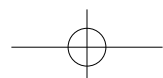




QNAP

資料保護解決方案 Solution Brief

建構具備勒索軟體防護能力的架構並確保業務連續性



資料遺失 如何演變成 企業危機

真實世界的事件，顯示一個系統故障如何引發下一個危機

網路入侵

駭客在入侵網路設備後，對一家日本食品公司發動勒索軟體攻擊，並進一步進行橫向移動¹。

無法使用的備份

僅有 32% 認為他們能在一週內復原²。

備份銷毀

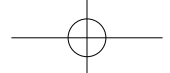
像是 Storm-0501 等勒索軟體活動，現在刻意鎖定並銷毀備份資料³。

營運停擺

一家德國行動保險業者在遭到加密後無法復原，最終申請破產⁴。

來源：

1. 《關於網路攻擊資料外洩的調查結果與未來措施》Asahi Group
2. Veeam 資料保護趨勢報告
3. Storm-0501 的演變技術導致雲端勒索軟體
4. 勒索軟體導致保險公司破產



這些事件的共通點

就是單一層面的防禦已不足以阻擋完整的攻擊鏈與故障。



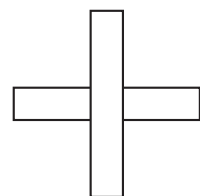
3

那麼，如何避免危機？ 

1 + 3 資料保護框架

打造具備勒索軟體防護力的架構體系

備份
與復原



預防

保護

可用性

- **備份** 仍然是事件發生後最直接且可靠的復原機制。
- 近年的案例顯示，資料遺失與營運中斷鮮少是因單一防護機制失效所致。現代資料保護策略正從以備份為中心的思維，轉向多層次的韌性架構。透過在備份基礎上強化網路端**預防**、系統與**資料保護**，以及系統級的**高可用性**，企業能有效降低多個環節的失效風險，全面提升整體的營運韌性。



關於 QNAP

深耕業界超過 20 年，QNAP 作為全球領先的 NAS 儲存品牌，以『提供全方位且值得信賴的資料保護解決方案』為使命。我們跨越儲存界限，整合了網路、監控、雲端及資安領域；透過嚴謹負責的研發精神，QNAP 已發展成為企業首選的全方位基礎架構解決方案供應商，是組織轉型最可靠的後盾。



5

查看 QNAP 資料保護解決方案 

QNAP 端對端資料保護

全面守護跨工作負載、平台及據點的企業資料

備份多種工作負載



Hyper Data Protection(HDP) New

免授權費，備份 Windows® PC、伺服器、VMware®/Hyper-V™ 虛擬機、SaaS 等



Qsync

PC/Mac 的即時檔案同步與備份

備份 NAS 資料



Hybrid Backup Sync (HBS 3)

