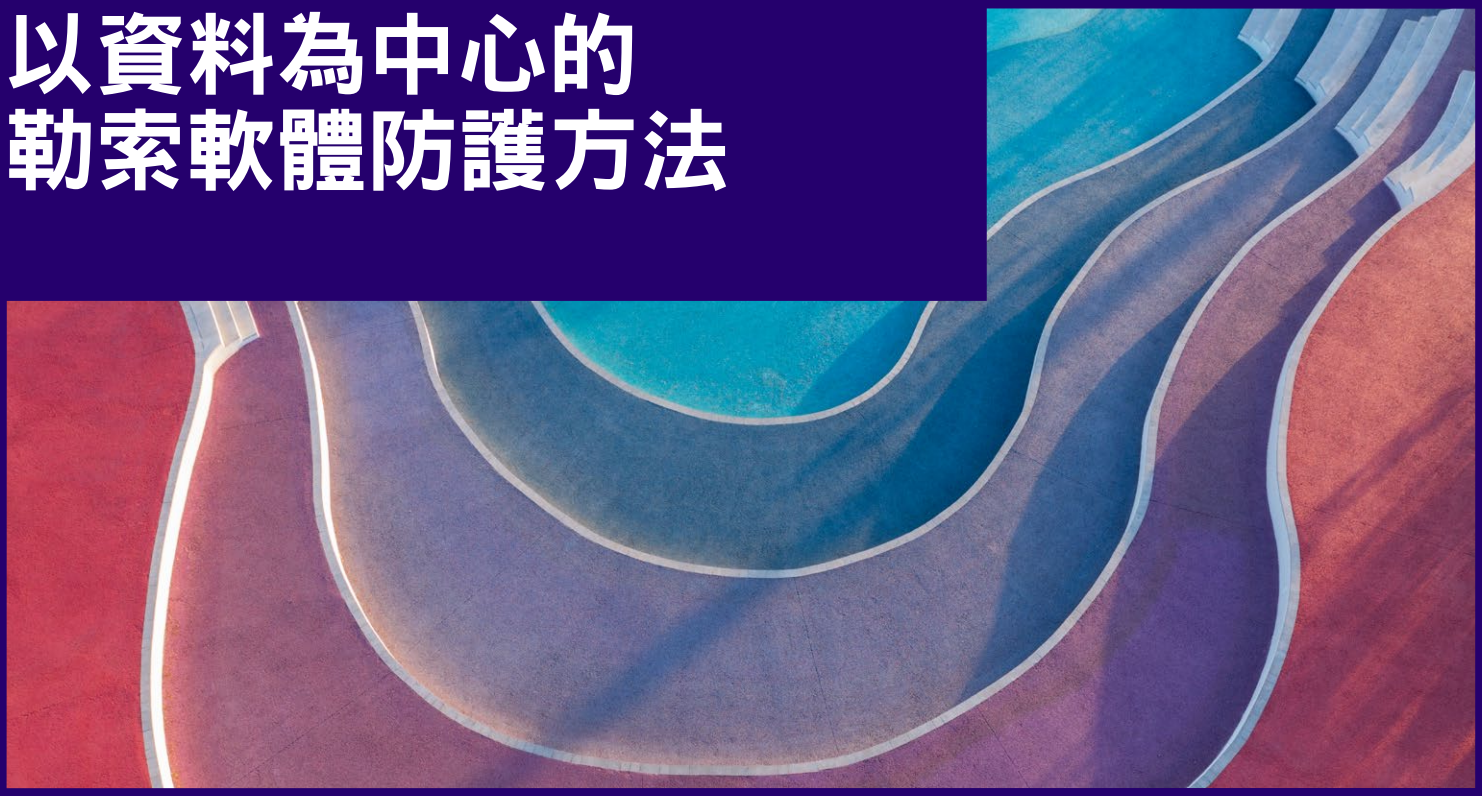
解決方案簡介

防護，偵測，恢復
以資料為中心的勒索軟體防護方法



保護：保護環境安全
偵測：預測威脅
恢復：快速恢復

當今企業所面臨的挑戰
勒索軟體攻擊對各種規模的組織來說，都是日益普遍且複雜的威脅。這些惡意攻擊會加密重要資料，並要求支付放行費用，通常會造成重大財務損失和營運中斷。

- 網路事故是全球第一的商業風險。
- 到 2031 年，勒索軟體預計每 2 秒就會發動攻擊一次。
- 去年有 59% 的組織受到勒索軟體的影響。
- 勒索軟體攻擊從 2022 年至 2023 年增加了 73%。

