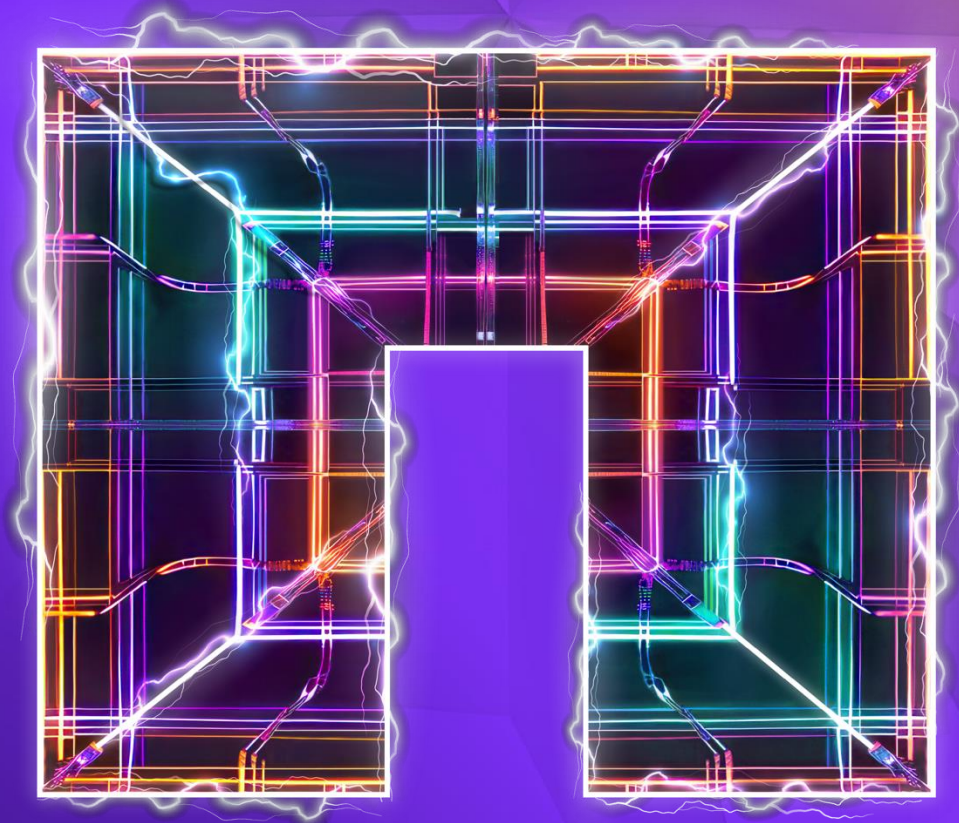


打造 AI 智慧與安全穩固 校園資料中心

Henry Chen 陳思翰
資深技術顧問, NetApp Taiwan



議程

- AI 案例分享 –

美國海軍 / 國家衛生研究院 / 成功大學

- 資安暨後量子加密平台 – 美國國防部

- AFF 儲存效率案例分享 – 臺灣大學

- 資料保護案例分享 – 臺大醫院



#1 IN TAIWAN

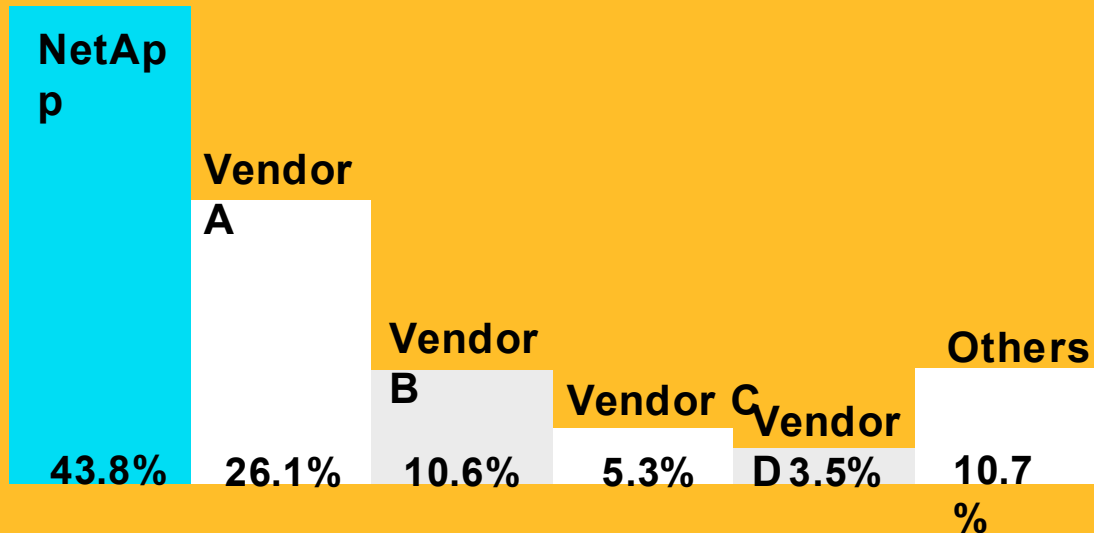
2025 Q1 強勢稱霸

連續七季穩佔領導地位

(2023Q3~2025Q1, 按廠商收入)

