

# NETAPP 勒索軟體的 復原能力



即時偵測勒索軟體攻擊，防止資料遺失，快速恢復，並最大限度地減少對業務的影響

## 您準備好應對勒索軟體攻擊了嗎？

應對勒索軟體攻擊的關鍵方面是保護儲存層（最後一道防線）的工作負載資料。隨著攻擊變得越來越複雜、自動化和昂貴，阻止勒索軟體攻擊是不切實際的。當攻擊者入侵時你必須做好準備。

僅靠備份是不夠的。您需要能夠評估關鍵工作負載資料的風險、偵測威脅並即時回應。您還需要制定可以快速輕鬆執行的恢復計畫。然而，有效抵禦勒索軟體攻擊是一項營運負擔，需要完成許多容易出錯的手動任務，而且擁有必要專業知識的員工太少。

如果您沒有實施應有的安全計畫，針對您的工作負載的攻擊將無法被偵測到，並且您的回應將會延遲。工作負載恢復將非常複雜——平均需要 7 天<sup>1</sup> ——並且您的資料甚至可能無法完全恢復。不只成效不足，反應也太慢了。

## 以全方位保護作為最後一道防線

NetApp® 勒索軟體復原服務使您能夠快速輕鬆地執行安全計畫，從預防到偵測、回應和復原。

勒索軟體恢復方案提供單一介面來智慧地協調以工作負載為中心的勒索軟體防禦。只需點擊幾下，您就可以識別並保護處於危險中的關鍵工作負載資料。該服務還能準確、自動地偵測和回應潛在的攻擊並限制其影響。您可以在幾分鐘內恢復工作負載，不受惡意軟體的影響，保護您寶貴的資料並最大限度地減少對您的業務造成的損害和中斷成本。

勒索軟體恢復功能將 NetApp ONTAP® 軟體的強大功能與 NetApp 資料服務結合，透過自動化工作流程添加智慧建議和指導，以：

- 確認**。自動識別NetApp儲存裝置中的工作負載（虛擬機器、檔案共用、熱門資料庫）及其資料，將資料對應至工作負載，並確定資料的敏感度、重要性和風險。
- 防護**，取得工作負載保護策略的建議並一鍵套用。
- 偵測**，即時檢測可疑文件和用戶行為活動，這可能預示著潛在的資料外洩嘗試以及文件加密和大規模刪除嘗試。
- 回應**。當懷疑有潛在攻擊時，透過自動建立NetApp Snapshot™ 副本並阻止使用者來保護工作負載。該服務還與業界領先的安全資訊和事件管理 (SIEM) 解決方案整合。
- 恢復**，透過簡單、協調的復原過程快速恢復工作負載及其相關資料。透過使用隔離的復原環境，您可以獲得乾淨、無惡意軟體的資料復原。
- 治理**。實作您的勒索軟體防護策略與原則，並監控施行成果。

### 準備攻擊：節省時間並提高效率

勒索軟體恢復功能可自動識別NetApp儲存體中的資料類型、將資料對應到特定工作負載、評估資料敏感度和關鍵性並分析風險。此過程減少了您對複雜的手動分析、額外的第三方工具和專業知識的依賴。

## 主要優勢

在最後一道防線獲得全面、精心策劃的保護：

- 全面了解您的工作負載保護狀況。
- 儘早發現攻擊並防止資料遺失。
- 快速且無惡意軟體地恢復整個工作負載，以最大限度地減少中斷、成本、收入損失和業務損害。
- 取得資料進行鑑識分析並提出建議以改善您的安全態勢。

然後，勒索軟體恢復功能會使用 ONTAP 功能提出智慧保護策略，包括具有 AI (ARP/AI) 異常檢測的 NetApp 自主勒索軟體保護、FPolicy 惡意擴充封鎖和防篡改 Snapshot 副本。勒索軟體恢復功能也會根據資料資產的敏感度和關鍵性客製化保護建議。

只需按一下滑鼠，便能將防護原則無縫且一致地套用到您的工作負載資料。勒索軟體恢復功能是在背景運行，以配置 ONTAP 和 NetApp 資料服務功能並協調每個 Volume 的保護工作流程，從而減少重複手動任務的需要。

