開始
NetApp Ransomware Resilience

NetApp
February 18, 2026

目錄

開始 1
了解NetApp Ransomware Resilience 1
資料層的勒索軟體抵禦能力 1
勒索軟體復原能力可以做什麼 2
使用勒索軟體恢復能力的好處 3
成本 3
授權 4
NetApp Console 4
勒索軟體復原的工作原理 4
支援的備份目標、系統和工作負載資料來源 6
關鍵術語 7
NetApp Ransomware Resilience前提條件 7
支援的系統 8
NetApp Console需求 8
ONTAP 需求 8
資料備份 9
可疑用戶行為要求 9
更新ONTAP系統中的非管理員使用者權限 9
NetApp Ransomware Resilience快速入門 10
設定NetApp Ransomware Resilience 11
準備備份目標 11
設定NetApp Console 11
存取NetApp Ransomware Resilience 12
設定NetApp Ransomware Resilience的許可 13
許可證類型 13
其他許可證 13
試試 Ransomware Resilience 30 天免費試用版 14
透過 AWS Marketplace 訂閱 15
透過 Microsoft Azure Marketplace 訂閱 16
透過 Google Cloud Platform Marketplace 訂閱 18
自帶授權 (BYOL) 20
控制台許可證到期後請更新 21
結束 PAYGO 訂閱 22
更多資訊 22
發現NetApp Ransomware Resilience中的工作負載 22
選擇要發現和保護的工作負載 22
發現先前選定的系統新建立的工作負載 24
發現新系統 24
排除工作負載 25

在NetApp Ransomware Resilience中進行勒索軟體攻擊準備演練 26
配置勒索軟體攻擊準備演習 27
開始準備演習 29
響應戰備演習警報 29
恢復測試工作負載 31
準備演練後更改警報狀態 32
審查準備演習報告 32
在NetApp Ransomware Resilience中配置保護設置 33
直接存取設定頁面 33
模擬勒索軟體攻擊 33
配置工作負載發現 34
新增備份目標 34
將 NetApp Ransomware Resilience 連接到安全性與事件管理系統（SIEM），以進行威脅分析與偵測 41
傳送至 SIEM 的事件資料 41
設定 AWS Security Hub 進行威脅偵測 42
設定 Microsoft Sentinel 進行威脅偵測 42
設定 Splunk Cloud 進行威脅偵測 45
在勒索軟體防禦中連接 SIEM 45
設定使用者活動偵測 46
瞭解 NetApp Ransomware Resilience 中的使用者活動偵測 46
NetApp Ransomware Resilience 中的使用者行為偵測需求 48
在 NetApp Ransomware Resilience 中設定代理程式與收集器以偵測使用者活動 52

開始

了解NetApp Ransomware Resilience

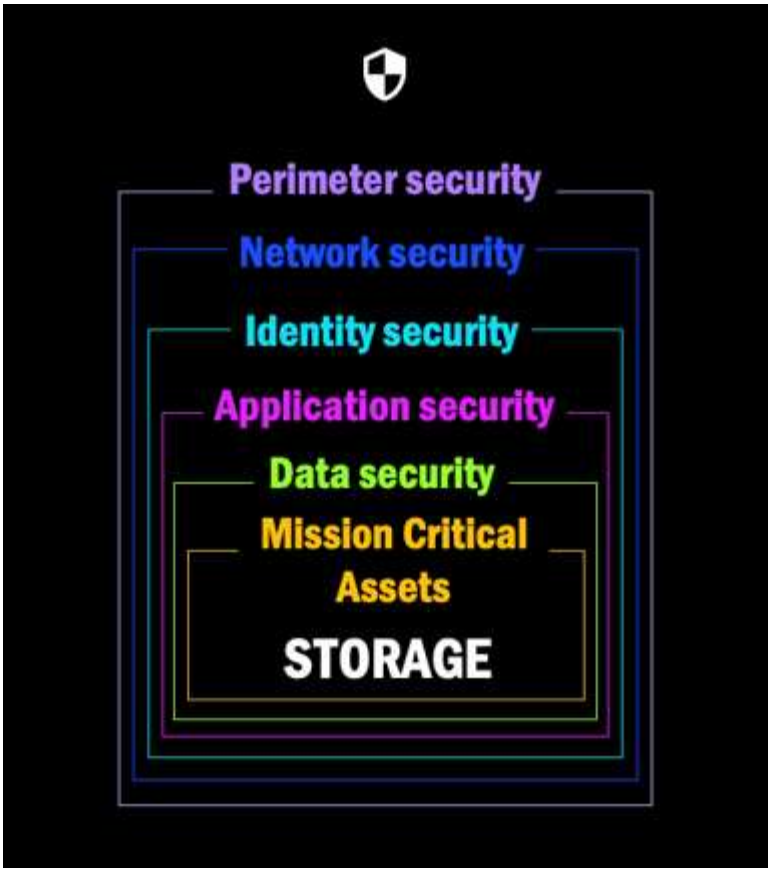
勒索軟體攻擊可以阻止對您資料的訪問，攻擊者可以要求贖金以換取資料發布或解密。據 IDC 稱，勒索軟體受害者遭受多次勒索軟體攻擊的情況並不少見。攻擊可能會中斷您對資料的訪問，時間從一天到幾週不等。