雖然許多企業都著重於網路和端點安全性，但重要的是，不能忽略保護資料所在儲存層的重要性。透過在儲存層實作強大的安全措施，例如加密、存取控制和不可變的備份，您可以建立更多防線來對抗勒索軟體。

這種方法有助於保護資料來源，使攻擊者更難加密或毀損重要資訊。安全儲存解決方案可協助加快還原時間，並在攻擊成功時將資料遺失降至最低，這也突顯了包括強化儲存基礎架構在內的全方位安全策略的重要性。

NetApp 網路恢復能力：以資料為中心的勒索軟體防護方法

防範網路事件必須包含多層次防禦措施，才能防範各種威脅。強大的網路防禦功能從**身分識別安全**層開始，除了最外層的**周邊安全**措施外，這是第一道防線。

網路安全性建立在此基礎之上，可保護傳輸中的資料，並偵測內部網路內的異常活動。**端點安全性**則為連線至網路的個別裝置增加一層防禦。**應用程式安全性**著重於保護軟體應用程式免除弱點和攻擊。

最後，安全態勢的核心是**資料安全性**，用以保護組織最寶貴的資產，包括資料和最重要的任務資產。此層通常包含資料保護功能，並提供強大的備份與還原解決方案。

這些互連的安全層結合在一起，將組成一套全方位的防禦策略，旨在保護企業的數位資產，使其免受周邊環境和資料中心的威脅，同時解決 IT 基礎架構各個層級的威脅。

關鍵任務資產的資料層保護更為重要，而且具有獨特的需求。為了有效運作，此層的解決方案必須提供以下四項關鍵屬性：

- 透過設計來保護安全，將成功攻擊貴組織的機會降至最低。
- 即時偵測與回應，將攻擊成功的影響降到最低。
- 氣隙式單讀多寫（WORM）保護，以隔離關鍵資料備份。
- 簡單的控制面板，提供全方位的勒索軟體保護與快速恢復。

NetApp 可在資料層進行偵測、保護及恢復。

安全可靠的設計：儲存方案原生內建的 ONTAP 勒索軟體防護

NetApp ONTAP 軟體透過安全的設計方法，提供強大的勒索軟體防護。核心功能包括不可變更且不可刪除的 Snapshot 快照複本，即使是系統管理員也無法變更資料，因此可建立可靠的還原點。ONTAP FPolicy 功能可封鎖惡意檔案，防止威脅在系統內擴散，進而增強安全性。

主要優勢

- **融入安全考量的設計：**儲存層內建資料保護功能。
- **即時偵測並回應：**AI 驅動的勒索軟體防禦。
- **Cyber Vault：**不可改變且無法磨滅的備份。
- **統一化控制平台：**從偵測到恢復，智慧協調所有保護機制。
- **恢復保證：**NetApp Snapshot 複本不會遺失資料。

為了強化存取控制，多管理員驗證要求多位管理員核准後才能執行關鍵動作，以降低內部威脅或認證遭入侵的風險。而多因素驗證則增加額外的安全層級，只有獲授權的人員才能存取敏感資料和系統。

即時偵測並回應

除了強大的勒索軟體防護功能之外，NetApp 還利用 ONTAP 內建的 AI 自主技術，提供 99% 準確度和近乎即時回應能力的即時偵測。這項進階偵測功能可持續監控可疑活動和異常狀況，在 Amazon FSX for ONTAP 的檔案、區塊和原生雲端上迅速識別可能的勒索軟體攻擊。一旦偵測到威脅，系統便會自動隔離受影響的資料，並防止進一步擴散，將潛在損害降至最低。

NetApp Data Infrastructure Insights（DII）提供額外的防禦層級，可抵禦內部威脅。它會偵測潛在的異常使用者行為，並立即採取行動，例如封鎖使用者存取儲存系統及拍攝快照。此外，DII 還提供詳細分析，以供鑑識分析和稽核。這套全方位方法結合主動式威脅偵測、快速回應機制，以及詳細的使用者活動監控，將提供多層面的防護措施，以便有效防範外部勒索軟體攻擊和內部威脅。

圖 1：NetApp 提供全球最安全的資料儲存方案，並提供多層防禦功能，以智慧且高效的方式保護您的資料，包括透過端點對端點加密、多因素驗證及角色型存取控制來存取資料。

