發行說明
NetApp Ransomware Resilience

NetApp
February 27, 2026

目錄

發行說明

NetApp Ransomware Resilience的新功能

了解NetApp Ransomware Resilience的新功能。

2026 年 2 月 16 日

Azure NetApp Files 支援

Ransomware Resilience 現已支援 Azure NetApp Files 系統，使您能夠有效率地偵測和應對 Azure NetApp Files 中的勒索軟體威脅。當您發現工作負載時，Ransomware Resilience 現在會呈現 Azure NetApp Files 並在保護儀表板中顯示。Ransomware Resilience 對 Azure NetApp Files 的支援僅包括使用快照的偵測和保護策略。對 Azure NetApp Files 的支援目前處於預覽階段。

如需詳細資訊，請參閱 "了解勒索軟體抵禦能力"。

將使用者從使用者行為警示中排除

NetApp Ransomware Resilience 現已允許您將特定使用者從使用者行為警報中排除。排除受信任的使用者可以防止誤報和不必要的警報。

如需詳細資訊，請參閱 "將使用者排除在警示範圍之外"。

使用者行為活動的保護群組支援

Ransomware Resilience 防護群組現在支援可疑使用者行為偵測的偵測原則。將勒索軟體防護策略套用至防護群組時,它會在工作負載之間套用原則,簡化網路安全態勢的管理。

如需詳細資訊，請參閱 "建立保護組"。

2026年1月19日

不支援的捲

Ransomware Resilience 報告現在會在 **Summary** 報告中記錄受支援和不受支援的磁碟區的資訊。使用此資訊可以診斷系統中的磁碟區為何可能不符合勒索軟體防護條件。

有關詳細信息，請參閱 "下載勒索軟體復原力報告"。

2026年1月12日

將快照複製到**ONTAP**

Ransomware Resilience 現已支援將快照複製到輔助 ONTAP 網站。使用複製策略的保護群組，您可以為每個工作負載複製到相同或不同的目標位置。您可以建立包含複製功能的勒索軟體防護策略，也可以使用預先定義的策略。

有關詳細信息，請參閱 "在勒索軟體復原中保護工作負載"。

將工作負載排除在勒索軟體復原能力之外

勒索軟體復原功能現在支援將系統中的特定工作負載從保護範圍和勒索軟體復原儀表板中排除。發現工作負載後，您可以將其排除在外；如果您想要添加勒索軟體防護，則可以重新將其包含在內。排除在外的工作負載無需付費。

有關詳細信息，請參閱 "排除工作負載"。

標記提醒，如正在審核中

勒索軟體復原功能現在允許您將警報標記為「審核中」。使用「審核中」標籤可以提高團隊在對活躍的勒索軟體威脅進行分類和管理時的清晰度。

有關詳細信息，請參閱 "管理勒索軟體復原能力中的警報"。

2025年12月8日

擴充功能阻止功能已在工作負載層級啟用。

啟用擴充封鎖功能後，現在是在工作負載層級而不是儲存虛擬機器層級啟用此功能。

編輯使用者行為警報狀態

勒索軟體復原功能現在允許您編輯使用者行為警報的狀態。您可以手動關閉和解決警報。

有關詳細信息，請參閱 "管理勒索軟體復原能力中的警報"。

支援多個控制台代理

勒索軟體復原功能現在支援使用多個控制台代理程式來管理相同系統。

有關控制台代理的更多信息，請參閱"建立控制台代理"。

2025年11月10日

此版本包含一般增強與改進。

2025年10月6日

BlueXP ransomware protection現已升級NetApp Ransomware Resilience

BlueXP ransomware protection服務已更名為NetApp Ransomware Resilience。

BlueXP現在是NetApp Console

NetApp Console提供企業級跨本地和雲端環境的儲存和資料服務的集中管理，提供即時洞察、更快的工作流程和簡化的管理。

有關更改的詳細信息，請參閱 "NetApp Console發行說明"。

資料外洩檢測

勒索軟體復原力包括一種新的檢測機制，只需幾個步驟即可激活，以檢測異常用戶讀取作為資料外洩的早期指標。勒索軟體彈性透過建立歷史基線來收集和分析使用者讀取事件，該基線是根據過去資料得出的預期正常行為的概況。當新用戶活動明顯偏離既定規範（例如意外的閱讀激增與可疑的閱讀模式相結合）時，就會產生警報。勒索軟體復原力包括一個用於偵測可疑讀取模式的 AI 模型。