NetApp Ransomware Resilience可保護您的資料免受勒索軟體攻擊。在勒索軟體復原功能中，可透過 NetApp 控制台為 Oracle、VM 資料儲存和本機 NAS 儲存體（使用 NFS 和 CIFS 協定）和 SAN 儲存體（FC、iSCSI 和 NVMe）上的檔案共用以及 Amazon Web Services 的Cloud Volumes ONTAP 、Google Cloud 的Cloud Volumes ONTAP 、Microsoft Web Services 的Cloud Volumes ONTAP ONTAPx 的NetApp ConsoleAmazon FSx for NetApp ONTAP的工作。您可以將資料備份到 Amazon Web Services、Google Cloud、Microsoft Azure 雲端儲存和NetApp StorageGRID。

資料層的勒索軟體抵禦能力

您的安全態勢通常包含多層防禦，以防禦一系列網路威脅。

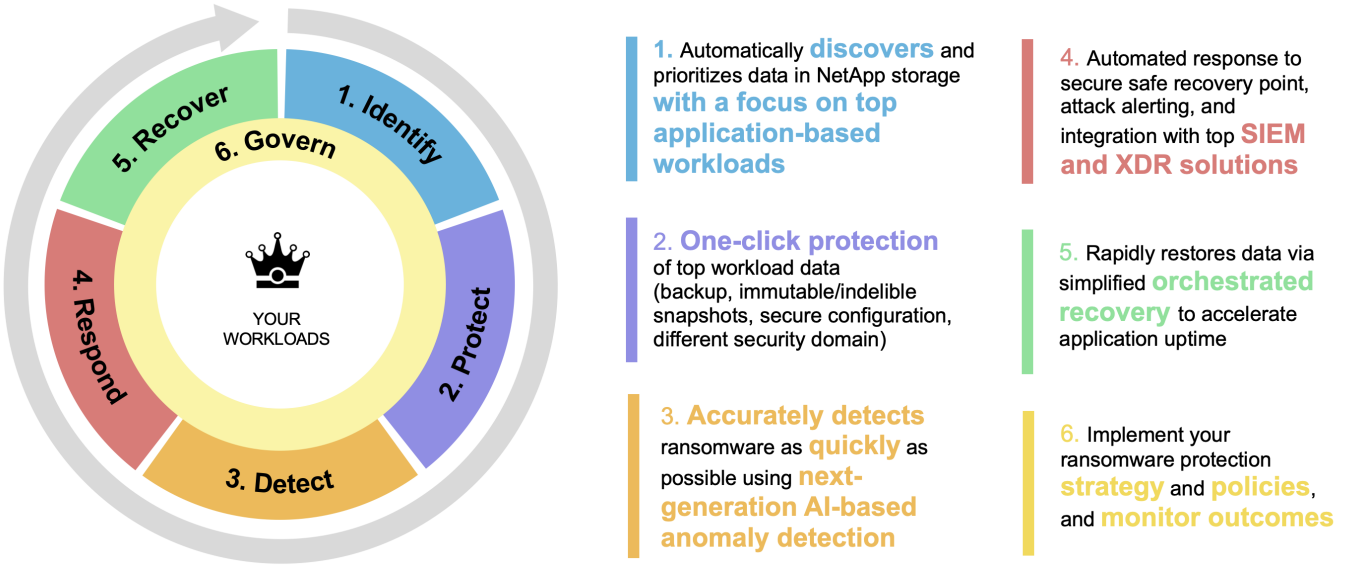
- 最外層：這是使用防火牆、入侵偵測系統和虛擬專用網路來保護網路邊界的第一道防線。
- 網路安全：這一層建立在網路分段、流量監控和加密的基礎上。
- 身分安全：使用身分驗證方法、存取控制和身分管理來確保只有授權使用者才能存取敏感資源。
- 應用程式安全：使用安全編碼實踐、安全測試和運行時應用程式自我保護來保護軟體應用程式。
- 資料安全：透過資料保護、備份和復原策略保護您的資料。勒索軟體復原力在此層上運作。



勒索軟體復原能力可以做什麼

勒索軟體復原功能充分利用了多種NetApp技術，以便您的儲存管理員、資料安全管理員或安全營運工程師可以實現以下目標：

- 識別 NetApp本地 NAS（NFS 或 CIFS）和 SAN（FC、iSCSI 和 NVMe）系統中所有基於應用程式、檔案共用或 VMware 管理的工作負載，包括NetApp Console、專案和控制台代理程式。勒索軟體彈性對資料優先級進行分類，並為您提供勒索軟體彈性改進的建議。
- 透過對資料啟用備份、快照副本和勒索軟體保護策略來*保護*您的工作負載。
- *偵測*可能是勒索軟體攻擊的異常。註腳：[儘管攻擊可能未被發現，但我們的研究表明， NetApp技術已對某些基於文件加密的勒索軟體攻擊實現了高度檢測。]
- *應對*潛在的勒索軟體攻擊，自動啟動一個鎖定的時間點快照，以防止副本被意外或惡意刪除。您的備份資料將保持不可更改，並在來源端和目標端受到端到端的保護，免受勒索軟體攻擊。
- 透過協調多種NetApp技術來*恢復*您的工作負載，從而幫助加快工作負載的正常運作時間。您可以選擇恢復特定的磁碟區。勒索軟體彈性提供最佳選項的建議。
- 管理：實施勒索軟體保護策略並監控結果。



