋮
>	<input type="checkbox"/>	785BD0F8-2002-11EE-B31B-97E70	Login attempts from un-usual IP at	Medium	Detects if there are login attempts	Jul 11, 2023 9:19 PM	Not reviewed	⋮
>	<input type="checkbox"/>	12C43F60-2001-11EE-B22A-6E6E6	Login attempts from un-usual IP at	Medium	Detects if there are login attempts	Jul 11, 2023 9:09 PM	Not reviewed	⋮
>	<input type="checkbox"/>	AD8D5E8E-1FFF-11EE-8A26-29F21	Login attempts from un-usual IP at	Medium	Detects if there are login attempts	Jul 11, 2023 8:59 PM	Not reviewed	⋮

Anomaly detection

Backup anomalies

System anomalies

Search...

<input type="checkbox"/>	Anomaly ID	Anomaly type	Severity	Description	
▼	<input type="checkbox"/>	89243E2C-3112-11EE-93BC-9EB4C	Multiple policies deletion by user	Medium	Detects if multiple policies gets
	Anomaly ID	Anomaly type	Review status		
	89243E2C-3112-11EE-93BC-9EB4CC24F943	Multiple policies deletion by user	Not reviewed		

Anomaly details

Current count
2

Expected count
1

Rule description
Detects if multiple policies gets deleted in given time frame.



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。

The screenshot shows the Veritas NetBackup Malware detection interface. On the left is a dark sidebar with navigation options: Dashboard, Activity monitor, Recovery, Protection (expanded), Protection plans, Policies, Workloads, Storage, Catalog, Detection and reporting (expanded), Anomaly detection, Malware detection (selected), Paused protection, Usage, Credential management, and Hosts. The main panel is titled 'Malware detection' and contains a table of scan results. Below the table is a 'Malware scan and recover option' dialog box with four radio button options.

Display name	Date of scan	Scan status	Files infect...	Backup ID	Client
	April 19, 2023 6:2	Infected	47	r7515-097-vm06.vxindia.veritas.com_1681900022	r7515-097-vm06.vxindia.veritas.cc
TestVM_FOR_MalwareScanning	April 19, 2023 6:3	Infected	47	503ba947-d3a7-6e89-11f6-7b96d05a1d32_1681899937	503ba947-d3a7-6e89-11f6-7b96d0
	April 19, 2023 6:4	Infected	25	10.221.111.69@cluster-r7515-088v06_1681900491	10.221.111.69@cluster-r7515-088
	April 21, 2023 12:	Not infected	0	r7515-097-vm06.vxindia.veritas.com_1682094466	r7515-097-vm06.vxindia.veritas.cc
	April 22, 2023 6:4	Infected	47	r7515-097-vm06.vxindia.veritas.com_1681900022	r7515-097-vm06.vxindia.veritas.cc
	April 22, 2023 8:1	Not infected	0	r7515-097-vm06.vxindia.veritas.com_1682208000	r7515-097-vm06.vxindia.veritas.cc

Malware scan and recover option

- ☒ If any files are infected with malware, recover only uninfected files (clean)
- ☐ If any files are infected with malware, recover the latest clean copy of the files within the selected date range
- ☐ If any files are infected with malware, recover all files, including infected files
- ☐ If any files are infected with malware, do not perform the recovery job

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)



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

The screenshot displays the Veritas Information Classifier Policies interface. The main table lists various policies, including medical diagnosis policies, U.S. regulations (CMIA, DEA, HIPAA), COVID-19 related policies, and international regulations. The 'U.S. Health Insurance Portability and Accountability Act (HIPAA) Policy' is highlighted. An inset window shows the detailed configuration for the 'Credit Card' policy, which is enabled and tagged as 'Credit Card'. It lists conditions and a test for matching credit card numbers. A dropdown menu for 'Personally Identifiable Information' is open, showing a list of country-specific policies, with 'Germany Personal Data Policy' selected. The text 'PII detection for most countries' is visible below the dropdown.