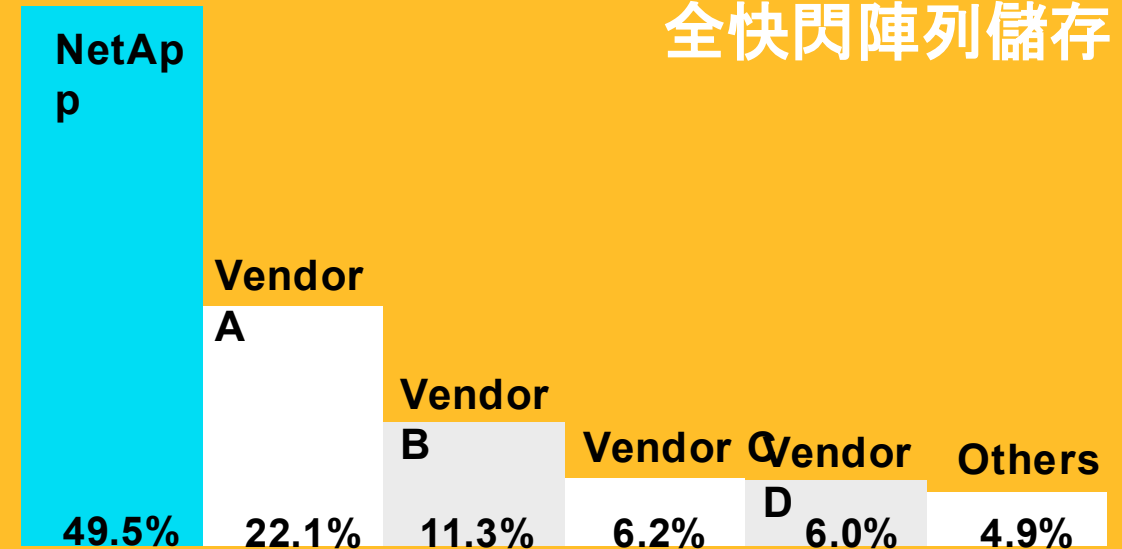
企業外部 OEM 儲存系統 (SAN/NAS ex HCI)

開放式網路儲存



2025 Q1 廠商市場收入計算

全快閃陣列儲存



2025 Q1 廠商市場收入計算

Why NetApp in U.S Military ?



美國政府最大儲存平台供應商



> 800 PB 資料 & 12,000 儲存節點
@美國聯邦政府



IDC 蟬聯多年市占率第一



唯一美國國防部資安認證供應商



唯一整合三大公有雲



美國陸軍



美國海軍陸戰



美國海軍



美國空軍



美國海巡隊

唯一經過驗證可以在任何 地方儲存機敏資料的企業 儲存供應商



Commercial Solutions
for Classified (CSfC)
Component List



FIPS 140-2



Department of Defense
Approved Product List
(DoDIN APL)



Common Criteria

美國國防資訊系統局認證 NetApp 部署文件



Technical Report

Military Unique Deployment Guide (MUDG) for ONTAP Data Storage Controller (DSC)

Instructions to obtain the MUDG for NetApp customers and employees

Lisa Rogers, NetApp
March 2024 | TR-4754

Under guidance from DISA (Defense Information Systems Agency)



Abstract

TR-4754 provides instructions to access the Military Unique Deployment Guide (MUDG) for ONTAP Data Storage Controller (DSC) for NetApp customers and employees.

Instructions for customers to access the MUDG

U.S. government civilians or U.S. uniformed military personnel can request a copy of the CAP through email. Requests must be received from a .mil or .gov email address and be sent with a digital Public Key Infrastructure (PKI) signature attached.

To request a copy of the CAP (which includes the MUDG), U.S. government civilians or U.S. uniformed military personnel should complete the following steps:

1. Go to the **DoDIN Approved Products List** at <https://aplits.disa.mil/processAPList.action>.
2. In the Vendor dropdown, select **NetApp**.
3. Click **Search APL** to display the current ONTAP certification.
4. Click **Request CAP** to automatically create the email below. If the requestor does not have a .mil or .gov email address, the requestor should have their military lead make the request.

To: disa.meade.ie.list.approved-products-certification-office@mail.mil
Subject: Request Cybersecurity Assessment Package (CAP) for TN <#####>

Notice to requester

Due to the sensitive nature of the Cybersecurity Assessment Package (CAP) that you are requesting, the information can only be sent to US Government Civilians or U.S. Uniformed Military Personnel. This request must be received from a .mil or .gov email address and be sent with a digital PKI Signature attached. Failure to comply will result in a denial of the request.

As a reminder, the information contained in the CAP that is being requested is designated as CUI and is legally privileged/binding. It is intended solely for the addressee. Distribution or disclosure of any information contained within to anyone outside the military community or the federal government is strictly prohibited.

5. Modify the email as needed then send.

ONTAP 全方位儲存平台

滿足各種需求的資料儲存

統一化

SAN
最佳化

成本最低
次要儲存運用
混合式 Flash

FAS



NEW

最佳性價比
大容量 Flash

AFF C-Series



NEW

最佳效能
第一級工作負載運用
高效能 Flash

AFF A-Series



High-End
RELEASED
in
May

Low-Mid
NEW

ASA C-Series



ASA A-Series



混合多雲



Google Cloud

Microsoft Azure

美國海軍 TRIDENT WARRIOR

AI 與隱私保護演習平台

NVIDIA TESLA V100 + NETAPP AFF GPU DIRECT STORAGE

美國海軍 Trident Warrior 演習背景與挑戰

- 需在不暴露原始影像的情況下，進行即時辨識 VIP 臉部
- 傳統解決方案常需高硬體資源，且在機器學習生命週期中表現不一致，導致部署延遲



NVIDIA + NetApp 解決方案

- NVIDIA TESLA V100 GPU + NetApp AFF GPU Direct Storage
- Stained Glass Transform™ 將影像轉換為僅供 AI 模型解讀的隨機化再表示 (Randomized Re-Representations)
- 部署過程中，資料保留在海軍內部，確保資料主權與安全。

成果與效益

- 超過 99% 高精準臉部辨識
- 部署過程中，資料保留在海軍內部，確保資料主權與安全
- 未來可結合公雲 LLMs 和生成式 AI 模組



首先, AI workload 需要 external storage?