可靠地將 NAS 資料備份及同步至其他 NAS、遠端伺服器或 20+ 雲端服務

管理平台

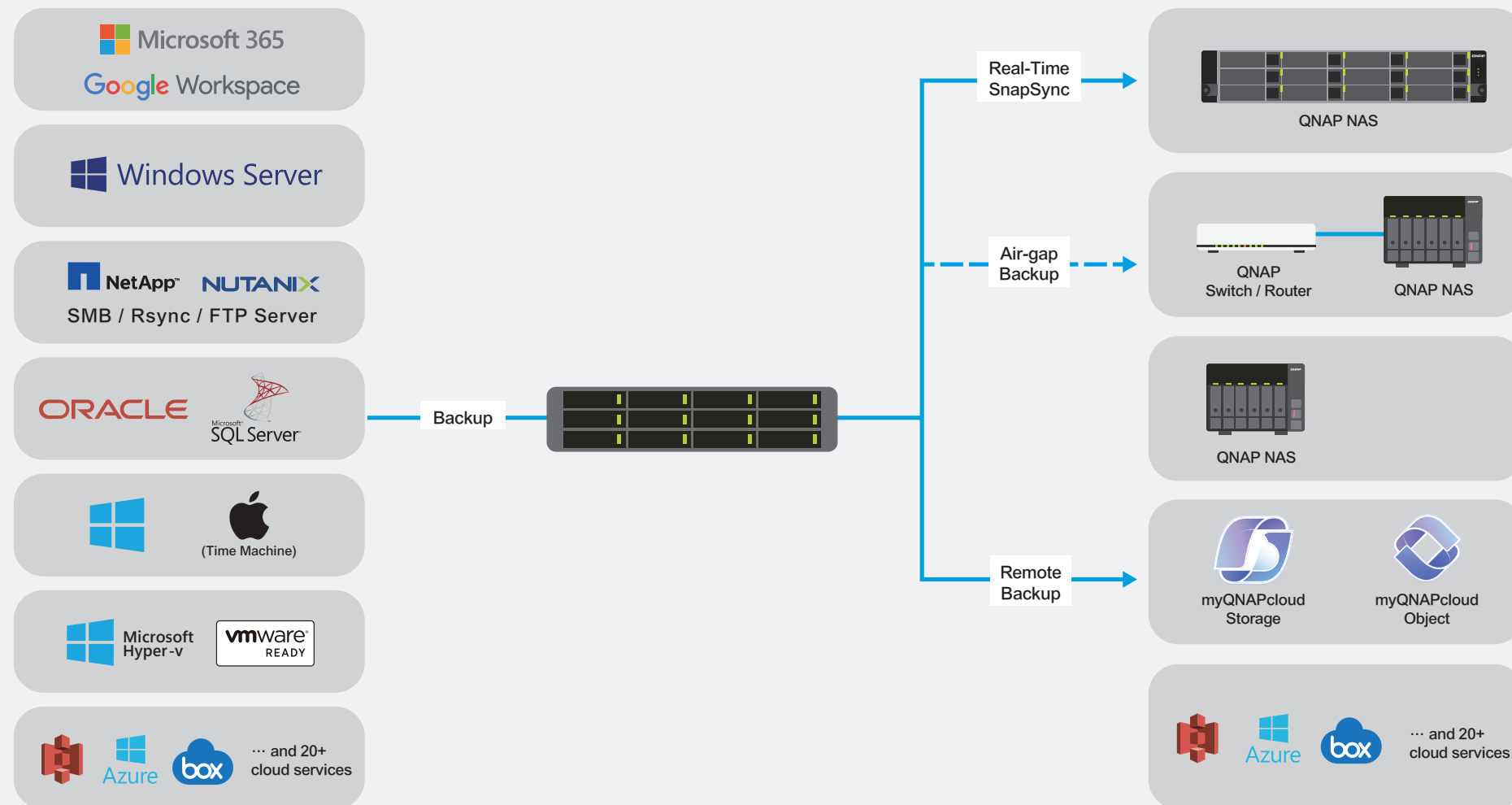


Hybrid Backup Center

集中化雲端儀表板，用於監控和管理跨站點、跨裝置的備份與還原任務



橫跨裝置、網站與雲端的統一備份架構



專為可靠資料保護所打造

以毫不妥協的可靠性基礎賦能全球企業

為何選擇 QNAP?

因為我們不僅儲存您的資料，更結合領先業界的硬體與具備韌性的軟體生態系，確保您的業務永不停歇。



高效能基礎架構

- Intel® / AMD® 多核心運算力
- 高速 25/10GbE 連線，為 100GbE 預做準備
- 可擴展、PB 級的儲存空間，滿足長期資料增長

QuTS hero

可靠的 ZFS 系統

- 自我修復能力以防止靜默資料損毀
- 即時 SnapSync 以實現零 RPO 的災難復原
- 不可變快照提供防勒索軟體的復原點

了解更多 | [QuTS hero](#)



myQNAPcloud

安全的混合雲策略

- QNAP 打造的雲空間，讓異地備份更輕鬆
- 相容 S3 的物件儲存最佳化資料管理
- 透過 WORM（一次寫入多次讀取）和物件鎖定提升安全性

了解更多 | [myQNAPcloud One](#)

具勒索軟體防護能力的備份

不可變性與隔離作為最後一道防線

在勒索軟體攻擊中，最大的風險通常是備份被刪除或篡改，導致無法復原。QNAP 透過不可變性和隔離雙重保護，確保資料無法被干預，即使管理員權限遭盜取，攻擊者也難以越權破壞已鎖定的備份副本。