與儲存層的 ARP 加密偵測不同，勒索軟體彈性 SaaS 服務透過收集 FPolicy 事件來偵測使用者行為異常。

> 您必須使用新的"勒索軟體恢復用戶行為管理員和勒索軟體恢復用戶行為檢視器"角色來存取可疑用戶行為檢測設定。

有關詳細信息，請參閱"啟用可疑用戶活動偵測"和"查看異常用戶行為"。

其他可疑用戶活動檢測

除了資料外洩偵測之外，勒索軟體復原能力還根據觀察到的可疑使用者活動偵測以下警報類型：

- 資料破壞 - 潛在攻擊 - 當檔案刪除的數量超過歷史標準時，會建立具有潛在攻擊嚴重程度的警報。
- 可疑使用者行為 - 潛在攻擊 - 當觀察到類似於勒索軟體攻擊的讀取、重新命名和刪除操作時，會建立嚴重程度為潛在攻擊的警報
- 可疑使用者行為 - 警告 - 當檔案活動（讀取、刪除、重新命名等）的總數超過歷史標準時，將建立嚴重程度為警告的警報

用於資料外洩偵測的新使用者角色

為了管理可疑使用者活動警報，Ransomware Resilience 為控制台組織管理員引入了兩個新角色，以授予對可疑使用者活動偵測的存取權：Ransomware Resilience 使用者行為管理員和 Ransomware Resilience 使用者行為檢視器。

您必須是使用者行為管理員才能配置可疑使用者行為設定。勒索軟體復原管理員角色不支援配置可疑使用者行為設定。

有關更多信息，請參閱"NetApp Ransomware Resilience基於角色的訪問" 。

2025年8月12日

此版本包含一般增強與改進。

2025年7月15日

SAN 工作負載支持

此版本包括對BlueXP ransomware protection中的 SAN 工作負載的支援。現在，除了 NFS 和 CIFS 工作負載之外，您還可以保護 SAN 工作負載。

有關詳細信息，請參閱"BlueXP ransomware protection先決條件" 。

改進的工作負載保護

此版本改進了具有其他NetApp工具（如SnapCenter或BlueXP backup and recovery）的快照和備份策略的工作負載的設定過程。在先前的版本中， BlueXP ransomware protection發現了來自其他工具的策略，只允許您更改偵測策略。在這個版本中，您現在可以用BlueXP ransomware protection策略取代快照和備份策略，或繼續使用其他工具中的策略。

有關詳細信息，請參閱"保護工作負載"。

電子郵件通知

如果BlueXP ransomware protection偵測到可能的攻擊， BlueXP通知中會出現通知，並且會向您設定的電子郵件地址發送電子郵件。

電子郵件包含有關嚴重性、受影響的工作負載的信息，以及BlueXP ransomware protection*警報* 標籤中的警報連結。

如果您在BlueXP ransomware protection中配置了安全性和事件管理 (SIEM) 系統，該服務會向您的 SIEM 系統發送警報詳細資訊。

有關詳細信息，請參閱"處理偵測到的勒索軟體警報"。

2025年6月9日

著陸頁更新

此版本包括對BlueXP ransomware protection登陸頁面的更新，使開始免費試用和發現變得更加容易。

準備演習更新

以前，您可以透過模擬對新樣本工作負載的攻擊來執行勒索軟體準備演練。利用此功能，您可以調查模擬攻擊並恢復工作負載。使用此功能來測試警報通知、回應和恢復。根據需要經常運行和安排這些演習。

在此版本中，您可以使用BlueXP ransomware protection儀表板上的新按鈕在測試工作負載上執行勒索軟體準備演練，從而更輕鬆地模擬勒索軟體攻擊、調查其影響並有效地恢復工作負載，所有這些都在受控環境中完成。