Name	Status	Tags
Medical Diagnosis - Irritable Bowel Syndrome (IBS) Policy	Disabled	ICD-10-K58
Medical Diagnosis - Kidney Stone Policy	Disabled	ICD-10-N20.0
Medical Diagnosis - Leukemia Policy	Disabled	ICD-10-C90, ICD-10-C91, ICD-10-C92
Medical Diagnosis - Lung Cancer Policy	Disabled	ICD-10-C80.0
Medical Diagnosis - Lupus Policy	Disabled	ICD-10-L93
Medical Diagnosis - Lyme Disease Policy	Disabled	ICD-10-A69.2
Medical Diagnosis - Menopause Policy	Disabled	ICD-10-N95, ICD-10-Z78.0, ICD-10-Z79.0
Medical Diagnosis - Mononucleosis Policy	Disabled	ICD-10-B27
Medical Diagnosis - Ovarian Cancer Policy	Disabled	ICD-10-C25.0
Medical Diagnosis - Stomach Ulcer Policy	Disabled	ICD-10-K25.9
Medical Record Number Policy	Disabled	Medical Record
U.S. California Confidentiality of Medical Information Act (CMIA) Policy	Disabled	US-CA-CMIA
U.S. Drug Enforcement Agency (DEA) Number Policy	Disabled	US-DEA
U.S. Health Insurance Portability and Accountability Act (HIPAA) Policy	Disabled	US-HIPAA
US-COVID-19	Disabled	COVID-19
US-COVID-19 ICD-10-CM Diagnosis Indexes (CDC Feb-Apr-2020)	Disabled	COVID-19-ICD-10-CM
US-COVID-19 ICD-10-CM Diagnosis Indexes possibly leading to COVID-19 (CDC Feb-Apr-2020)	Disabled	COVID-19-Possible
US-COVID-19 ICD-10-CM Exposure Diagnosis Index (CDC Feb-Apr-2020)	Disabled	COVID-19-Exposure
US-COVID-19 ICD-10-CM Ruled Out Diagnosis Index (CDC Feb-Apr-2020)	Disabled	COVID-19-Ruled-Out
US-COVID-19 ICD-10-CM Signs and Symptoms Diagnosis Indexes (CDC Feb-Apr-2020)	Disabled	COVID-19-Symptoms
International Regulations		
Language Detection		
Personally Identifiable Information		
Special Category Data		
Transparent		

Credit Card

Name: Credit Card

Description: From Very Low confidence to Very High confidence

Status: Enabled

Tags: Credit Card

Conditions: All of

Test: Drag & drop a file here, or browse to select. Include text in images

Content matches Credit Card Number (with very low to very high confidence)

Personally Identifiable Information

- ☐ Argentina Personal Data Policy
- ☐ Australia Personal Data Policy
- ☐ Austria Personal Data Policy
- ☐ Belgium Personal Data Policy
- ☐ Brazil Personal Data Policy
- ☐ Bulgaria Personal Data Policy
- ☐ Canada Personal Data (PIPEDA) Policy
- ☐ China Personal Data Policy
- ☐ Croatia Personal Data Policy
- ☐ Cyprus Personal Data Policy
- ☐ Czech Republic Personal Data Policy
- ☐ Denmark Personal Data Policy
- ☐ Estonia Personal Data Policy
- ☐ Finland Personal Data Policy
- ☐ France Personal Data Policy
- ☒ Germany Personal Data Policy