使用勒索軟體恢復能力的好處

勒索軟體復原能力有以下優勢：

- 發現工作負載及其現有的快照和備份計劃，並對其相對重要性進行排序。
- 評估您的勒索軟體防護態勢並將其顯示在易於理解的儀表板中。
- 根據發現和保護態勢分析提供後續步驟的建議。
- 一鍵存取即可套用 AI/ML 驅動的資料保護建議。
- 保護基於應用程式的工作負載（例如 Oracle、VMware 資料儲存和檔案共用）中的資料。
- 使用人工智慧技術即時偵測針對主儲存資料的勒索軟體攻擊。
- 透過建立快照副本和啟動有關異常活動的警報來啟動自動操作以回應偵測到的潛在攻擊。
- 應用精心策劃的恢復以滿足 RPO 政策。勒索軟體復原能力透過使用多種NetApp復原服務（包括NetApp Backup and Recovery（以前稱為雲端備份）和SnapCenter）來協調勒索軟體事件的復原。
- 使用基於角色的存取控制 (RBAC) 來管理對功能和操作的存取。

成本

您可以免費試用 Ransomware Resilience 30 天。NetApp不會向您收取使用 Ransomware Resilience 試用版的費用。

如果您同時擁有備份和復原以及勒索軟體復原功能，則受這兩種產品保護的任何公開資料僅由勒索軟體復原功能計費。

購買許可證或 PayGo 訂閱後，任何啟用了勒索軟體偵測策略（自主勒索軟體保護）（由勒索軟體復原力發現或設定）且至少有一個快照或備份策略的工作負載，勒索軟體復原力都會將其歸類為“受保護”，併計入購買的容量或 PayGo 訂閱。如果在沒有檢測策略的情況下發現工作負載，即使它具有備份或快照策略，也會將其歸類為“有風險”，並且不會計入購買的容量。

90 天試用期結束後，受保護的工作負載將計入購買的容量或訂閱。勒索軟體恢復按每 GB 為與受保護工作負載相關的資料（在效率之前）收費。

授權

透過 Ransomware Resilience，您可以使用不同的授權計劃，包括免費試用、即用即付訂閱或自備授權。

勒索軟體復原需要NetApp ONTAP One 許可證。

勒索軟體恢復許可證不包括其他NetApp產品。即使您沒有許可證，Ransomware Resilience 也可以使用備份和還原。

為了偵測異常使用者行為，Ransomware Resilience 使用NetApp Autonomous Ransomware Protection，這是ONTAP內的一種機器學習 (ML) 模型，可偵測惡意檔案活動。該模型包含在勒索軟體恢復許可證中。

有關詳細信息，請參閱"設定許可" 。

NetApp Console

可透過NetApp Console存取勒索軟體復原功能。

NetApp Console提供企業級跨本機和雲端環境的NetApp儲存和資料服務的集中管理。需要控制台才能存取和使用NetApp資料服務。作為管理介面，它使您能夠從一個介面管理許多儲存資源。控制台管理員可以控制企業內所有系統的儲存和服務的存取。

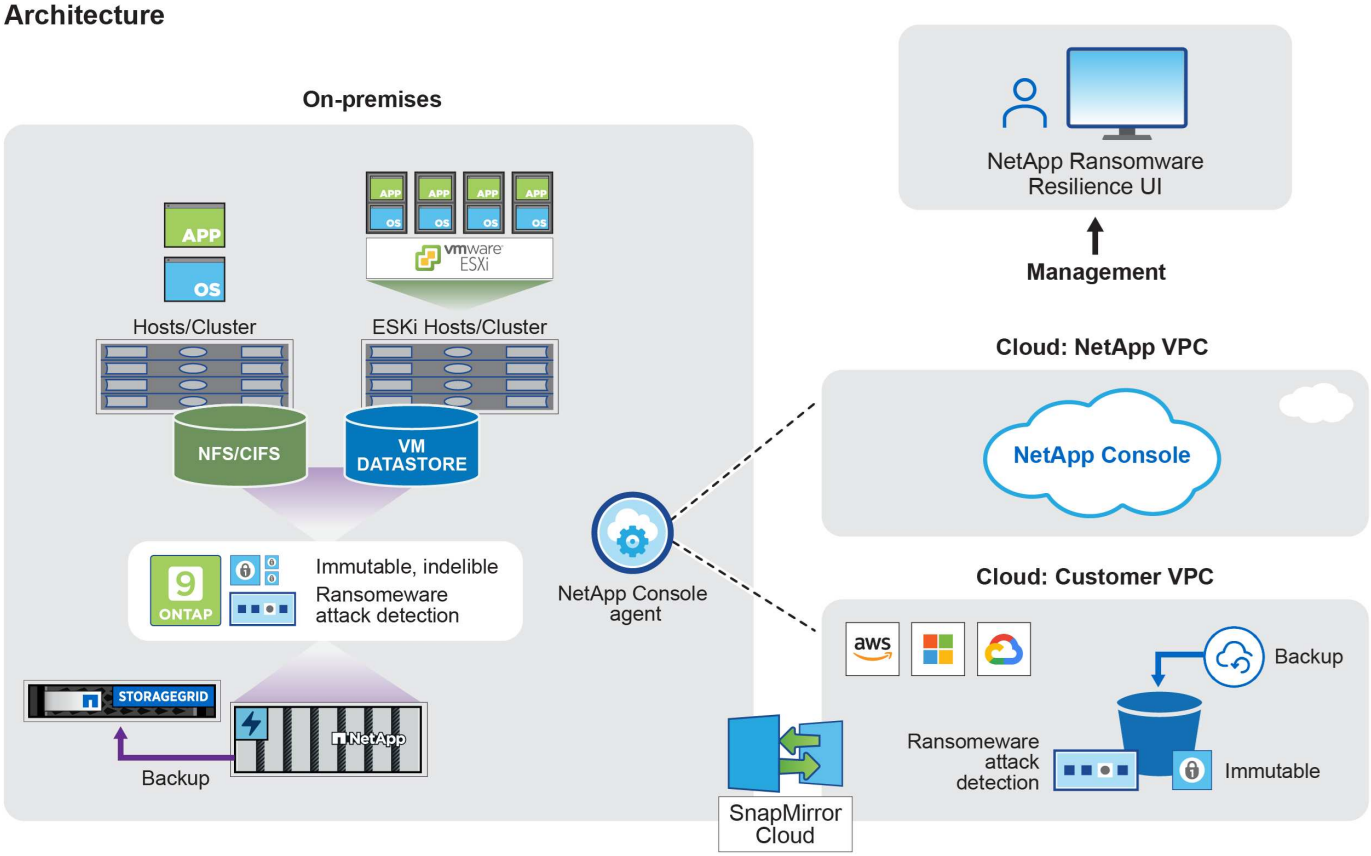
您無需許可證或訂閱即可開始使用 NetApp Console，只有在雲端部署 Console 代理程式以確保與儲存系統或 NetApp 資料服務的連線時才會產生費用。但是，某些可從 Console 存取的 NetApp 資料服務需要獲得許可或訂閱才能使用。