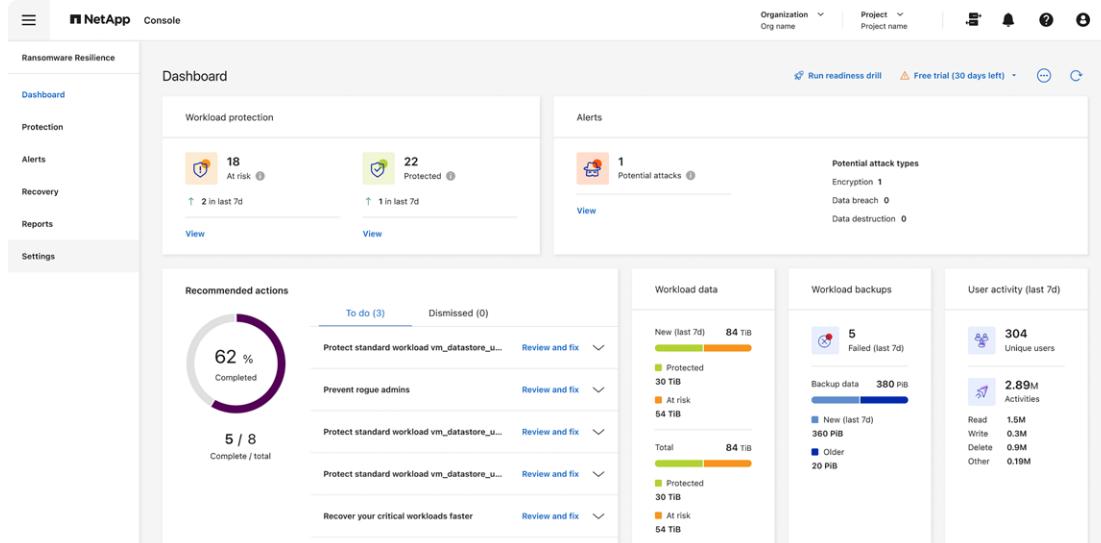
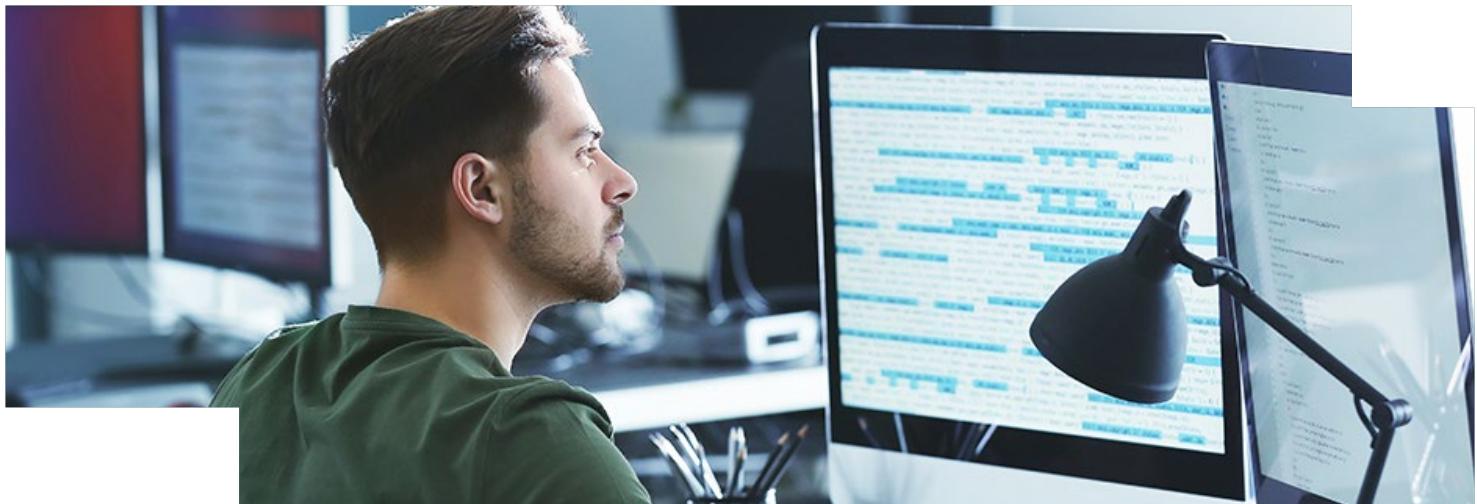


圖 1：NetApp 勒索軟體復原服務透過單一控制平面提供全面、協調的以工作負載為中心的勒索軟體防禦，從偵測到復原。



## 即時偵測並回應威脅

勒索軟體恢復功能持續監控可疑檔案和使用者行為異常。它可以透過識別早期用戶行為來檢測資料洩露，這些行為可能預示著潛在的資料外洩嘗試以及檔案加密和大規模刪除嘗試。當懷疑發生攻擊時，勒索軟體恢復功能會建立快照副本以防止資料遺失，並阻止實施攻擊的使用者以阻止他們並防止進一步的攻擊。

該服務在您的主儲存設備上使用創新的、先進的、基於人工智慧的勒索軟體檢測。這種方法意味著可以快速發現潛在的攻擊並立即緩解。

勒索軟體恢復功能提供事件報告以支援取證，並與業界領先的 SIEM 解決方案整合。

## 幾分鐘內輕鬆恢復工作負載

勒索軟體恢復功能協調所有相關工作負載資料的應用程式一致性復原工作流程，並讓您即時了解流程和狀態。快照副本可以在工作負載層級恢復，也可以在 Volume 或檔案層級更精細地恢復。

作為復原過程的一部分，勒索軟體復原提供了一個隔離的復原環境，可以隔離受感染的工作負載、刪除惡意軟體、推薦復原點並引導使用者完成直覺的復原過程。這種方法可以提供乾淨的、無惡意軟體的恢復，並防止資料再次感染。

## 將業務中斷減至最低

勒索軟體恢復功能消除了保護您的工作負載免受勒索軟體相關停機和資料遺失的負擔和焦慮。它提供全面的服務，可提高您的準備程度、應對攻擊並引導您完成恢復。只有選擇 NetApp，您才能高枕無憂，因為您知道，當攻擊發生時，您會立即收到警報，您寶貴的工作負載資料將受到保護，並且恢復將變得快速而簡單，從而最大限度地減少對您業務的干擾。

## 立即取得 NetApp 勒索軟體恢復方案

<sup>1</sup> ESG，2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation，2023 年 11 月。

本文件為機器翻譯，生成譯文僅供參考。若與英文版之間有任何矛盾或不一致之處，應以英文版內容為主。

#### 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 是一家智慧資料基礎設施公司，它結合了統一資料儲存、整合資料、營運和工作負載服務，將顛覆性的世界轉化為每個客戶的機會。NetApp 打造無封閉環境的基礎架構，利用觀察能力及人工智能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。我們的營運和工作負載服務透過可觀察性和人工智能持續優化基礎設施和工作負載的效能和效率。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。了解更多信息 [www.netapp.com](http://www.netapp.com) 或關注我們 [LinkedIn](#), [Facebook](#), 和 [Instagram](#)。