現在，除了 NFS 工作負載之外，您還可以在 CIFS（SMB）工作負載上執行準備情況演練。

有關詳細信息，請參閱 "進行勒索軟體攻擊準備演習"。

啟用**BlueXP classification**更新

在BlueXP ransomware protection服務中使用BlueXP classification之前，您需要啟用BlueXP classification來掃描您的資料。將資料分類有助於您找到個人識別資訊 (PII)，這可能會增加安全風險。

您可以在BlueXP ransomware protection中對文件共享工作負載部署BlueXP classification。在*隱私暴露*欄中，選擇*識別暴露*選項。如果您已啟用分類服務，此操作將識別曝光。否則，在此版本中，對話方塊會顯示部署BlueXP classification的選項。選擇*部署*前往BlueXP classification服務登入頁面，您可以在其中部署服務。西

如需詳細資訊、請參閱 "在雲端部署BlueXP classification"、若要在 BlueXP ransomware protection 中使用服務、請參閱 "使用BlueXP classification掃描個人識別資訊"。

2025年5月13日

BlueXP ransomware protection中不支援的工作環境報告

在發現工作流程期間，當您將滑鼠懸停在「支援」或「不支援的工作負載」上時， BlueXP ransomware protection會報告更多詳細資訊。這將幫助您了解為什麼您的某些工作負載未被BlueXP ransomware protection服務發現。

服務不支援工作環境的原因有很多，例如，工作環境中的ONTAP版本可能低於所需的版本。當您將滑鼠懸停在未支援的工作環境上時，工具提示會顯示原因。

您可以在初始發現期間查看不受支援的工作環境，也可以在其中下載結果。您也可以從「設定」頁面中的「工作負載發現」選項查看發現的結果。

有關詳細信息，請參閱 "發現BlueXP ransomware protection中的工作負載"。

2025年4月29日

支援Amazon FSx for NetApp ONTAP

此版本支援Amazon FSx for NetApp ONTAP 。此功能可協助您使用BlueXP ransomware protection來保護 FSx for ONTAP工作負載。

FSx for ONTAP是一項完全託管的服務，可在雲端提供NetApp ONTAP儲存的強大功能。它提供與您在本機上使用的相同的功能、效能和管理能力，同時具有原生 AWS 服務的靈活性和可擴充性。

BlueXP ransomware protection工作流程進行了以下更改：

- Discovery 包含 FSx for ONTAP 9.15 工作環境中的工作負載。
- 「保護」標籤顯示 FSx for ONTAP環境中的工作負載。在這種環境中，您應該使用 FSx for ONTAP備份服務執行備份作業。您可以使用BlueXP ransomware protection快照恢復這些工作負載。

  無法在BlueXP中設定在 FSx for ONTAP上執行的工作負載的備份策略。 Amazon FSx for NetApp ONTAP中設定的任何現有備份策略均保持不變。

- 警報事件展示了新的 FSx for ONTAP工作環境。

有關詳細信息，請參閱 "了解BlueXP ransomware protection與工作環境"。

有關受支援選項的信息，請參閱 "BlueXP ransomware protection的局限性"。

需要BlueXP訪問角色

現在您需要以下存取角色之一來查看、發現或管理BlueXP ransomware protection：組織管理員、資料夾或專案管理員、勒索軟體保護管理員或勒索軟體保護檢視器。

"了解所有服務的BlueXP訪問角色" 。

2025年4月14日

準備演習報告

透過此版本，您可以查看勒索軟體攻擊準備演習報告。準備演練使您能夠模擬對新建立的範例工作負載的勒索軟體攻擊。然後，調查模擬攻擊並恢復樣本工作負載。此功能可協助您透過測試警報通知、回應和復原流程來了解在發生實際勒索軟體攻擊時是否已做好準備。

有關詳細信息，請參閱 "進行勒索軟體攻擊準備演習"。

新的基於角色的存取控制角色和權限

以前，您可以根據使用者的職責為其分配角色和權限，這有助於您管理使用者對BlueXP ransomware protection的存取。在這個版本中，有兩個特定於BlueXP ransomware protection的新角色具有更新的權限。新角色如下：