不可變備份

對靜態備份資料強制執行不可變性，建立可信的復原基準，以對抗勒索軟體和人為操作錯誤。

不可變快照

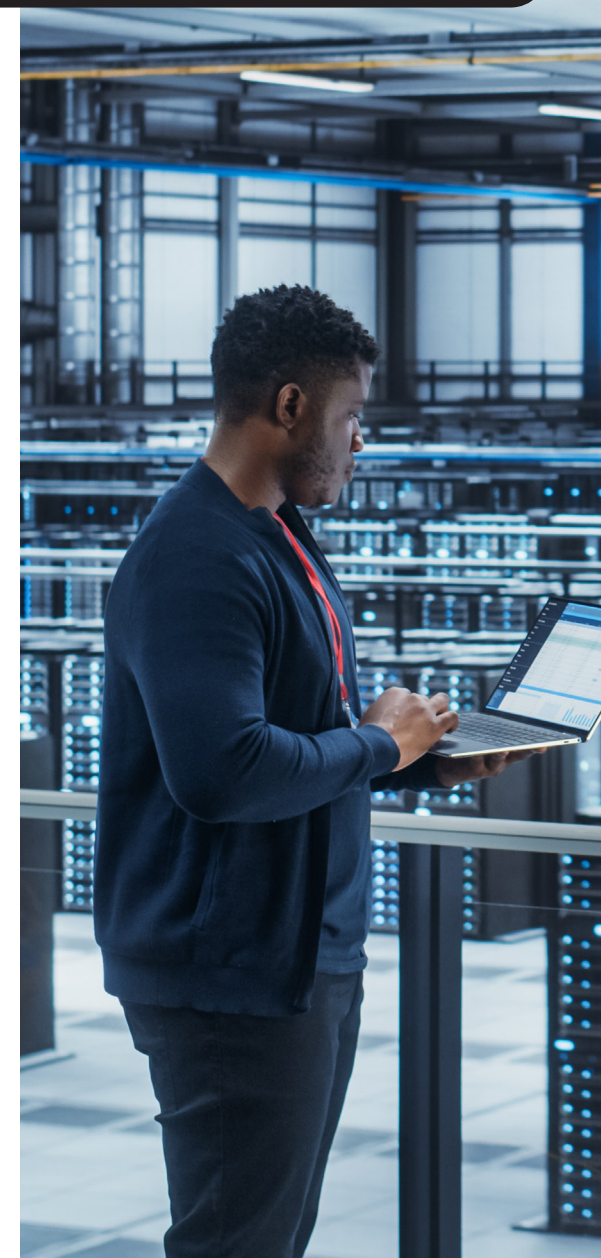
建立唯讀的時間點快照，保留資料狀態並支援快速回復，免於意外更改或勒索軟體的影響。