詳細了解"NetApp Console"。

勒索軟體復原的工作原理

Ransomware Resilience 使用 NetApp Backup and Recovery 來探索並設定檔案共用工作負載的快照和備份原則。

Architecture



特徵	描述
確認	• 尋找連接到控制台的所有客戶本地 NAS（NFS 和 CIFS 協定）、SAN（FC、iSCSI 和 NVMe）和Cloud Volumes ONTAP資料。 • 從 ONTAP 和 SnapCenter 服務 API 中識別客戶數據，並將其與工作負載關聯。深入瞭解 "ONTAP"。 • 發現每個磁碟區的目前NetApp快照副本和備份策略的保護等級以及任何機上偵測功能。然後，勒索軟體復原能力透過使用備份和復原、 ONTAP服務以及NetApp技術（例如自主勒索軟體保護（ARP 或 ARP/AI，取決於您的ONTAP版本）、FPolicy、備份策略和快照策略）將此保護狀態與工作負載關聯。了解更多 "自主勒索軟體防護"，"NetApp Backup and Recovery" ， 和 "ONTAP FPolicy"。 • 根據自動發現的保護等級為每個工作負載分配業務優先級，並根據工作負載的業務優先級建議保護策略。工作負載優先順序是基於已應用於與工作負載相關的每個磁碟區的快照頻率。
保護	• 主動監控工作負載，並透過將原則套用至每個已識別的工作負載來協調 Backup and Recovery 和 ONTAP API 的使用。

特徵	描述
探測	• 使用整合式機器學習 (ML) 模型偵測潛在攻擊，該模型可偵測潛在的異常加密和活動。 • 提供雙層偵測，首先偵測主儲存中的潛在勒索軟體攻擊，然後透過取得額外的自動快照副本來建立最近的資料還原點，以回應異常活動。勒索軟體復原能力能夠更深入地挖掘以更精確地識別潛在攻擊，而不會影響主要工作負載的效能。 • 使用ONTAP、自主勒索軟體防護（ARP 或 ARP/AI，取決於您的ONTAP版本）和 FPolicy 技術確定攻擊相關工作負載的特定可疑檔案和對應。
回應	• 顯示相關數據，例如文件活動、使用者活動和熵，以幫助您完成有關攻擊的取證審查。 • 使用NetApp技術和產品（例如ONTAP、自主勒索軟體防護（ARP 或 ARP/AI，取決於您的ONTAP版本）和 FPolicy）啟動快速快照副本。
恢復	• 透過使用備份和復原、 ONTAP、自主勒索軟體防護（ARP 或 ARP/AI，取決於您的ONTAP版本）以及 FPolicy 技術和服務，確定最佳快照或備份並推薦最佳復原點實際 (RPA)。 • 協調包括虛擬機器、文件共享、區塊儲存和資料庫在內的工作負載的恢復，並保持應用程式的一致性。
治理	• 分配勒索軟體保護策略 • 幫助您監控結果。

支援的備份目標、系統和工作負載資料來源

勒索軟體復原支援以下備份目標、系統和資料來源：

支援的備份目標

- 亞馬遜網路服務（AWS）S3
- 谷歌雲端平台
- 微軟 Azure Blob
- NetAppStorageGRID

支援的系統

環境	協定	支援的版本
Amazon FSx for NetApp ONTAP*	CIFS、NFS 和 SAN	不適用
Azure NetApp Files	CIFS 和 NFS	不適用
適用於 AWS 的Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本

環境	協定	支援的版本
適用於 Google Cloud Platform 的Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本
適用於 Microsoft Azure 的Cloud Volumes ONTAP	CIFS 和 NFS	9.12.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本
ONTAP （本地部署）	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本

* Amazon FSx for NetApp ONTAP使用自主勒索軟體保護 (ARP) 而非 ARP/AI。有關兩者區別的更多信息，請參閱"ARP/AI"。

> 在ONTAP中使用 ARP/AI 需要ONTAP 9.16 或更高版本。+ ONTAP不為FabricPool FlexCache、FlexGroup磁碟區、一致性群組掛載點磁碟區、掛載路徑磁碟區、離線磁碟區和資料保護 (DP) 磁碟區提供勒索軟體防護支援。請務必查看"ONTAP中支援且不受支援的配置"。