- 勒索軟體保護管理員
- 勒索軟體保護檢視器

有關權限的詳細信息，請參閱 "BlueXP ransomware protection基於角色的功能訪問"。

付款改進

此版本對支付流程進行了多項改進。

有關詳細信息，請參閱 "設定許可證和付款選項"。

2025年3月10日

模擬攻擊並做出回應

透過此版本，模擬勒索軟體攻擊來測試您對勒索軟體警報的回應。此功能可協助您透過測試警報通知、回應和復原流程來了解在發生實際勒索軟體攻擊時是否已做好準備。

有關詳細信息，請參閱 "進行勒索軟體攻擊準備演習"。

發現過程的增強

此版本包括對選擇性發現和重新發現過程的增強：

- 透過此版本，您可以發現新增到先前選擇的工作環境中的新建立的工作負載。
- 您也可以在此版本中選擇_新_工作環境。此功能可協助您保護新增至環境中的新工作負載。
- 您可以在最初的發現過程中或在設定選項中執行這些發現過程。

有關詳細信息，請參閱 "發現先前選定的工作環境的新建立的工作負載"和 "使用“設定”選項配置功能"。

偵測到高度加密時發出警報

在此版本中，即使沒有高檔案副檔名更改，您也可以在工作負載上偵測到高加密時查看警報。此功能使用ONTAP自主勒索軟體防護 (ARP) AI，可協助您識別面臨勒索軟體攻擊風險的工作負載。使用此功能並下載受影響文件的完整清單（無論擴展名是否更改）。

有關詳細信息，請參閱 "響應檢測到的勒索軟體警報"。

2024年12月16日

使用**Data Infrastructure Insights**儲存工作負載安全性偵測異常使用者行為

在此版本中，您可以使用Data Infrastructure Insights儲存工作負載安全性來偵測儲存工作負載中的異常使用者行為。此功能可協助您識別潛在的安全威脅並阻止潛在的惡意使用者以保護您的資料。

有關詳細信息，請參閱 "響應檢測到的勒索軟體警報"。

在使用Data Infrastructure Insights儲存工作負載安全性偵測異常使用者行為之前，您需要使用BlueXP ransomware protection*設定* 選項來設定此選項。

參考 "配置BlueXP ransomware protection設置"。

選擇要發現和保護的工作負載

在此版本中，您現在可以執行以下操作：

- 在每個連接器中，選擇您想要發現工作負載的工作環境。如果您想保護環境中的特定工作負載而不是其他工作負載，您可能會受益於此功能。
- 在工作負載發現期間，您可以啟用每個連接器的工作負載自動發現。此功能可讓您選擇要保護的工作負載。
- 發現先前選擇的工作環境的新建立的工作負載。

參考 "發現工作負載"。

2024年11月7日

啟用資料分類並掃描個人識別資訊 **(PII)**

在這個版本中，您可以啟用BlueXP classification（ BlueXP系列的核心元件）來掃描和分類檔案共用工作負載中的資料。將資料分類可以幫助您識別資料是否包含個人資訊或私人資訊，這可能會增加安全風險。此流程也會影響工作負載的重要性，並協助您確保使用適當的保護等級來保護工作負載。

部署了BlueXP classification的客戶通常可以在BlueXP ransomware protection中掃描 PII 資料。 BlueXP classification是作為BlueXP平台的一部分提供，無需額外付費，並且可以在本地或客戶雲端中部署。

若要啟動掃描，請在「保護」頁面上，選擇「保護」儀表板「隱私暴露」列中的 識別暴露。有關更多信息，請參閱 "使用 BlueXP classification 掃描個人識別敏感資料"。

SIEM 與 **Microsoft Sentinel** 集成

現在，您可以使用 Microsoft Sentinel 將資料傳送至安全性和事件管理系統 (SIEM) 以進行威脅分析和偵測。以前，您可以選擇 AWS Security Hub 或 Splunk Cloud 作為您的 SIEM。