myQNAPcloud One

透過 WORM 和物件鎖定 (Object Lock) 技術，將不可變性擴充到雲端，支援長期的資料保留及合規性要求。

Airgap+

在非備份期間以實體與邏輯方式隔離備份目標，減少備份環境曝露於網路攻擊的風險。



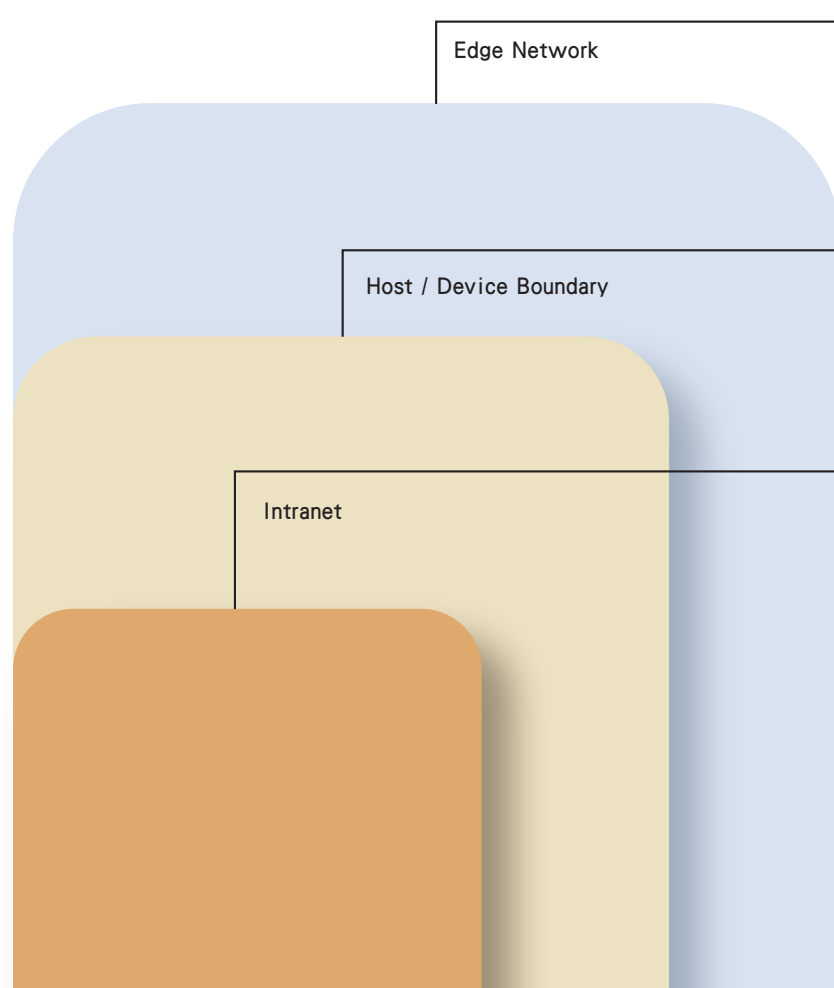
Backup

網路層面預防

在威脅擴大前阻止橫向移動

有效的資料保護應從網路層開始，這通常是多數攻擊首先取得立足點並開始蔓延的地方。QNAP NAS 與網路解決方案整合了異常偵測及回應、網路分段與隔離，以及安全連線架構，在攻擊升級之前遏制風險，將事件保持在可控範圍內。

Prevention



支援 IPS 特徵碼

QNAP QHora 路由器支援 IPS (入侵防禦系統)，可持續監測網路流量，在已知漏洞與攻擊模式生效前主動進行攔截。

QuFirewall + Ransomware Guard

於 NAS 本機端控管進出流量並攔截已知惡意行為，為儲存設備增設對抗勒索軟體威脅的第一道防線。

ADRA NDR (網路偵測與回應)

偵測並分析異常的內部流量與橫向移動行為，藉此識別受駭系統，並在威脅擴散前即時隔離。

VLAN

QNAP 交換器支援 VLAN 網路分段，以限制攻擊傳播並保護關鍵系統免遭橫向擴散。

系統層級保護

防止系統和權限遭濫用，以維持營運控制

面對勒索軟體與內部威脅，落實存取控制與防止資料篡改至關重要。藉由推行最小權限存取、管理職責分離，以及系統級的資料防護，企業可以大幅減少攻擊所帶來的營運衝擊。

存取控制



結合 Microsoft Entra ID 與 ACL 的 RBAC

整合 Entra ID (前身為 Azure AD) 與 Windows ACL 以落實基於角色的權限原則與存取控制。



委派管理

實施權責分離，將管理權限濫用與內部人員誤用的風險降至最低。



多重要素驗證 (MFA)