PII detection for most countries



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：

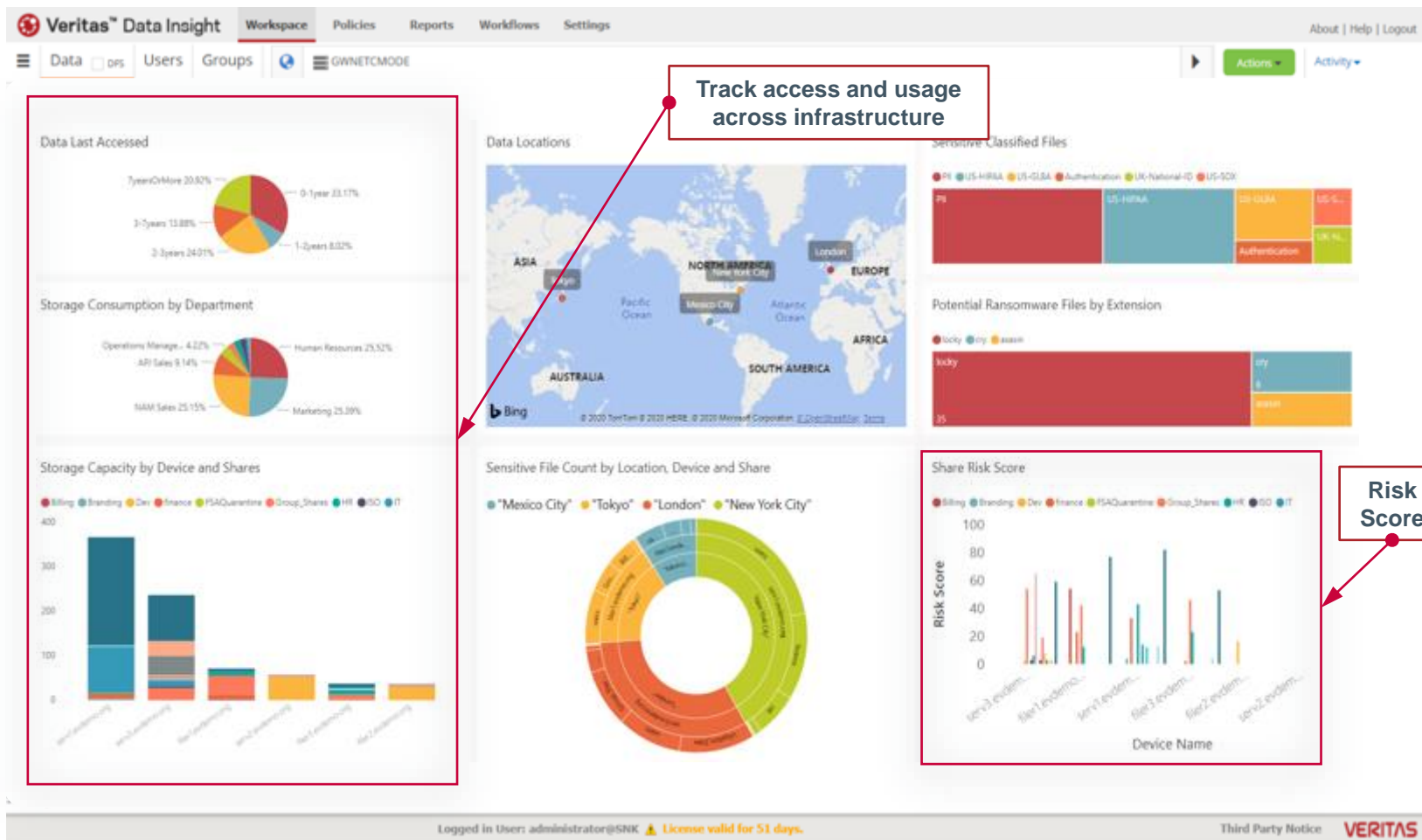
根據用戶風險和資料敏感度為異常使用者存取建立警報

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





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

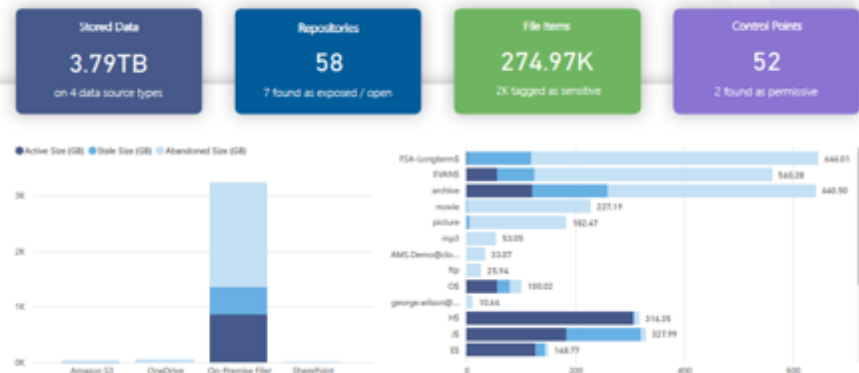
