

# NETAPP BLUEXP 勒索軟體防護



提供所需的智慧功能及協助，盡可能減少工作負載資料損失並快速恢復

## 您準備好應對勒索軟體攻擊了嗎？

準備好應對勒索軟體且能快速恢復，是當今的必備能力，而非一種選擇。現在的攻擊日漸精密複雜，都透過自動化程序引發，並造成更慘重的損失。想要防止零時差漏洞和憑證盜竊是不切實際的，更務實的做法是在攻擊者入侵時做好防禦準備。

做好準備，意味著必須在最後一道防線的儲存層，為您的工作負載資料提供周全保護。但光有備份還不夠，您還需要瞭解關鍵工作負載資料可能存在的風險，有能力快速偵測威脅並立即因應，同時擬定在您面對壓力時也能快速輕鬆執行的恢復計畫。但實現這些目標的營運負擔相當沉重，因為容易出錯的手動任務太多，可用的人力也不足。

然而未能達成這些要求，就無法發現對您工作負載發起的攻擊，進而造成延誤回應；此外，工作負載的恢復作業極其複雜，平均需要 7 天<sup>1</sup> 才能完成，而且不是所有資料都能恢復。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 推出 NetApp® BlueXP™ 勒索軟體防護方案，並且是唯一提供單一控制台的儲存廠商，讓您能夠輕鬆運用智慧科技來協調及執行以工作負載為中心的全方位勒索軟體防護。只需點擊幾下，就能識別和保護您處於風險之中的關鍵工作負載資料，準確且自動地偵測及回應潛在攻擊，限制其造成的影響。您也能在幾分鐘內恢復工作負載，保護寶貴的工作負載資料，將代價高昂的營運中斷減到最少。

BlueXP 勒索軟體防護結合了 NetApp ONTAP® 軟體的強大功能與 BlueXP 的資料服務，再加入智慧建議和指導，並透過自動化工作流程完成下列工作：

- **識別**：自動識別 NetApp 儲存設備之中的工作負載（虛擬機器、檔案共用、常用資料庫）及其資料，將資料對應至工作負載，判斷工作負載的重要性，並分析工作負載風險。
- **保護**：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、以機器學習 (ML) 為基礎的偵測功能，近乎即時地偵測工作負載資料可能遭受的攻擊。
- **回應**：如果發現疑似的可能攻擊，就會建立無法變更及刪除的 NetApp 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。
- **控管**：實作您的勒索軟體防護策略與政策，並監控施行成果。

### 使用勒索軟體輔助準備工作來節省時間並改善效率

BlueXP 勒索軟體防護會自動識別 NetApp 儲存設備中的資料類型，將資料對應至工作負載，判斷工作負載的重要性，並分析工作負載風險。這些功能可減少組織對複雜的手動分析、專業技能和多重第三方工具的需求。

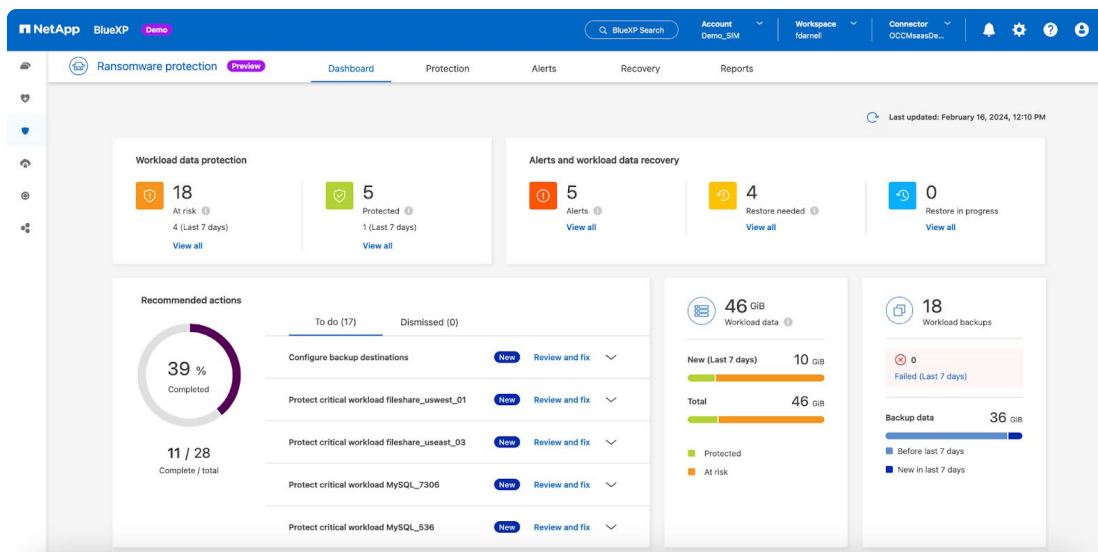
BlueXP 勒索軟體防護會建議即時可用的智慧防護原則，使用領先業界的 ONTAP 功能，包括省空間且無法變更及刪除的 Snapshot