隔離式備份，用於網路拖運

NetApp Cyber Vault 採用 SnapLock® 法規遵循軟體，為企業組織提供全方位且靈活的解決方案，以保護最重要的資料資產。ONTAP 的邏輯氣隙與堅實的強化方法，可讓您建立安全且隔離的儲存環境，以因應不斷演變的網路威脅。有了 NetApp，您就能對資料的機密性、完整性和可用度充滿信心，同時維持儲存基礎架構的敏捷度和效率。

為了提高安全性，NetApp 可讓您建立額外的資料保護層：

- 安全隔離的儲存基礎架構（例如，氣隙隔離的儲存系統）
- 備份資料的複本，不僅不可改變，也不可
- 嚴格的存取控制與多因素驗證
- 快速資料還原功能
- SnapLock 採用 WORM 技術，可防止資料遭到加密及刪除，並提供不會毀壞且省空間的資料複本

簡單但強大的控制面板

NetApp 是唯一提供單一控制面板與 NetApp BlueXP™ 的儲存廠商，可智慧地協調及執行以工作負載為中心的端點對端點勒索軟體防禦技術。有了這些技術，您只要按一下滑鼠，就能**識別並保護**關鍵工作負載資料，準確且自動地**偵測並回應**，以限制潛在攻擊的影響程度，並在幾分鐘內**恢復**工作負載，而不需幾天或幾個月，保護您寶貴的工作負載資料，並將業務中斷的成本降至最低。

BlueXP 勒索軟體防護協調程式將 NetApp ONTAP 的強大功能與 BlueXP 資料服務結合在一起，利用自動化工作流程來新增人工智慧和機器學習建議與指引，協助您：

- **識別**：自動識別 NetApp 儲存環境中的工作負載（虛擬機器、檔案共享、資料庫）及其資料、將資料對應至工作負載、判定工作負載的重要性，並分析工作負載風險。
- **防護**：向您建議工作負載保護原則，只要按一下滑鼠即可套用。

- **偵測**：透過領先業界的機器學習型偵測功能，以近乎即時的方式偵測工作負載資料是否可能遭受攻擊。
- **回應**：如果發現疑似的可能攻擊行動，就會建立無法變更及刪除的 Snapshot 快照複本，提供近乎即時的自動回應。
- **恢復**：驗證備份完整性，識別最佳恢復點，並透過簡化、協調完善、與應用程式一致的恢復功能，快速恢復工作負載及其相關資料。

「我們最近剛遇到勒索軟體事件，當我們看到 Cloud Insights 勒索軟體偵測所提供的資訊時，我們佩服得五體投地。」

運輸公司 IT 總監

BlueXP 勒索軟體防護協調程式提供全方位的解決方案，協助您做好勒索軟體防護準備，回應攻擊，並引導您完成恢復，藉此免除因為保護工作負載免於勒索軟體相關停機和資料遺失所致的負擔與焦慮。只有 NetApp 能讓您高枕無憂，因為一旦發生攻擊，您就會立即知道，您寶貴的工作負載資料已受到周全保護，而且恢復作業會更輕鬆快速，如此一來，企業營運中斷就能降至最低。

NetApp 的勒索軟體防護功能可協助您識別及保護資料所在位置，準確且自動地偵測及回應，以限制潛在攻擊的影響程度，並在幾分鐘內恢復資料，而不需幾天或幾個月。這項功能有助於保存您寶貴的資料，並將網路恢復作業所造成的業務中斷成本降至最低。

勒索軟體可能會擊垮不認真看待此事的企業。只有 NetApp 以資料為中心的網路恢復方法，才能為主要和次要資料提供全方位的整合式安全保護，並保證協助您恢復。

深入瞭解 NetApp BlueXP 勒索軟體保護

NetApp 台灣
台北市 110 信義區松仁路 97 號 8 樓之 2 電話：886 2 8729 5000 傳真：886 2 8729 5050

聯絡業務人員

關於 NetApp

NetApp 是一家智慧型資料基礎架構公司，結合統一化資料儲存、整合式資料服務及 CloudOps 解決方案，將顛覆變動的世界轉化為每位客戶的大好商機。NetApp 打造無封閉環境的基礎架構，利用觀察能力及人工智慧來實現業界最理想的資料管理。我們的資料儲存服務，是唯一原生內嵌在全球各大公有雲中的企業級儲存服務，可提供無縫接軌的操作彈性。此外，我們的資料服務透過卓越的網路恢復能力、治理功能和應用靈活度，來協助您建立起資料優勢。我們的 CloudOps 解決方案透過優異的觀察能力及人工智慧，能夠持續最佳化效能與效率。無論資料類型、工作負載，或環境為何，您都可以利用 NetApp 來推動資料基礎架構轉型，實現更多商業契機。**www.netapp.com**