支援的工作負載資料來源

勒索軟體復原能力可保護主資料磁碟區上的以下基於應用程式的工作負載：

- 區塊儲存
- 資料庫:
  - 微軟 SQL 伺服器
  - 甲骨文
  - PostgreSQL
- NetApp檔案分享
- VMware 資料儲存區

關鍵術語

了解一些與勒索軟體保護相關的術語可能會對您有所幫助。

- 保護：勒索軟體復原中的保護意味著確保使用保護策略定期在不同的安全域中進行快照和不可變備份。
- 工作負載：勒索軟體復原中的工作負載可以包括 Oracle 資料庫、VMware 資料儲存或檔案共用。

NetApp Ransomware Resilience前提條件

首先驗證您的操作環境、網路存取和 Web 瀏覽器是否已準備就緒，即可開始使用NetApp Ransomware Resilience。

若要使用勒索軟體復原功能，請確保滿足先決條件。

支援的系統

請確保您使用的是受支援的系統：

環境	協定	支援的版本
Amazon FSx for NetApp ONTAP*	CIFS、NFS 和 SAN	不適用
Azure NetApp Files	CIFS 和 NFS	不適用
適用於 AWS 的Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本
適用於 Google Cloud Platform 的Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本
適用於 Microsoft Azure 的Cloud Volumes ONTAP	CIFS 和 NFS	9.12.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本
ONTAP （本地部署）	CIFS 和 NFS	9.11.1 及更高版本
	SAN（FC、iSCSI 和 NVMe）	9.17.1 及更高版本

* Amazon FSx for NetApp ONTAP使用自主勒索軟體保護 (ARP) 而非 ARP/AI。有關兩者區別的更多信息，請參閱"ARP/AI"。

NetApp Console需求

您的NetApp Console配置需要：

- 具有組織管理員權限的NetApp Console使用者帳戶，用於發現資源。
- 一個控制台組織和系統，其中至少有一個活動的控制台代理連接到"支援的系統"。
  - 如果您的本機ONTAP叢集或 AWS 或 Azure 雲端中的Cloud Volumes ONTAP未在控制台中設置，請參閱"了解如何配置控制台代理"和"標準控制台要求"。

> 如果您在單一控制台組織中擁有多個控制台代理，則勒索軟體復原功能將掃描除控制台 UI 中目前選擇的代理之外的所有控制台代理中的ONTAP資源。

- 控制台代理必須具有 `cloudmanager-ransomware-protection`容器處於活動狀態。
- 至少一個具有NetApp本地ONTAP叢集或 AWS 或 Azure 中的Cloud Volumes ONTAP 的控制台系統。勒索軟體復原支援 NAS（NFS 和 SMB）和 SAN（iSCSI、FC 和 NVMe）協定。
  - ONTAP或Cloud Volumes ONTAP叢集（ ONTAP版本 9.11.1 或更高版本）支援勒索軟體復原功能。

> 若要在 SAN 工作負載上使用勒索軟體復原功能，您必須執行ONTAP 9.17.1 或更高版本。

ONTAP 需求

- 您必須執行ONTAP 9.11.1 或更高版本，並且在本機ONTAP實例上啟用ONTAP One 授權。有關ONTAP支援的更多信息，請參閱"自主勒索軟體防護概述"。

- 若要套用保護配置（例如啟用自主勒索軟體保護），勒索軟體復原能力需要ONTAP叢集上的管理員權限。ONTAP叢集應該只使用ONTAP叢集管理員使用者憑證進行加入。

> 如果您已使用非管理員憑證將ONTAP叢集連接到控制台，則[您必須更新ONTAP叢集中的憑證](#update-non-admin-user-permissions-in-an-ontap-system)。

資料備份

- 在NetApp StorageGRID、AWS S3、Azure Blob 或 Google Cloud Platform 中擁有一個帳戶，用於備份目標，並配置了適當的存取權。

  請參閱 "AWS、Azure 或 S3 權限列表"了解詳情。

- 不需要在系統上啟用NetApp Backup and Recovery 。

  勒索軟體復原力有助於透過設定選項來配置備份目標。看"配置設定" 。

可疑用戶行為要求

為了使 Ransomware Resilience 能夠發出有關可疑使用者行為的警報，您必須設定使用者活動代理程式。若要安裝使用者活動代理程式，請確保您的系統符合"要求"。

更新**ONTAP**系統中的非管理員使用者權限

如果您需要更新特定系統中的非管理員使用者權限，請依照下列步驟操作。

1. 登入 Console 。在儀表板中，找到需要更新 ONTAP 使用者權限的系統。
2. 選擇系統以檢視其詳細資訊。
3. 選擇“查看其他資訊”以顯示使用者名稱。
4. 以管理員使用者身分登入ONTAP集群 CLI。
5. 顯示該使用者的現有角色：

   ```
   security login show -user-or-group-name <username>
   ```

6. 更改使用者的角色。進入：

   ```
   security login modify -user-or-group-name <username> -application
   console|http|ontapi|ssh|telnet -authentication-method password -role
   admin
   ```

7. 返回NetApp Console以使用勒索軟體復原功能。

NetApp Ransomware Resilience快速入門

了解設定勒索軟體保護功能和保護工作負載所需遵循的進階步驟。

請按照每個步驟中的連結獲取詳細資訊。

1 審查先決條件

這些任務需要_Console admin_角色。

- "確保已安裝控制台代理"
- "確保您的系統符合要求"
- "審查勒索軟體恢復使用者角色並為存取勒索軟體復原的使用者分配權限"
- "設定許可"