優化資料儲存：

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。

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

Veritas Dark Data Assessment

Environment Summary ①



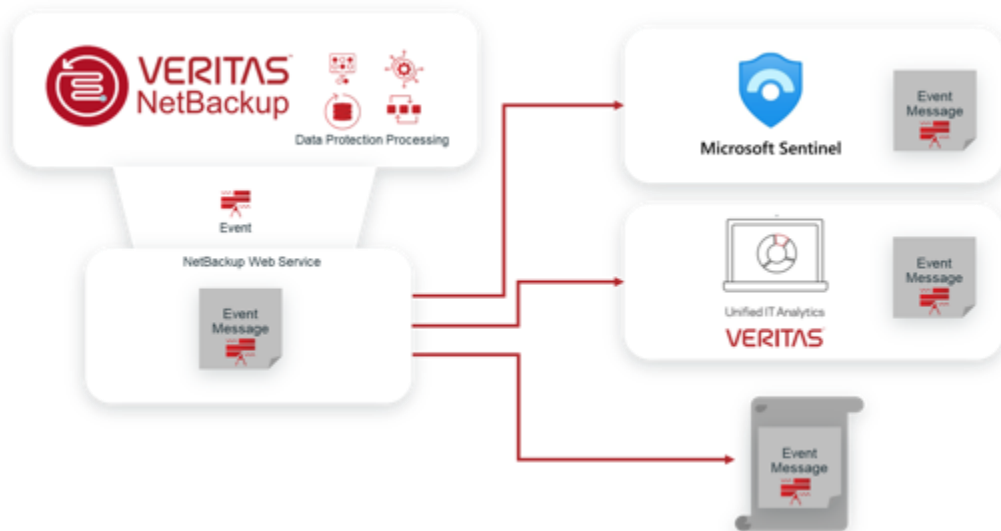
Sensitive Data Summary ①



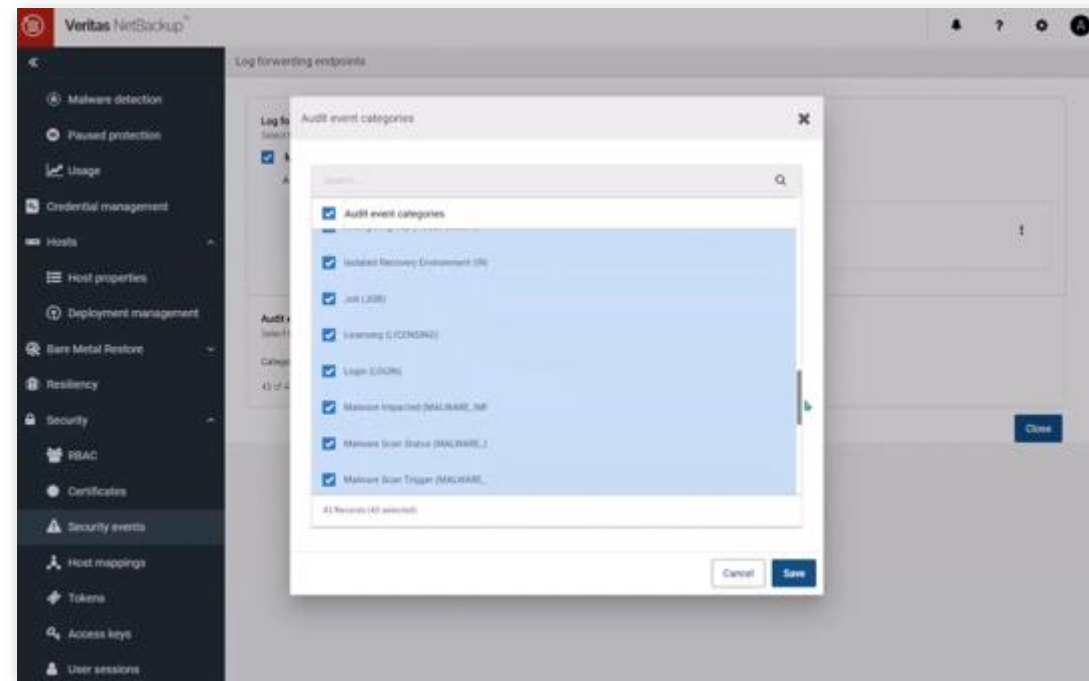