資料規模

要讓AI模型準確度越高，訓練用的資料越多越好，在這個前提下，資料量會不斷成長

Local storage空間遲早不夠，**所以需要容易擴充的external storage**。另外，現在的Gen AI LLM模型越來越大，參數越來越多，GPU memory過於昂貴空間不夠的狀況下，也需要高效能的external storage來幫忙最佳化整體成本。

LLM的典型狀況是，一個具有1 billion (10億) 參數的model，需要GPU memory至少80GB (32-bit full precision)。Meta的LLaMA 2有約70 billions (700億) 參數，估計需要 $80GB \times 70 = 5600GB = 5.6TB$ 的GPU memory，而OpenAI的GPT4則是號稱有兩萬億參數，估計需要 $80GB \times 2000 = 160TB$ 的GPU memory...?

資料分享

多個GPU node需要由統一平台提供資料給不同GPU node進行運算，避免資料孤島

所以需要分享資料用的external storage，解除local storage管理資料的限制與麻煩，提升資料科學家的工作效率

資料獨立

AI時代的應用不斷改變，但資料才是企業最寶貴的資產，**因此將計算與儲存分開，做到計算不斷迭代，而資料永久持續**

這也正是Microsoft, Facebook, AWS, Google, Nvidia等科技巨頭的做法，所以需要獨立運作的external storage來達到此目的。

資料安全

如何**最有效率地保護資料**，備份資料、還原資料、移動資料、加密資料、防止勒索病毒、訪問控制、分析使用行為、分類識別隱私等，這些都是非常重要的安全考量，所以需要專業的external storage來提供這些企業級服務