2 開始使用勒索軟體防禦

這些任務需要「勒索軟體復原管理員」角色。

- "在控制台中發現工作負載"
- "在儀表板上查看工作負載保護健康狀況"
- "（可選）進行勒索軟體攻擊準備演習"

3 在 **Ransomware Resilience** 中設定保護和偵測

這些任務需要「勒索軟體復原管理員」角色。配置可疑用戶行為活動需要額外的「勒索軟體恢復用戶行為管理員」角色。

- "保護工作負載"
  - 可選地，"透過配置可疑使用者活動偵測來增強保護"
- （可選）配置備份目標：
  - "準備NetApp StorageGRID、Amazon Web Services、Google Cloud Platform 或 Microsoft Azure 作為備份目標"。
  - "配置備份目標"
- "回應偵測到的潛在勒索軟體攻擊"
- "從攻擊中恢復（事件消除後）"

4 下一步是什麼？

在勒索軟體復原中配置保護後，您可以執行以下操作。

- "啟用資料分類來識別治理和安全風險"

- "向 SIEM 發送警報"
- "下載警報、保護、準備演習、恢復或摘要報告"

設定NetApp Ransomware Resilience

您可以輕鬆部署NetApp Ransomware Resilience。在開始之前，請查看"先決條件"以確保您的環境已準備就緒。

準備備份目標

準備以下備份目標之一：

- NetAppStorageGRID
- 亞馬遜網路服務
- 谷歌雲端平台
- 微軟 Azure

在備份目標本身中配置選項後，您稍後會將其配置為 Ransomware Resilience 中的備份目標。有關如何在 Ransomware Resilience 中配置備份目標的詳細信息，請參閱"配置備份目標"。

準備**StorageGRID**以成為備份目標

如果要使用StorageGRID作為備份目標，請參閱 "StorageGRID文檔"有關StorageGRID的詳細資訊。

準備 **AWS** 成為備份目標

- 在 AWS 中設定一個帳戶。
- 配置 "AWS 權限"在 AWS 中。

有關在控制台中管理 AWS 存儲的詳細信息，請參閱 "管理您的 Amazon S3 儲存桶"。

準備 **Azure** 以成為備份目標

- 在 Azure 中設定一個帳戶。
- 配置 "Azure 權限"在 Azure 中。

有關在控制台中管理 Azure 儲存體的詳細信息，請參閱 "管理 Azure 儲存體帳戶"。

設定NetApp Console

下一步是設定控制台和勒索軟體復原能力。

審查 "標準模式的控制台要求"。

建立控制台代理

聯絡您的NetApp銷售代表試用或使用此服務。然後，當您使用控制台代理時，它將包含適當的勒索軟體恢復功

能。

若要使用勒索軟體復原功能建立控制台代理，請聯絡具有建立控制台代理權限的控制台組織管理員，並參考描述"如何建立控制台代理"。

如果您有多個控制台代理，則勒索軟體復原功能會掃描除控制台中目前顯示的代理之外的所有控制台代理的資料。該服務發現與該組織相關的所有項目和所有控制台代理。

存取NetApp Ransomware Resilience

透過NetApp Console登入NetApp Ransomware Resilience 。

若要登入控制台，您可以使用您的NetApp支援網站憑證，也可以使用您的電子郵件和密碼註冊NetApp雲端登入。 "了解有關登入的更多信息" 。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"了解NetApp Console的勒索軟體復原角色" 。