發現異常時觸發事件回應：

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



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



PREVENT DATA DESTRUCTION — PREPARE

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：

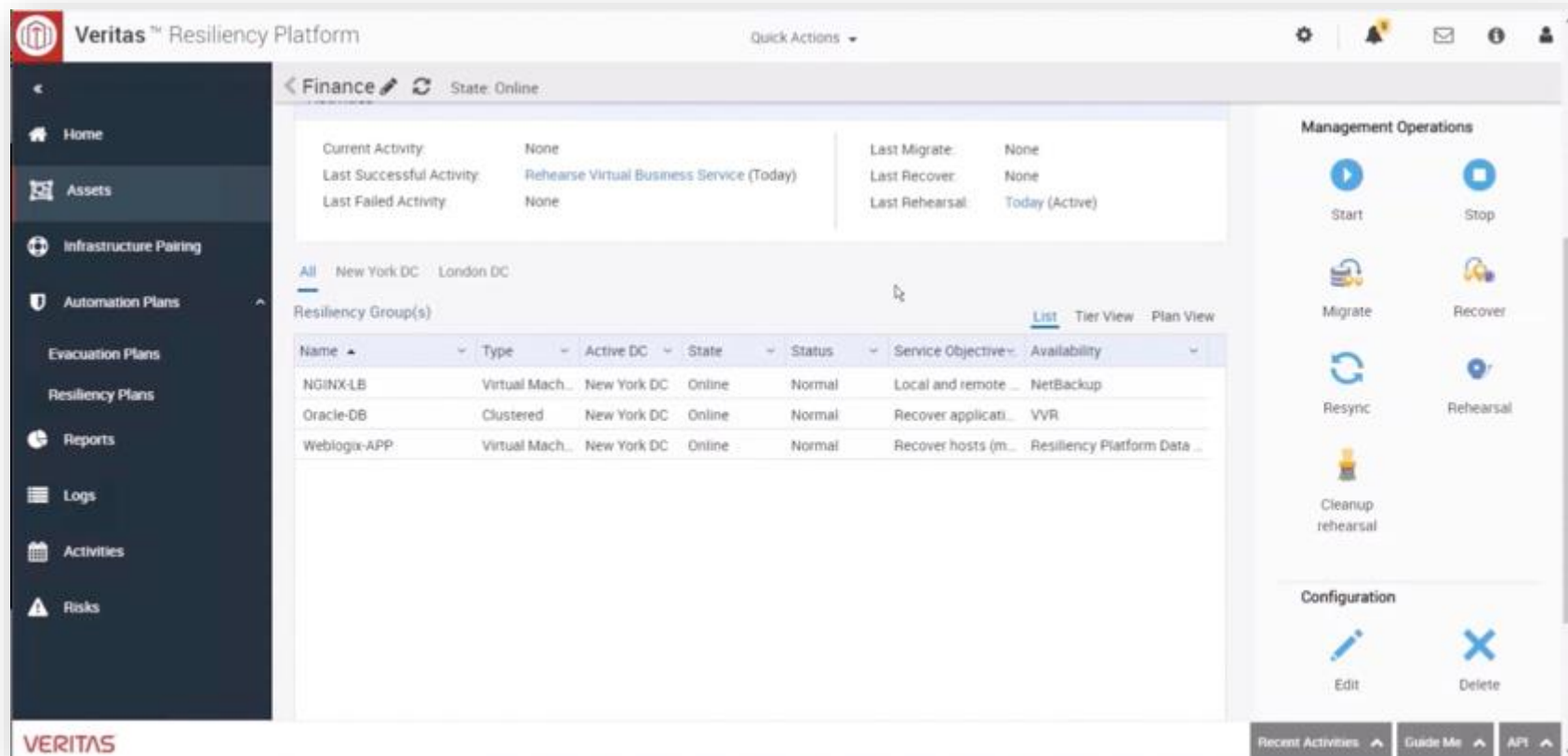
以程式設計方式定義獨特的 執行腳本/工作流，以自動執行災難和網路恢復的恢復過程和任務