NetApp AI Pod Reference Architecture

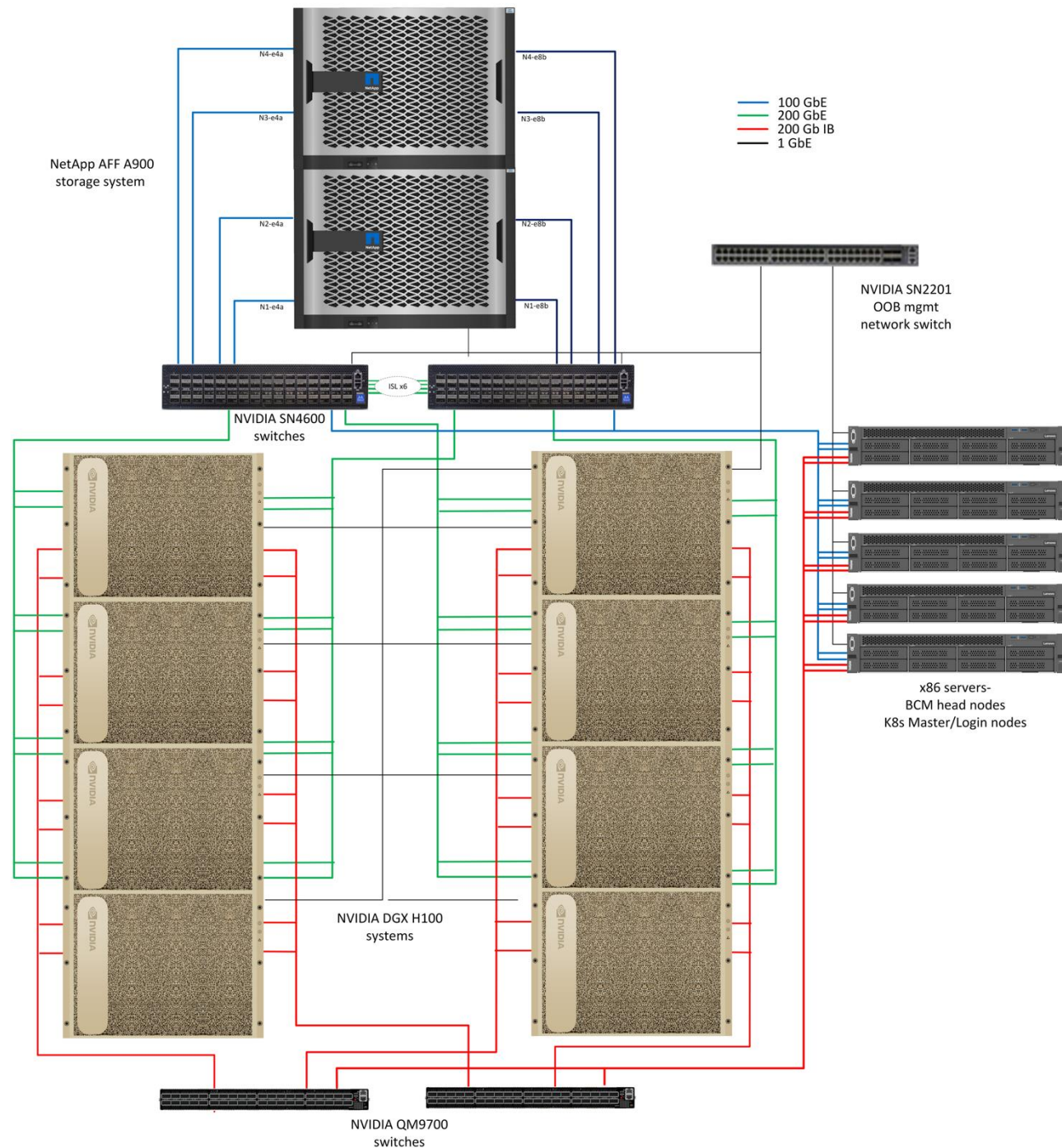
DGX H100 –
H100 GPU x8

NetApp Ontap –
A series, C series

Network –
GPU node之間溝通走
Infiniband 200Gb IB,
GPU node跟storage的溝通走
GDS over ethernet 100GbE

Nvidia認證NetApp

<https://www.nvidia.com/en-us/data-center/resources/netapp-ontap-ai-reference-architecture/>



Our turnkey solutions for AI infrastructure simplify and accelerate use cases

Power enterprise AI workloads across the data lifecycle

ENTERPRISE AI

HPC | Model Training | Fine-Tuning | Inferencing

High-performance computing
and model training

Model training, retraining, fine tuning, and inferencing

GenAI, RAG, inferencing for
departmental/branch office

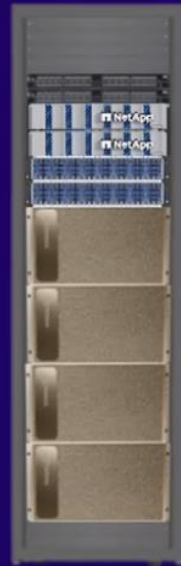
GenAI, RAG, training,
and bursting



NVIDIA DGX SuperPOD



FlexPod for AI



NetApp® AIPOD™



NetApp® AIPOD™
w/Lenovo



NetApp AIPOD™ Mini



Cloud Infrastructure

國衛院啟用 NetApp AFF A800，為生醫 AI 平台建立快速且流暢的資料傳輸通道

以 A800 為中繼儲存，快速輸送資料至 GPU 伺服器，提升 AI 建模效率

文/ 廠商新聞稿 | 2022-10-14 發表

讚 45

分享



「我認為 NetApp AFF A800 最大優勢，在於擁有優異的資料儲存與分享效率，並擁有高穩定度，且只要我們拋出問題、NetApp都能快速回應。這些特質，足以帶給國衛院充足信心，未來不論承載多麼龐大複雜的基因資料庫，也無所畏懼。」 國衛院群體健康科學研究所所長 邱弘毅



成功大學善用 NetApp 全快閃設備，駕馭 AI 發展及資料爆量趨勢

評估重點：符合關鍵應用、投資不浪費、不增加管理負擔、服務不中斷

文/ 廠商新聞稿 | 2024-01-19 發表

讚 50

分享



成功大學計算機與網路中心 李南逸組長（左）、陳培殷主任（中）、黃琮富資深網路管理師（右）

iT+ 看影片追技術



如何以 Cloud Native 工具服務打造您的雲端安全

Cloud Summit 臺灣雲端大會
| 29 分



在 DevOps 的路上測試該怎麼進行

DevOpsDays | 42 分



企業資安事件化繁為簡 必備良方 Cortex XDR

IT EXPLAINED | 40 分



【SOAR資安自動化協作】NETAPP CONFIDENTIAL

© 2024 NetApp, Inc. All rights reserved. 安基資訊 | 資安防護服務 · 企業

美國國防部

資安暨後量子加密平台

(THE U.S. DEPARTMENT OF DEFENSE)

ONTAP Anti-Ransomware 防勒索病毒

Post-quantum Cryptography (PQC) 後量子加密技術

“[NETAPP 通過 CSFC 認證] 是商業技術創新用來解決關鍵國家安全問題的一個典範。”

— 美國海軍退役上將 **ADMIRAL MICHAEL S. ROGERS** ,
前美國國家安全局局長暨中央安全局局長



Only enterprise storage validated by NSA CSfC to store top-secret data



Policy Engine



Automatically block known malicious file types

Immutable WORM Primary Data & Tamper-Proof Snapshots



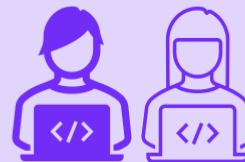
Prevent data destruction with immutable & indelible snapshots

AI Validate detection



AI-powered, real-time ransomware detection and response

Multi-Admin Verify



Block rogue admins and malicious users

End-to-End Encryption



Secure data access, end to end

Only enterprise storage validated by NSA CSfC to store top-secret data

Automatically Trigger Snapshot Protection



Monitor Config

Anti-ransomware

STATUS

Enabled in learning mode

Started Time: 16 Sep 2021 6:51:PM

The system has been auto-learning the workload characteristics of t

A learning period of 7 to 30 days is recommended.

You can switch from "learning" to "active" mode at any time.

Switching early might lead to too many false positive results.

Switch to active mode

Monitor new file types

New file types are file types that were never detected during the learning mode.