增加多層次驗證，嚴格防範未經授權的存取與憑證外洩。

NAS 系統保護



快照與版本控制

針對檔案意外更動或勒索軟體造成的衝擊，實現檔案與系統的快速復原。



Security Center

監控異常的檔案活動並偵測可疑行為，提供潛在威脅的早期預警。



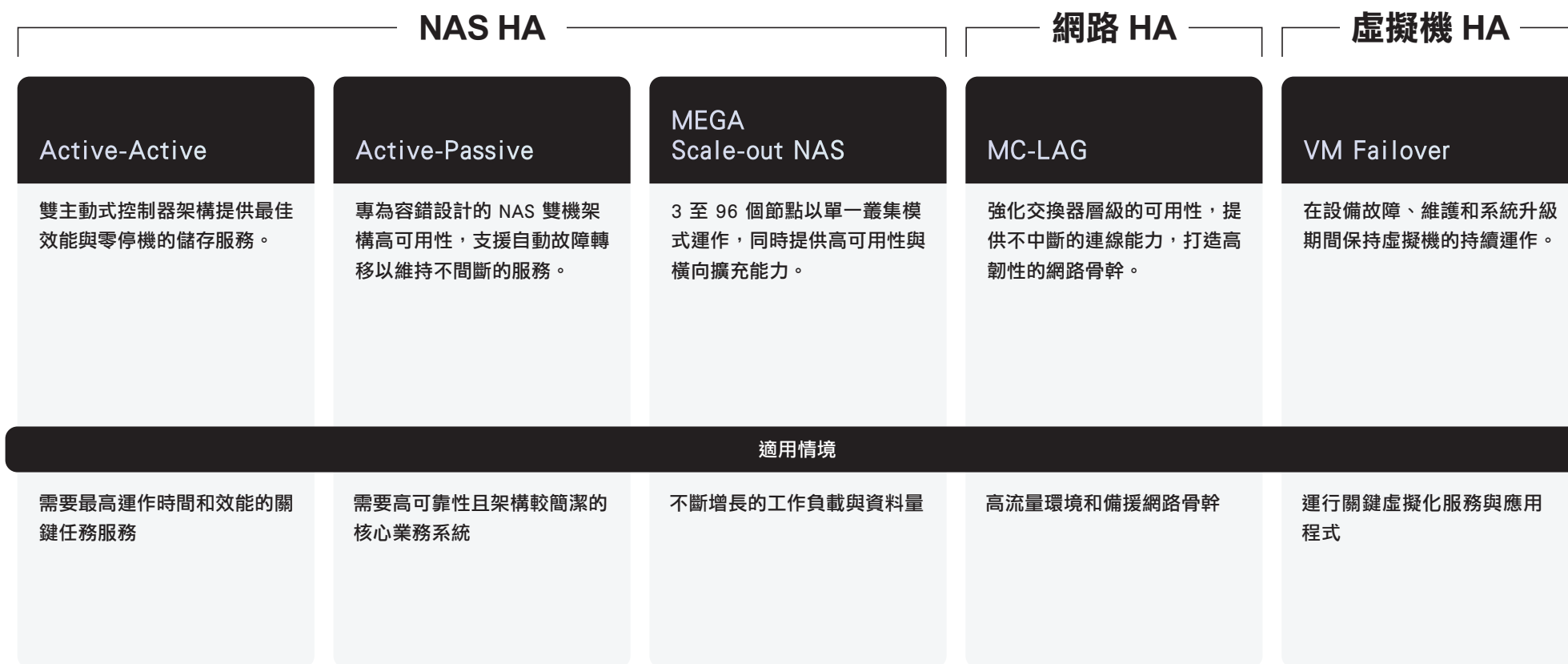
資料不可變性

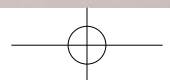
落實資料不可變性，防止未經授權的加密行為。
(前往第 9 頁了解更多)

高可用性 (HA)

提供多樣化的 HA 部署模式，確保企業營運持續不間斷

雖然備份和保護可以減少資料遺失，但 HA 確保業務營運從一開始就不需停擺。QNAP 支援多種高可用性架構，企業可根據任務要求、效能需求及規模，選擇合適的叢集備援架構。

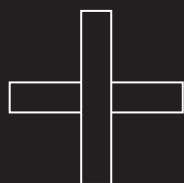




QNAP 的 1 + 3 資料保護

高度整合了從端點安全性到極速復原的多層次防護，是企業落實資料管理與資安韌性的最佳整合式首選。

備份
與復原



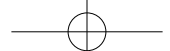
預防

保護

可用性

立即聯絡我們 
預約客製化展示或免費諮詢





QNAP



資料保護解決方案

建構具備勒索軟體防護能力的架構並確保業務連續性

QNAP Systems, Inc.

New Taipei City
Email: sales@qnap.com
Tel: +886 2 2641 2000

QNAP Inc. (USA)

Pomona CA
Email: usasales@qnap.com
Tel: +1-909-595-2782

QNAP Inc. (Canada)

Markham, Ontario
Email: canadasales@qnap.com
Tel: +1-905-947-1000

QNAP GmbH (Germany)

Willich
Email: desales@qnap.com
Tel: +49-2154-88428-0

QNAP SRL (Italy)

Roma
Email: eusales@qnap.com
Tel: +39-(0)687-738456

QNAP UK Limited

Swindon
Email: uksales@qnap.com
Tel: +44-(0)333-344-2522

QNAP Japan

Tokyo
Email: jpsales@qnap.com
Tel: +81-3-5901-9735

QNAP Korea

Seoul
Email: krsales@qnap.com

P/N: 51000-025610-RS | 202603 (CHT)A