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：

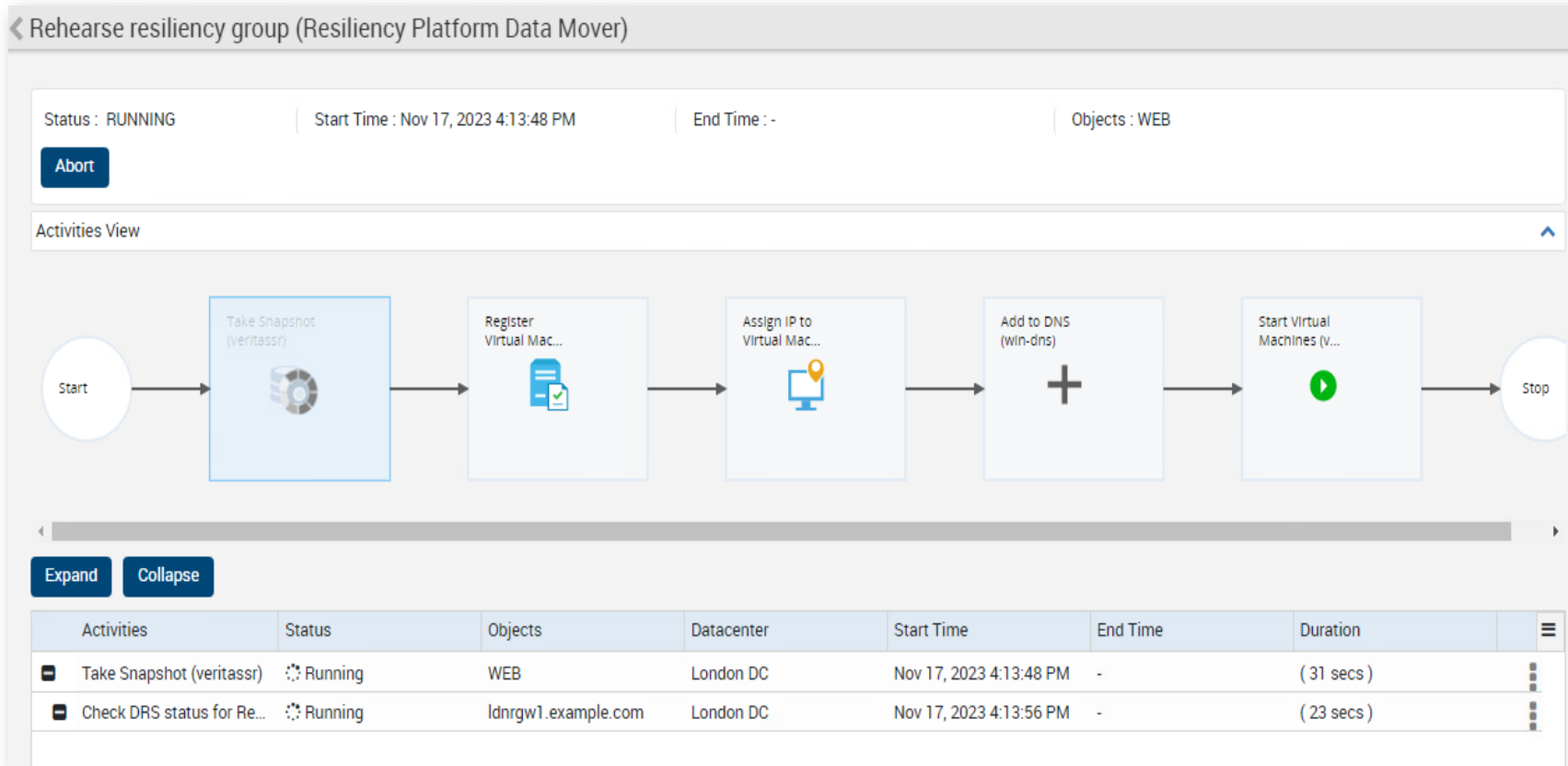
惡意軟體檢測自動化





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





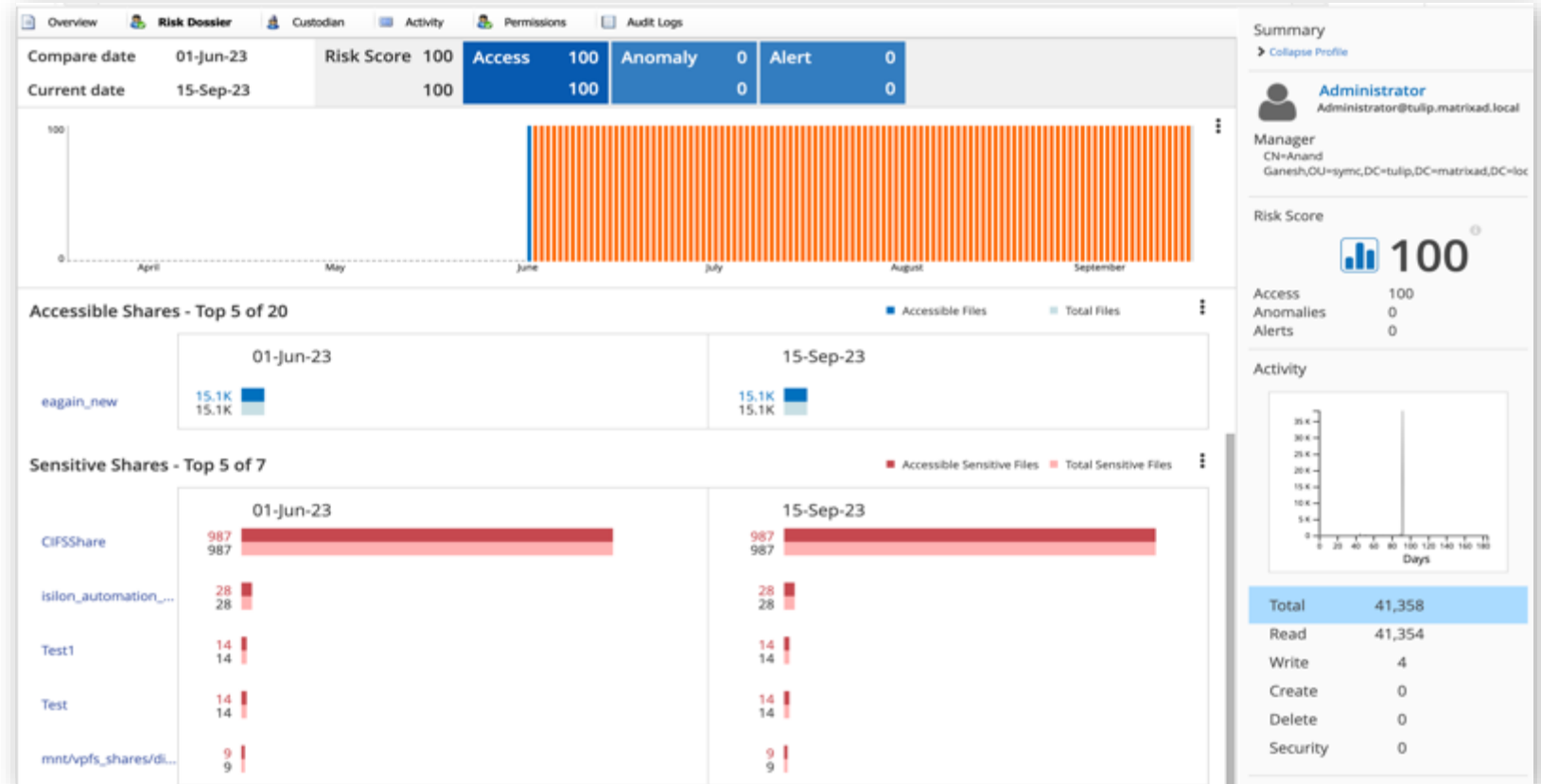
了解可能的資料外洩

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

Recover

Basic properties 2 Recovery details 3

Date range
Jun 26, 2023 3:20:14 PM – Jun 28, 2023 4:46:41 PM Edit

Keyword phrase
Enter keyword phrase

☒ Scan for malware before recovery
Additional malware scanning options are available in the next step.