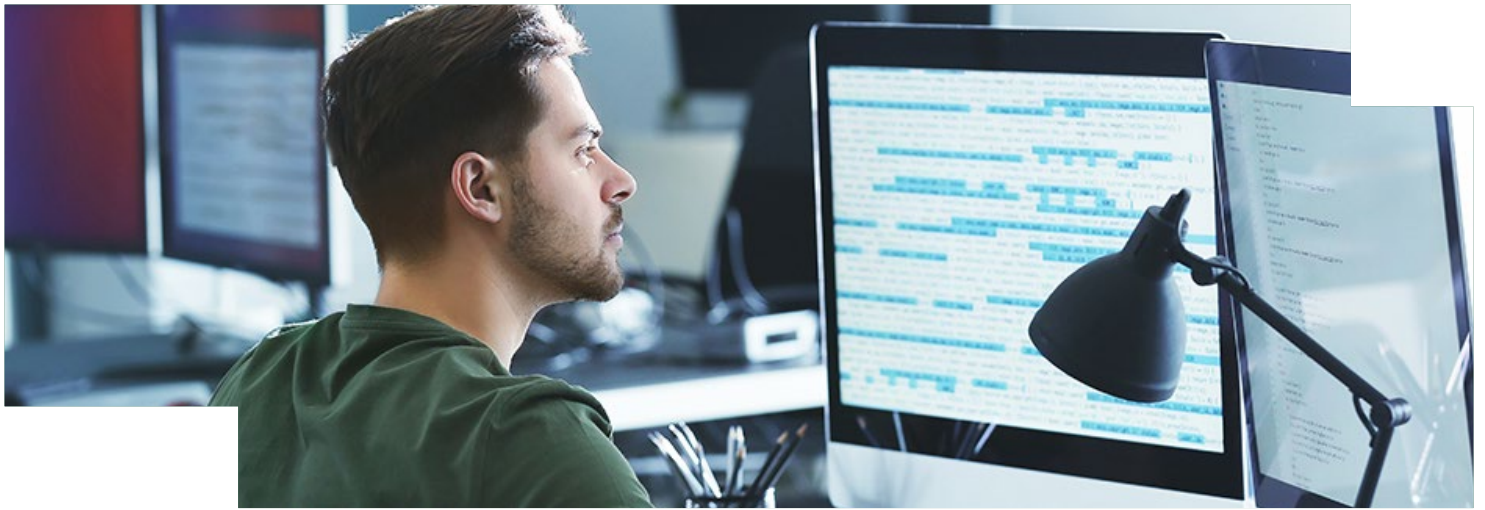
## 主要優勢

- 充當最後一道防線的全方位保護：除了備份，也涵蓋美國國家標準與技術研究所 (NIST) 網路安全架構的所有六大領域
- 以工作負載為中心並與應用程式一致的解決方案
- 提供已排定優先順序的智慧型建議
- 自動化及引導式行動
- 早期威脅偵測
- 快速恢復完整工作負載，並可選擇精細還原（依據 Volume 或檔案）

快照複本、在一線及二線儲存設備上的 Snapshot 複本鎖定、FPolicy 惡意擴充封鎖和自主勒索軟體防護異常偵測。為了得到最佳的投資報酬，BlueXP 勒索軟體防護也會根據工作負載的重要性而調整防護建議。

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。BlueXP 勒索軟體防護在背景運作，對 ONTAP 和 BlueXP 功能進行設定，並協調每個關聯 Volume 之間的防護工作流程，從而減少重複手動任務的需要。





### **部署以機器學習為基礎的異常偵測功能，提高正確性並加速回應以遏止風險**

BlueXP 勒索軟體防護會持續監控異常，並自動防止攻擊造成進一步的影響。當懷疑存在潛在攻擊時，它會建立無法變更及刪除的 Snapshot 快照複本，將對於正常作業的干擾減到最少。

此服務另一項創新之處在於，除了對主儲存設備使用以 AI / 機器學習為基礎的進階勒索軟體偵測之外，也會對二線儲存設備進行偵測，因此能快速發現並立即緩解對正式作業資料的潛在攻擊。

此外，也會提供事件報告，整合了安全資訊和事件管理 (SIEM) 來支援攻擊鑑識。

### **使用與應用程式一致的引導式還原，在幾分鐘內更輕鬆地恢復工作負載**

BlueXP 勒索軟體防護會根據您的恢復選擇，判斷哪個 Snapshot 快照複本或備份可提供最佳的實際恢復點 (RPA)，並能在工作負載層級或更精細的層級 (Volume 或檔案) 進行恢復。

BlueXP 勒索軟體防護會協調工作流程，將所有關聯工作負載資料恢復至與應用程式一致，還能讓您掌握即時恢復狀態，以加速恢復並促進成功。

### **將業務中斷減至最低**

BlueXP 勒索軟體防護可保護工作負載免受勒索軟體相關停機和資料遺失的影響，為您卸下負擔並消除焦慮。您將獲得全方位解決方案，可以提高您的勒索軟體防禦能力、迅速回應攻擊並引導您完成恢復作業。只有 NetApp 能讓您高枕無憂，因為發生攻擊時您將立即收到警報，您寶貴的工作負載資料將受到保護，同時能更輕鬆快速恢復，將業務中斷減至最低。

### **▶ 現在就取得 BlueXP 勒索軟體防護**

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

## 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 解決方案可透過觀察能力及人工智慧，持續優化效能與效率。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。如欲深入瞭解，請參訪 [www.netapp.com.tw](http://www.netapp.com.tw)，或在 [Twitter](#)、[LinkedIn](#)、[Facebook](#) 及 [Instagram](#) 關注我們。