MAXIMUM NUMBER OF NEW FILE TYPES THAT'S CONSIDERED NORMAL

20

 in

24

 Hours

Automatically block known malicious file types

Event severity settings

Event	Severity
Detected new file extensions	Don't generate ev...
Created a ransomware Snapshot copy	Notice
Detected a ransomware attack	Alert

Cancel

Save

Overview

Snapshot Copies

SnapMirror (Local or R

+ Add

	Name
	Anti_ransomware_backup.2021-11-18_1506
	hourly.2021-11-18_1505

Prevent data destruction with immutable & indelible snapshots

Suspected File Types

Suspected File Types

You can mark the suspected file types as false positive or potential ransomware attack. The system will make necessary adjustments to the way it detects abnormal activity in the future.

Search Filter

	Type
	lckd
FILES (SHOWING A MAXIMUM OF 20 FILES)	
	/Top_Dir_1/Sub_Dir_11/test_file_8335.5.png.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_27373.5.html.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_27373.5.mp4.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_27373.5.doc.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_27373.5.gif.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_103.2.jpg.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_103.2.doc.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_3040.5.html.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_3040.5.mp4.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_3040.5.doc.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_3040.5.gif.lckd
	/Top_Dir_1/Sub_Dir_11/test_file_3040.5.xyz.lckd

AI-powered, real-time ransomware detection response

利用 AI 進行自主勒索軟體防護

Next generation ransomware threat detection



世界上第一個針對主要儲存的 AI 驅動型 On-Box 勒索病毒偵測



下一代 AI/ML 從第一天起就確保精確檢測

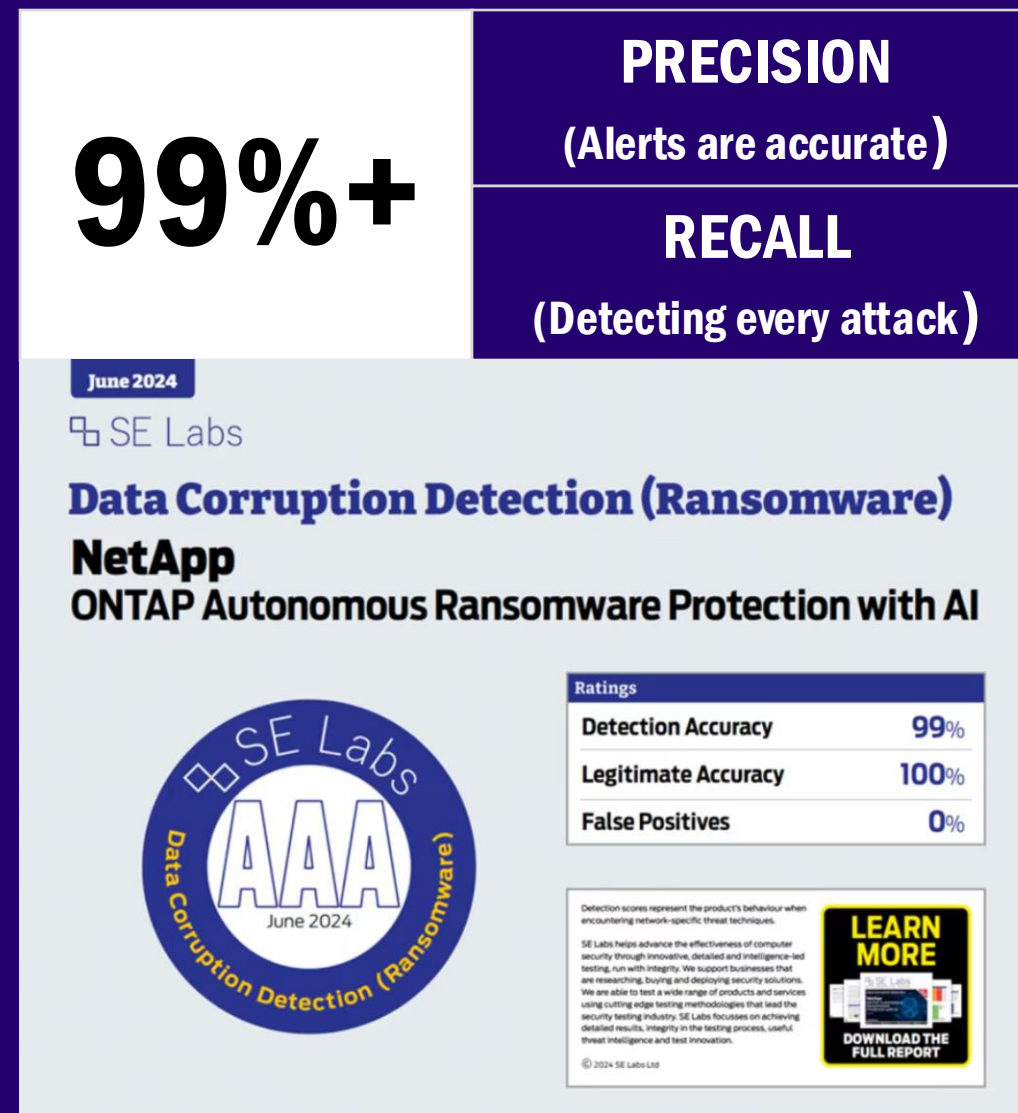


自動更新可提供最佳、高效且準確的一站式主動偵測



為現有 ARP 客戶輕鬆自動升級

SE LABS rating:
<https://ntap.com/3VIHMF2>



ONTAP內建的全方位資料保護

保護您的資料、發現攻擊並阻止、從災難中迅速恢復

保護

Policy Engine

Immutable WORM Primary Data &

VM內部的變更 (VM外部尚未變更)