☐ Allow the selection of images that are malware-affected

g10ch09b10-vm03.vxindia.veritas.com

- ☒ data
- ☐ home
- ☐ mnt

Name	Backup date	Size
<input checked="" type="checkbox"/> data	Jun 27, 2023 8:59 PM	-
<input type="checkbox"/> home	Jun 26, 2023 4:30 PM	-
<input type="checkbox"/> lib64	Jun 26, 2023 3:20 PM	0 B
<input type="checkbox"/> mnt	Jun 28, 2023 4:46 PM	-

Malware scan and recover option

- ☒ If any files are infected with malware, recover only uninfected files (clean)
- ☐ If any files are infected with malware, recover the latest clean copy of the files within the selected date range
- ☐ If any files are infected with malware, recover all files, including infected files
- ☐ If any files are infected with malware, do not perform the recovery job

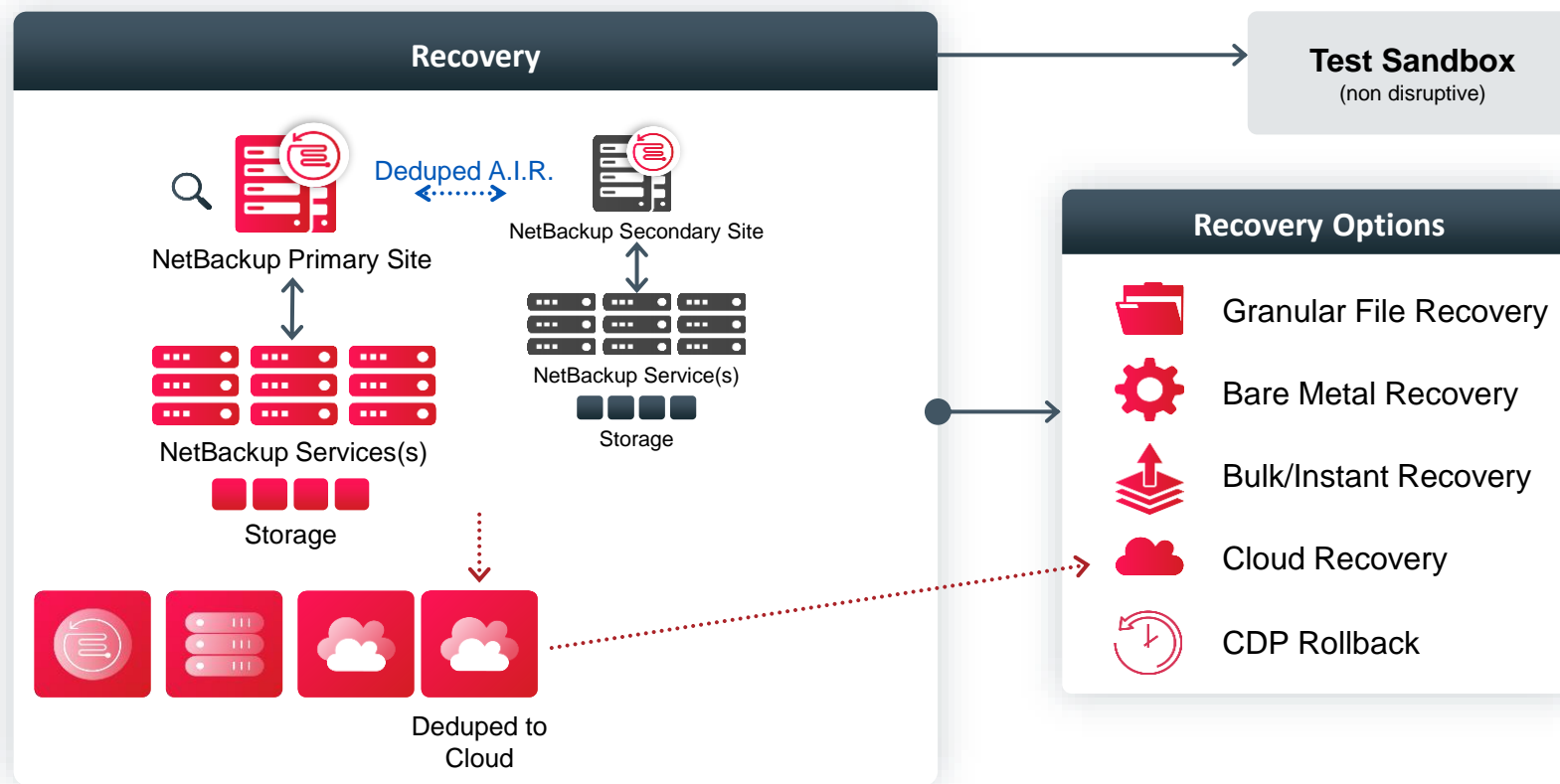


優先恢復關鍵應用進行網路恢復(Cyber Recovery)