步驟

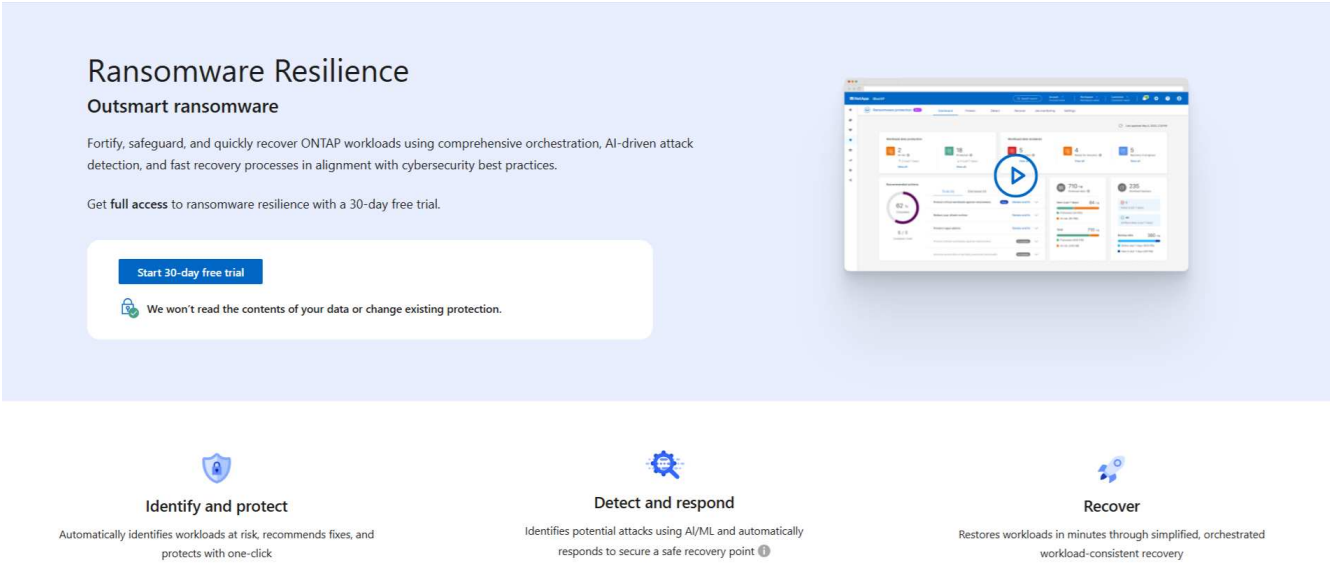
1. 打開網頁瀏覽器並前往"主機"。

   出現控制台登入頁面。

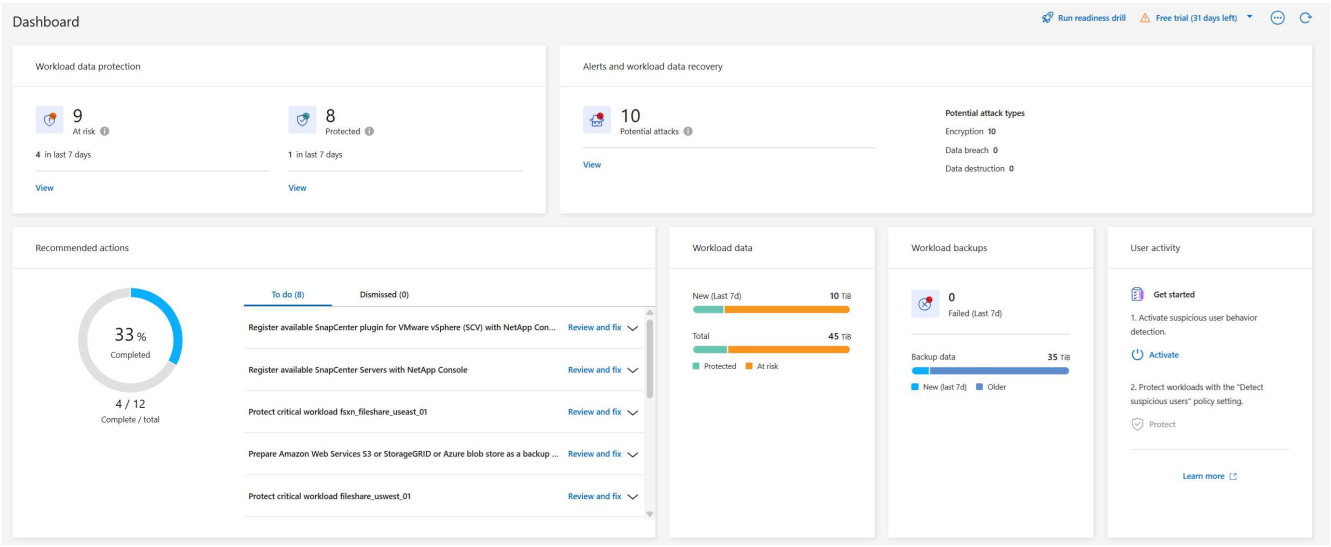
2. 登入控制台。
3. 從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

   如果這是您第一次登入此服務，則會出現登入頁面。

   如果您沒有控制台代理或它不是此服務的代理，則需要部署一個。"了解如何設定控制台代理" 。



否則，將出現勒索軟體復原力儀表板。



4. 如果您還沒有這樣做，請選擇「發現工作負載」選項。

   請參閱"發現工作負載" 。

設定NetApp Ransomware Resilience的許可

透過NetApp Ransomware Resilience，您可以使用不同的授權方案。

要執行此任務，您需要組織管理員、資料夾或專案管理員角色。 "了解控制台存取角色" 。

許可證類型

勒索軟體防護功能提供以下幾種許可類型：

- 30天免費試用
- 透過 Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace 或 Azure Marketplace 購買即用即付 (PAYGO) 訂閱
- 自帶授權 (BYOL)：您從NetApp銷售代表取得的NetApp授權文件 (NLF)。您可以使用許可證序號在控制台中啟動 BYOL。

設定 BYOL 或購買 PAYGO 訂閱後，您可以在控制台的Licenses and subscriptions部分看到授權。

免費試用期結束或許可證或訂閱到期後，您仍然可以：

- 查看工作負載和工作負載健康狀況
- 刪除策略等資源
- 運行在試用期間或許可證下建立的所有計劃操作

其他許可證

勒索軟體恢復許可證不包括其他NetApp產品。但是，即使您沒有單獨的備份和復原許可證，勒索軟體復原能力也可以與NetApp Backup and Recovery整合。