"了解有關配置BlueXP ransomware protection設定的更多信息"。

立即免費試用 **30** 天

隨著此版本的發布， BlueXP ransomware protection的新部署現在有 30 天的免費試用期。在此之前， BlueXP ransomware protection提供 90 天的免費試用。如果您已享有 90 天免費試用，則該優惠將持續 90 天。

在檔案層級恢復 **Podman** 的應用程式工作負載

在檔案層級恢復應用程式工作負載之前，您現在可以查看可能受到攻擊影響的檔案清單並確定要復原的檔案。以前，如果組織（以前是帳戶）中的BlueXP連接器正在使用 Podman，則此功能將被停用。現在它已為 Podman 啟用。您可以讓BlueXP ransomware protection選擇要恢復的文件，您可以上傳列出受警報影響的所有文件的 CSV 文件，或者您可以手動識別要恢復的文件。

"了解有關從勒索軟體攻擊中恢復的更多信息" 。

2024年9月30日

檔案共享工作負載的自訂分組

在此版本中，您現在可以將文件共用分組，以便更輕鬆地保護您的資料資產。此服務可以同時保護群組中的所有磁碟區。以前，您需要單獨保護每個磁碟區。

"了解有關在勒索軟體保護策略中分組文件共享工作負載的更多信息" 。

2024年9月2日

來自**Digital Advisor**的安全風險評估

BlueXP ransomware protection 現在會從 NetApp Digital Advisor 收集與叢集相關的高風險和重大安全風險資訊。如果發現任何風險，BlueXP ransomware protection 會在控制面板的 建議操作 窗格中提供建議：「修正叢集上的已知安全漏洞 <name>」。從控制面板的建議中選擇 檢視並修復 後，系統會提示您查看 Digital Advisor 和一篇通用漏洞揭露（CVE）文章，以解決安全風險。如果存在多個安全風險，請查看 Digital Advisor 中的資訊。

參考 "Digital Advisor文檔"。

備份到 **Google Cloud Platform**

在此版本中，您可以將備份目標設定為 Google Cloud Platform 儲存桶。以前，您只能將備份目標新增至NetApp StorageGRID、Amazon Web Services 和 Microsoft Azure。

"了解有關配置BlueXP ransomware protection設定的更多信息".

支持 **Google Cloud Platform**

該服務現在支援適用於 Google Cloud Platform 的Cloud Volumes ONTAP進行儲存保護。先前，該服務僅支援適用於 Amazon Web Services 和 Microsoft Azure 的Cloud Volumes ONTAP以及本機 NAS。

"了解BlueXP ransomware protection以及支援的資料來源、備份目標和工作環境" 。

基於角色的存取控制

現在您可以使用基於角色的存取控制 (RBAC) 限制對特定活動的存取。 BlueXP ransomware protection使

用BlueXP的兩個角色： BlueXP帳號管理員和非帳號管理員（檢視者）。

有關每個角色可以執行的操作的詳細信息，請參閱 "基於角色的存取控制權限"。

2024年8月5日

使用 **Splunk Cloud** 進行威脅偵測

您可以自動將資料傳送到您的安全性和事件管理系統 (SIEM) 進行威脅分析和偵測。在先前的版本中，您只能選擇 AWS Security Hub 作為您的 SIEM。在此版本中，您可以選擇 AWS Security Hub 或 Splunk Cloud 作為您的 SIEM。

"了解有關配置BlueXP ransomware protection設定的更多信息"。

2024年7月1日

自帶授權 **(BYOL)**

在此版本中，您可以使用 BYOL 許可證，它是您從NetApp銷售代表處獲得的NetApp許可證文件 (NLF)。

"了解有關設置許可的詳細信息" 。

在檔案層級恢復應用程式工作負載

在檔案層級恢復應用程式工作負載之前，您現在可以查看可能受到攻擊影響的檔案清單並確定要復原的檔案。您可以讓BlueXP ransomware protection選擇要恢復的文件，您可以上傳列出受警報影響的所有文件的 CSV 文件，或者您可以手動識別要恢復的文件。