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



= Immutable/Encrypted Storage

= Detection Capabilities

.....> = Dedupe

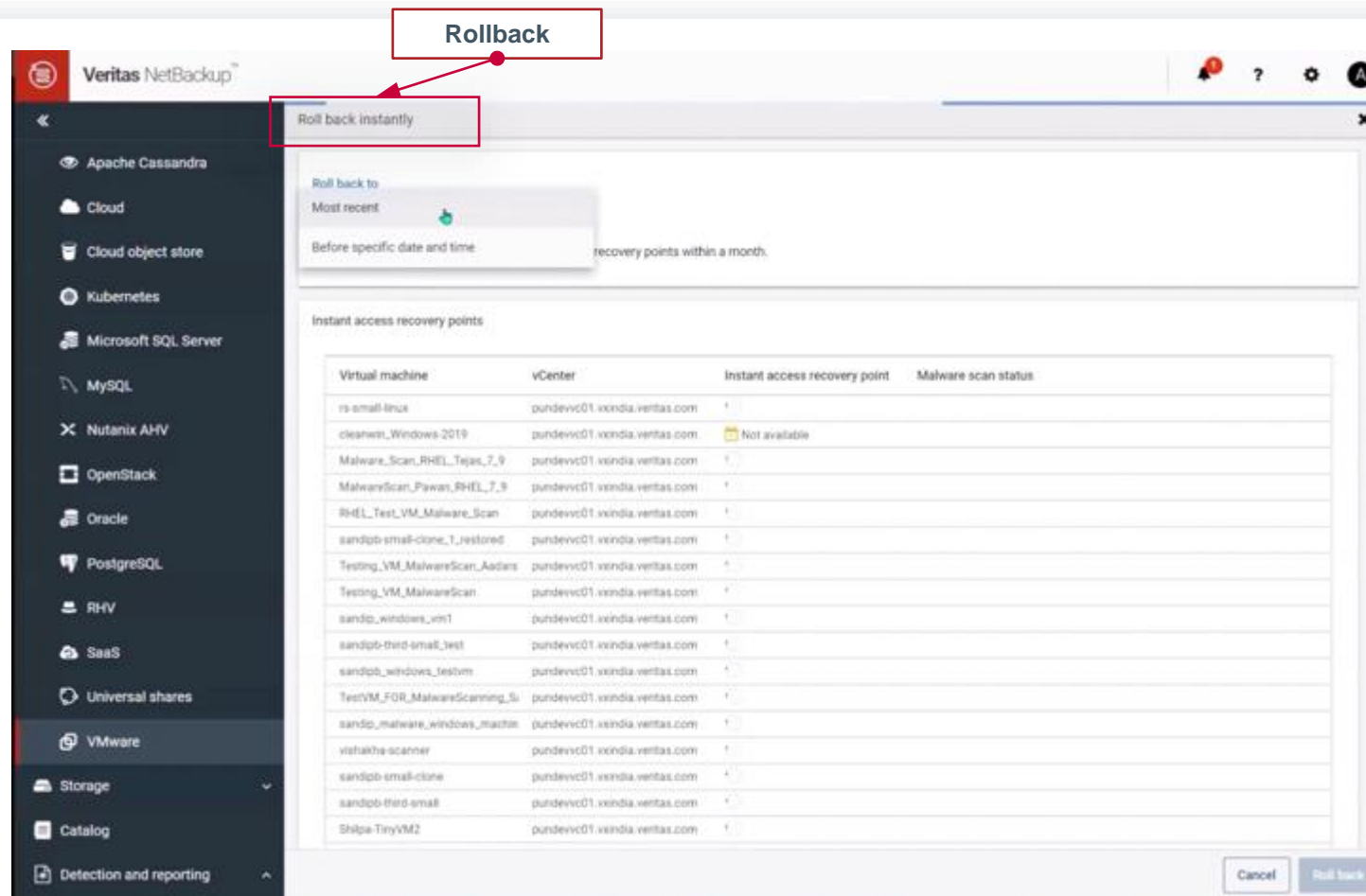


啟動災難還原流程

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

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)

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)

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



Thank You

VERITAS™