- 預設風險較低的檔案
例如.txt、.docx 或.mp4 檔案時
ARP會偵測到威脅
雖然在此場景中 ARP 建立了保護性快照
但它不會產生威脅警報
- 預設風險較高檔案
例如 .gzip 或受密碼保護的檔案
ARP 的偵測功能會受到限制
但ARP 仍然可以主動進行快照
如果檔案副檔名未被外部篡改
- 則不會觸發警報

阻止誤操作與惡意使用者

資料加密存取

VM on NFS volume

偵測

Autonomous
Ransomware Protection



利用AI
內建即時偵測勒索軟體
攻擊行為與告警

還原

VM外部的變更

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

PQC

(Post-quantum Cryptography)

後量子密碼學

1. 傳統密碼學是一把對一般現有電腦算力有效的鎖
2. 但量子電腦是一種全新的「超強開鎖工具」，可能輕鬆破解這些鎖。
3. PQC 就是專為連量子電腦都打不開而設計的新一代密碼鎖。

加密機制恐遭破解，數發部公布後量子密碼遷移指引

<https://ntap.com/43SVniW>

因應

衝擊

- 具備強大運算力的量子電腦問世，傳統密碼後端的加密機制就會被破解

- 既有的資料加密保護方式不再安全，系統的簽章與憑證會被破解與偽冒

原因

• 美國

- 聯邦政府已在進行後量子密碼遷移過程，概念上是要讓現行密碼的後端加密機制改變演算法，讓量子電腦無法破解密碼

- 2027 新購通訊設備須符合後量子密碼
- 2030年強制汰換較短的加密機制設備，
- 2035年要全面完全更換後量子密碼設備

• 台灣

- 2025/4/16
- 發布台灣首版「後量子密碼遷移指引」協助產業提升資安保障
- 依照框架可分為4大遷移程序，包括：
 - (一) 建立量子準備計畫
 - (二) 盤點加密資產清單，
 - (三) 與技術供應商討論量子準備計畫
 - (四) 確認供應鏈的量子準備程度。

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>



NEWS

NIST Releases First 3 Finalized Post-Quantum Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

While there have been no substantive changes made to the standards since the draft versions, NIST has changed the algorithms' names to specify the versions that appear in the three finalized standards, which are:

- **Federal Information Processing Standard (FIPS) 203**, intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the CRYSTALS-Kyber algorithm, which has been renamed ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism.
- **FIPS 204**, intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.
- **FIPS 205**, also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

NetApp's PQC Roadmap



TODAY



DATA-AT-REST

- PQC ready now using AES-XTS-256 for data-at-rest encryption

MID-2025



DATA-IN-TRANSIT

- Scheduled for ONTAP 9.17.1 release
- Lattice-based Key Encryption support for OpenSSL 3.5, ML-KEM, ML-DSA
(**FIPS203, FIPS204**)
- Stateless hash-based digital signature support for SLH-DSA
(**FIPS205**)

FUTURE



DATA-IN-USE

- In-use encryption includes off-load cards, and in-memory operations
- Working with hardware vendors and partners to develop future solutions