在此版本中，如果帳戶中的所有BlueXP連接器均未使用 Podman，則啟用單一檔案復原功能。否則，該帳戶將被停用。

"了解有關從勒索軟體攻擊中恢復的更多信息" 。

下載受影響文件的列表

在檔案層級復原應用程式工作負載之前，您現在可以造訪「警報」頁面以 CSV 檔案形式下載受影響檔案的列表，然後使用「復原」頁面上傳該 CSV 檔案。

"了解有關在恢復應用程式之前下載受影響文件的更多信息" 。

刪除保護計劃

透過此版本，您現在可以刪除勒索軟體保護策略。

"了解有關保護工作負載和管理勒索軟體保護策略的更多信息" 。

2024年6月10日

主儲存體上的快照副本鎖定

啟用此功能可鎖定主儲存體上的快照副本，以便即使勒索軟體攻擊進入備份儲存目標，它們在一定時間內也無法被修改或刪除。

"了解有關在勒索軟體保護策略中保護工作負載和啟用備份鎖定的更多信息" 。

支援適用於 **Microsoft Azure** 的**Cloud Volumes ONTAP**

此版本除了支援適用於 AWS 的Cloud Volumes ONTAP和本機ONTAP NAS 之外，還支援適用於 Microsoft Azure 的Cloud Volumes ONTAP作為系統。

"Azure 中的Cloud Volumes ONTAP快速入門"

"了解BlueXP ransomware protection" 。

Microsoft Azure 新增為備份目標

現在您可以將 Microsoft Azure 與 AWS 和NetApp StorageGRID一起新增為備份目標。

"了解有關如何配置保護設定的更多信息".

2024年5月14日

許可更新

您可以註冊 90 天免費試用。很快您將能夠透過 Amazon Web Services Marketplace 購買即用即付訂閱或自備NetApp授權。

"了解有關設置許可的詳細信息" 。

CIFS 協定

該服務現在支援使用 NFS 和 CIFS 協定的 AWS 系統中的本機ONTAP和Cloud Volumes ONTAP 。先前的版本僅支援 NFS 協定。

工作負載詳情

此版本現在在保護和其他頁面的工作負載資訊中提供了更多詳細信息，以改善工作負載保護評估。從工作負載詳細資料中，您可以查看目前指派的策略並查看配置的備份目標。

"詳細了解如何在“保護”頁面中查看工作負載詳細信息" 。

應用程式一致性和虛擬機器一致性保護和恢復

現在，您可以使用NetApp SnapCenter軟體執行應用程式一致性保護，並使用SnapCenter Plug-in for VMware vSphere虛擬機器一致性保護，從而實現靜止且一致的狀態，以避免日後需要復原時可能的資料遺失。如果需要恢復，您可以將應用程式或虛擬機器恢復到任何先前可用的狀態。

"了解有關保護工作負載的更多信息" 。

勒索軟體防護策略

如果工作負載上不存在快照或備份策略，您可以建立勒索軟體防護策略，其中可以包含您在此服務中建立的以下策略：

- 快照策略
- 備份策略
- 檢測策略

"了解有關保護工作負載的更多信息" 。

威脅偵測

現在可以使用第三方安全性和事件管理 (SIEM) 系統啟用威脅偵測。儀表板現在顯示「啟用威脅偵測」的新建議，可以在「設定」頁面上進行設定。

"了解有關配置“設定”選項的詳細信息".

消除誤報

從「警報」標籤中，您現在可以消除誤報或決定立即恢復資料。

"詳細了解如何回應勒索軟體警報" 。

檢測狀態

新的偵測狀態出現在「保護」頁面上，顯示套用於工作負載的勒索軟體偵測的狀態。

"了解有關保護工作負載和查看保護狀態的更多信息" 。

下載 **CSV** 文件

您可以從保護、警報和復原頁面下載 CSV 檔案*。

"詳細了解如何從儀表板和其他頁面下載 CSV 文件" 。

文件連結

查看文件連結現在包含在 UI 中。您可以從儀表板垂直*操作*存取此文檔  選項。選擇“新增功能”以查看發行說明中的詳細信息，或選擇“文件”查看BlueXP ransomware protection文件主頁。

BlueXP backup and recovery

BlueXP 備份和復原服務不再需要在系統上預先啟用。請參閱"先決條件"。BlueXP 勒索軟體防護服務可透過「設定」選項協助配置備份目標位置。請參閱"配置設定"。

設定選項

現在您可以在BlueXP ransomware protection設定中設定備份目的地。

"了解有關配置“設定”選項的詳細信息".