AFF 儲存效率 案例分享

臺灣大學



臺灣大學 – AI 智慧校園願景

- 計算機中心 AI 平台
- Inference Model 藉助地端資料中心
- AI 導入資安、My NTU 問答
- 容器化應用



周承復 主任
計算機及資訊網路中心



NetApp 在臺灣大學幫忙做什麼？

- 校務核心、公文、校務資料庫系統
- All Flash 儲存提升資料庫效能 1.7 倍 ↑
- 防勒索病毒資料保護平台
- 混合雲端備份平台



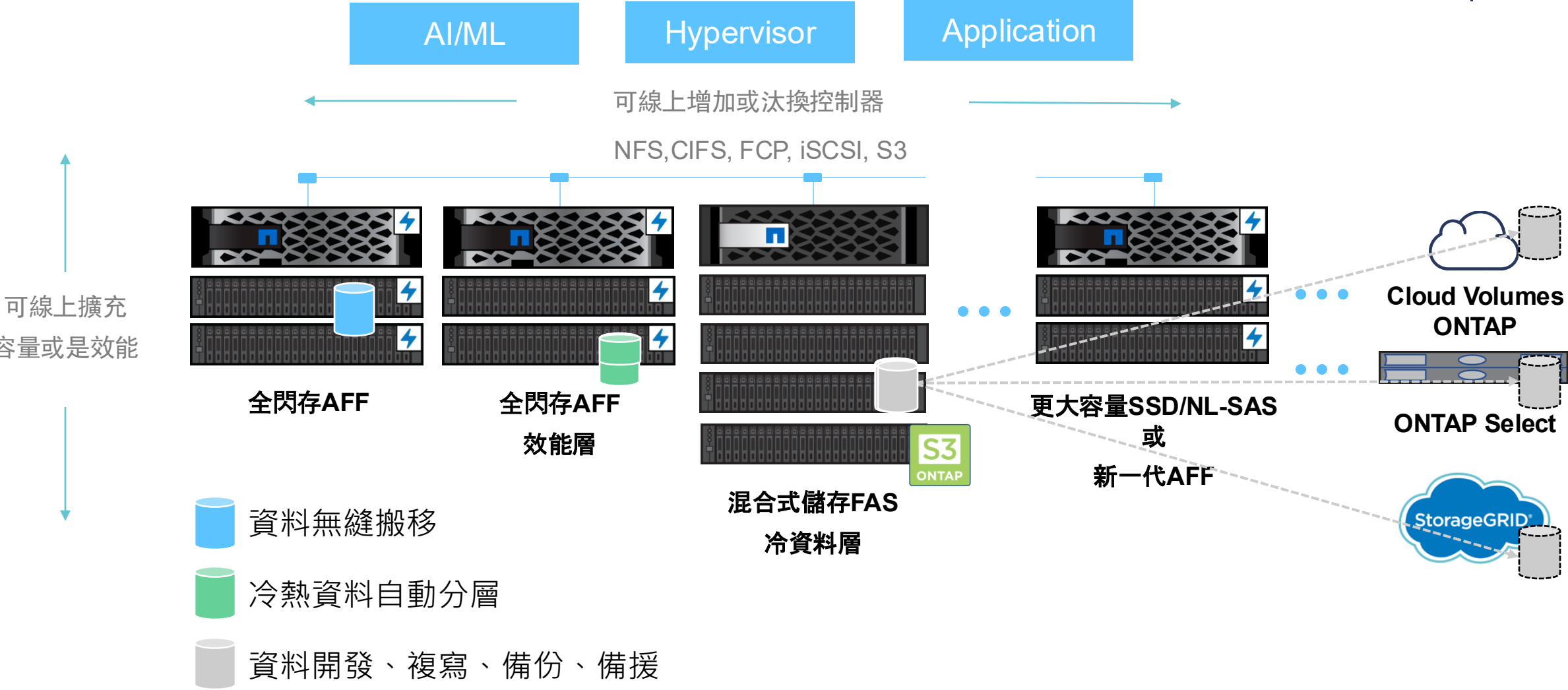
國立臺灣大學
National Taiwan University

周承復 主任

計算機及資訊網路中心

企業級資源池分享

因應需求，更新和擴展叢集群，而不會中斷業務

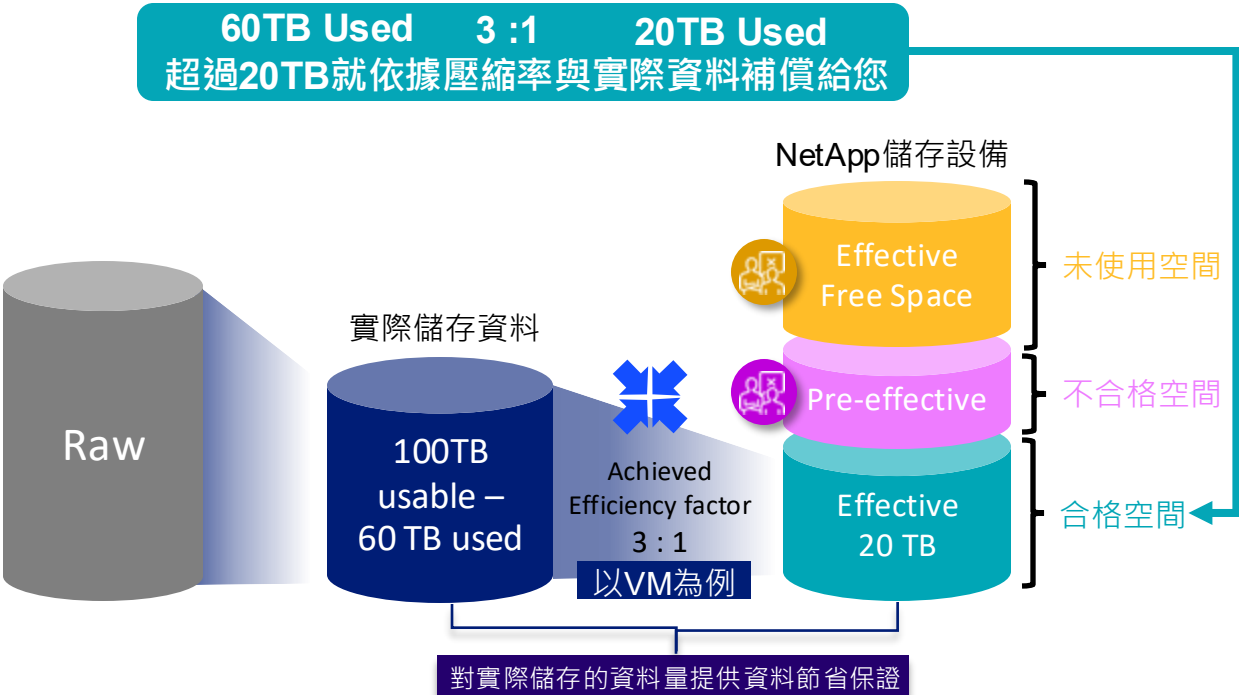


NetApp 儲存效率保證 (SEG)

業界最簡單也最有效的效率保證，無庸置疑

- 1. 能毫無風險地享有更多儲存容量更高價值及更出色的效率
- 2. 如果沒有達到您的工作負載效率目標，我們會免費補償給您
- 3. 無需取捨，一次擁有高效率和高效能
- 4. 適用於所有 NetApp® AFF 系統