2024年3月5日

保護策略管理

除了使用預定義策略之外，您現在還可以建立策略。 "了解有關管理策略的更多信息" 。

二級儲存的不變性（**DataLock**）

現在，您可以使用物件儲存中的NetApp DataLock 技術使備份在二級儲存中不可變。 "了解有關創建保護策略的更多信息" 。

自動備份到**NetApp StorageGRID**

除了使用 AWS 之外、您現在還可以選擇 StorageGRID 作為備份目的地 "了解有關配置備份目標的更多信息"。

調查潛在攻擊的附加功能

現在您可以查看更多取證詳細資訊來調查偵測到的潛在攻擊。 "詳細了解如何回應偵測到的勒索軟體警報" 。

恢復過程

恢復過程得到了加強。現在，您可以按磁碟區或所有磁碟區恢復工作負載。 "了解有關從勒索軟體攻擊中恢復的更多資訊（事件被消除後）" 。

"了解BlueXP ransomware protection" 。

2023年10月6日

BlueXP ransomware protection服務是一種用於保護資料、偵測潛在攻擊以及從勒索軟體攻擊中恢復資料的SaaS 解決方案。

預覽版服務可保護BlueXP組織內各個組織中 Oracle、VM 資料儲存和本機 NAS 儲存空間上的檔案共用以及 AWS 上的Cloud Volumes ONTAP （使用 NFS 協定）上的應用程式工作負載，並將資料備份到 Amazon Web Services 雲端儲存。

BlueXP ransomware protection服務充分利用了多種NetApp技術，以便您的資料安全管理員或安全營運工程師能夠實現以下目標：

- 一目了然地查看所有工作負載的勒索軟體保護情況。
- 深入了解勒索軟體防護建議
- 根據BlueXP ransomware protection建議改進防護態勢。
- 指派勒索軟體保護策略，以保護您的主要工作負載和高風險資料免受勒索軟體攻擊。
- 監控您的工作負載的健康狀況，防範勒索軟體攻擊並尋找資料異常。
- 快速評估勒索軟體事件對您的工作量的影響。
- 透過恢復數據並確保不會再次感染儲存的數據，智慧地從勒索軟體事件中恢復。

"了解BlueXP ransomware protection" 。

NetApp Ransomware Resilience的已知限制

已知限制標識了該產品的此版本不支援或無法與其正確互通的平台、裝置或功能。仔細審查這些限制。

準備演習重置選項問題

如果您選擇ONTAP 9.11.1 磁碟區進行勒索軟體攻擊準備演習，勒索軟體復原能力會發送警報。如果您使用「複製到磁碟區」選項還原資料並重設鑽孔機，則重設操作將會失敗。

Amazon FSx for NetApp ONTAP限制

勒索軟體復原能力支援Amazon FSx for NetApp ONTAP系統。以下限制適用於Amazon FSx for ONTAP：

- Amazon FSx for ONTAP 不支援備份原則。在此環境中，您應該使用 Amazon FSx 執行備份作業。您可以使用 NetApp Ransomware Resilience 來恢復這些工作負載。
- 復原操作僅從快照執行。

Azure NetApp Files 限制

Azure NetApp Files 在 Ransomware Resilience 中受到支援。以下限制適用於 Azure NetApp Files ：

- Azure NetApp Files 不支援使用備份原則的勒索軟體防護策略。但您可以使用 Azure NetApp Files 備份功能。
- Azure NetApp Files 不支援複製功能的勒索軟體防護策略。
- 選擇保護策略時，請確保其快照排程與 Azure NetApp Files 相容。Azure NetApp Files 中最常使用的快照排程是每小時一次。

版權資訊

商標資訊