SAN 工作負載為 4:1
NAS 工作負載為 1.5:1
VMware、Hyper-V 及 NAS 的 KVM 工作負載為 3:1



我們的保證很簡單、很直接

資料保護 案例分享

臺大醫院

NetApp SnapCenter + VMware plug-in

臺大醫院憑藉NetApp FAS8200助陣，樹立高效率SOC服務標竿，勾勒AI未來展望

以高速快取與無與倫比彈性助長ELK效能，形塑最迅捷的安全、除錯及維運流程

文/ 廠商新聞稿 | 2023-01-03 發表

讚 132

分享



「臺大醫院自2021年初啟用集中式圖像化日誌系統迄今近兩年來，讓資訊室同仁更方便搜尋與監控所有日誌，加速破解設備或應用系統的各種疑難雜症。ELK的成功，一部份歸功於搭配合適的儲存設備，有效消弭資料擷取的漫長時間堆疊與浪費。」 臺大醫院資訊室

IT+ 看影片追技術



補足 IT 管理的最後一哩路，遠距工作時代整合方案：Intel vPro 商用平台 + 旭辰 Smart IT

IT EXPLAINED | 38 分



Azure Red Hat OpenShift 協助企業加速創新

IT EXPLAINED | 48 分



安碁學苑資安人才培訓藍圖

臺灣資安大會 | 20 分

資料庫保護全攻略 (一)



ONTAP Tools

☰ vSphere Client

🔍 Search in all environments

🔄

👤 Administrator@VTME.LOCAL ▾

😊

❓ ▾

NetApp ONTAP tools [INSTANCE 10.193.54.102:8443 ▾](#)

ONTAP tools for VMware vSphere

vCenter server [vc1.demo.netapp.com ▾](#) ⓘ

Last refreshed: 04/26/2023 17:43:00
Next refresh: 04/26/2023 18:13:00

Getting Started **Traditional Dashboard** vVols Dashboard

ⓘ The dashboard displays metrics obtained from vCenter Server (IOPS, space utilized, latency and committed capacity) and ONTAP (space savings).

Overview

空間資訊與效能

Datastore capacity



● Used: 40.92 GB
● Free: 116.58 GB
Total: 157.50 GB

IOPS

0
Read IOPS
0
Write IOPS
0
Total IOPS

Aggregate space savings

Aggregate ▾ All ▾

1.28 : 1

○ Logical space used: 65.14 GB
● Physical space used: 51.03 GB
Space saving: 14.12 GB (21.67%)

Datstores

3

Top 5 datstores by **Space Utilized ▾** **High to Low ▾**

Type ☒ All ☐ NFS ☐ VMFS

nfs3		29.55%
nfs1		26.02%
iscsi1		8.62%

Storage Systems

Clusters: 1



SVMs: 1



[View all storage systems](#)

Virtual Machines

4

Top 5 VMs by **Committed Capacit... ▾** **High to Low ▾**

OTV1	9.44 GB
scv-1	5.63 GB
SiteA-vm01	2.87 GB
vCLS-e4ee0253-58d0-4952-b462-6ee69bdabdc	360.86 MB

Best Practice

ESXi Host Systems

1

NFS settings: 1



MPIO settings: 1



Adapter settings: 1



[Edit ESXi host settings](#)

- Supports VMware vSphere 8.x releases thus providing you the benefits of ONTAP 9.12.1 and VMware vSphere 8 features.
- Supports NVMe through NVMeOF vVols 3.0.

- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

The screenshot displays the vSphere Client interface with the SnapCenter plug-in installed. The left sidebar shows the 'burt_vm' VM selected. The main pane shows the 'Configure' tab for the VM, with the 'Backups' section under 'SnapCenter Plug-in for VMware vSphere' highlighted. A 'Guest File Restore' window is open, showing a list of files to restore. The 'master.mdf' file is selected for restoration.

整合快照還原

Backups

Name	Size
test_rg_nfs_07-27-2020_...	
burt_rg_07-27-2020_...	
test_rg_nfs_07-27-2020_...	
burt_rg_07-27-2020_...	
test_rg_nfs_07-27-2020_...	
burt_rg_07-27-2020_...	
test_rg_nfs_07-27-2020_...	
burt_rg_07-27-2020_...	

Guest File Restore

Guest Session

Backup Name

NFS_Datastore_Backup_0

Run As Credential

Proxy Credential

精細還原-單一檔案

What's new?

April 4, 2023

- Includes key security enhancements to adhere to high security levels.
- Supports VMware vSphere 8.x releases thus providing you the benefits of features.
- Supports NVMe through NVMeOF vVols 3.0.

SnapCenter – 支援平台列表

檔案系統 / 虛擬層資源 / 資料庫 / 儲存系統

應用程式 / 資料庫	 Exchange	 Microsoft SQL Server	 ORACLE DATABASE	 SAP HANA		
檔案系統	 Windows Server					
虛擬層資源	 vmware					
客製化支援	 mongoDB	 SAP MaxDB The SAP Database	 SAP ASE Sybase	 IBM DB2	 MySQL	 PostgreSQL
儲存系統	 ONTAP				 ONTAP	 ONTAP

重點整理

01

NetApp x NVIDIA AI 資料平台全面落地

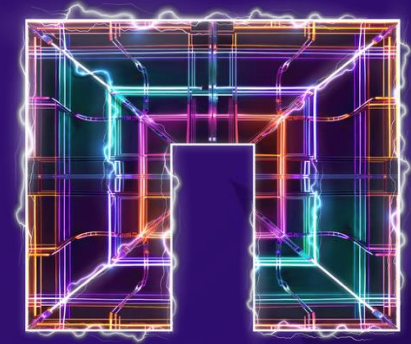
02

資料儲存效率保證，說到做到

03

業界唯一原生「主動式」防勒索病毒平台

謝謝



POWERED