如果您同時擁有備份和復原以及勒索軟體復原功能，則受這兩種產品保護的任何公開資料將僅由勒索軟體復原功能計費。

試試 **Ransomware Resilience 30** 天免費試用版

您可以免費試用 Ransomware Resilience 30 天。您必須是控制台組織管理員才能開始免費試用。

試用期間不強制執行儲存容量限制。

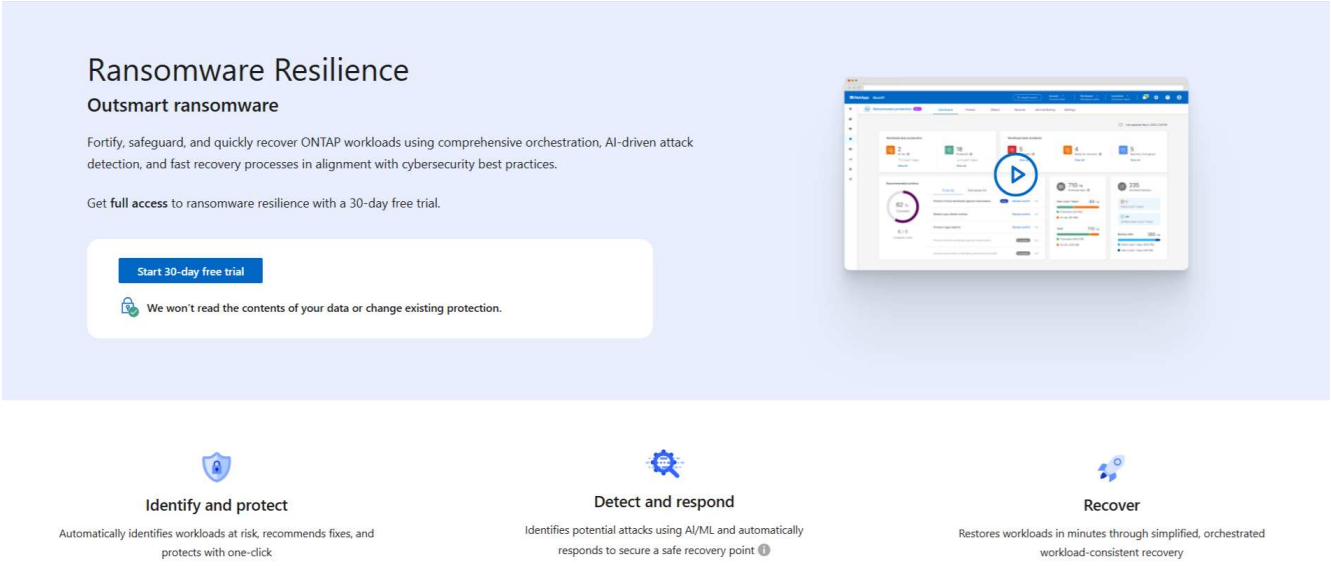
您可以隨時獲得許可證或訂閱，並且在 30 天試用期結束之前不會向您收費。要在 30 天試用期後繼續使用，您需要購買 BYOL 授權或 PAYGO 訂閱。

在試用期間，您可以使用全部功能。

步驟

1. 訪問 "安慰"。
2. 登入控制台。
3. 從NetApp Console中，選擇「保護」>「勒索軟體復原能力」。

   如果這是您第一次登入此服務，則會出現登入頁面。



4. 如果您尚未為其他服務新增控制台代理，"添加一個"。
5. 在勒索軟體復原登陸頁面中，選擇*從發現工作負載開始*來發現您的工作負載。

   僅當您成功安裝了控制台代理後，此選項才可用。

6. 要查看免費試用信息，請選擇右上角的下拉選項。

試用結束後，取得訂閱或授權

免費試用結束後，您可以透過其中一個市場進行訂閱，也可以從NetApp購買授權。

如果您已經擁有 PAYGO 訂閱，免費試用結束後許可證將自動切換到訂閱。

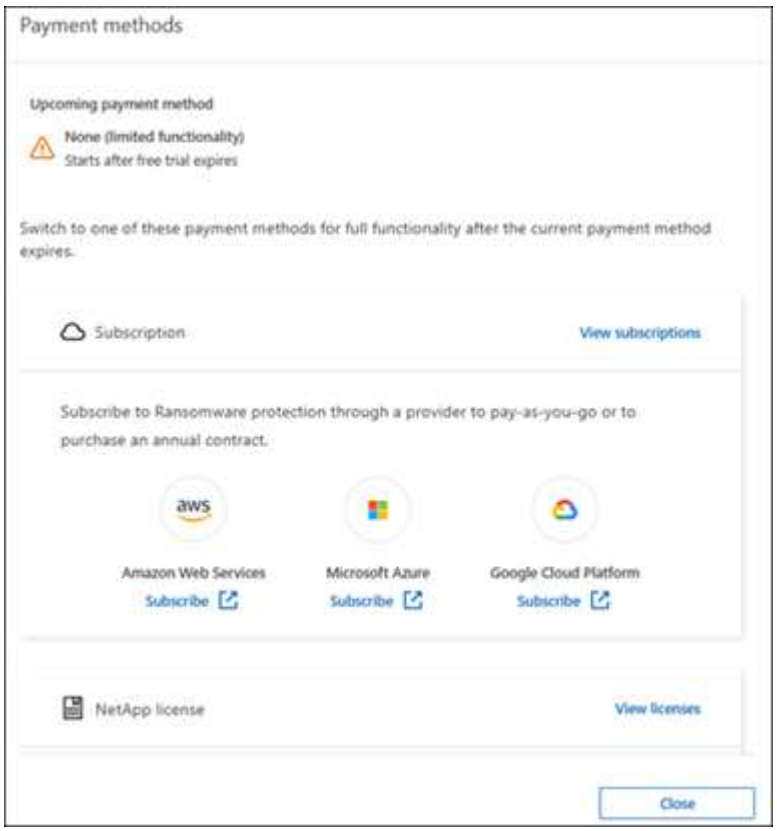
透過 AWS Marketplace 訂閱 透過 Microsoft Azure Marketplace 訂閱 透過 Google Cloud Platform Marketplace 訂閱 自帶授權 (BYOL)

透過 **AWS Marketplace** 訂閱

此流程提供如何在 AWS Marketplace 中直接訂閱的高級概述。

步驟

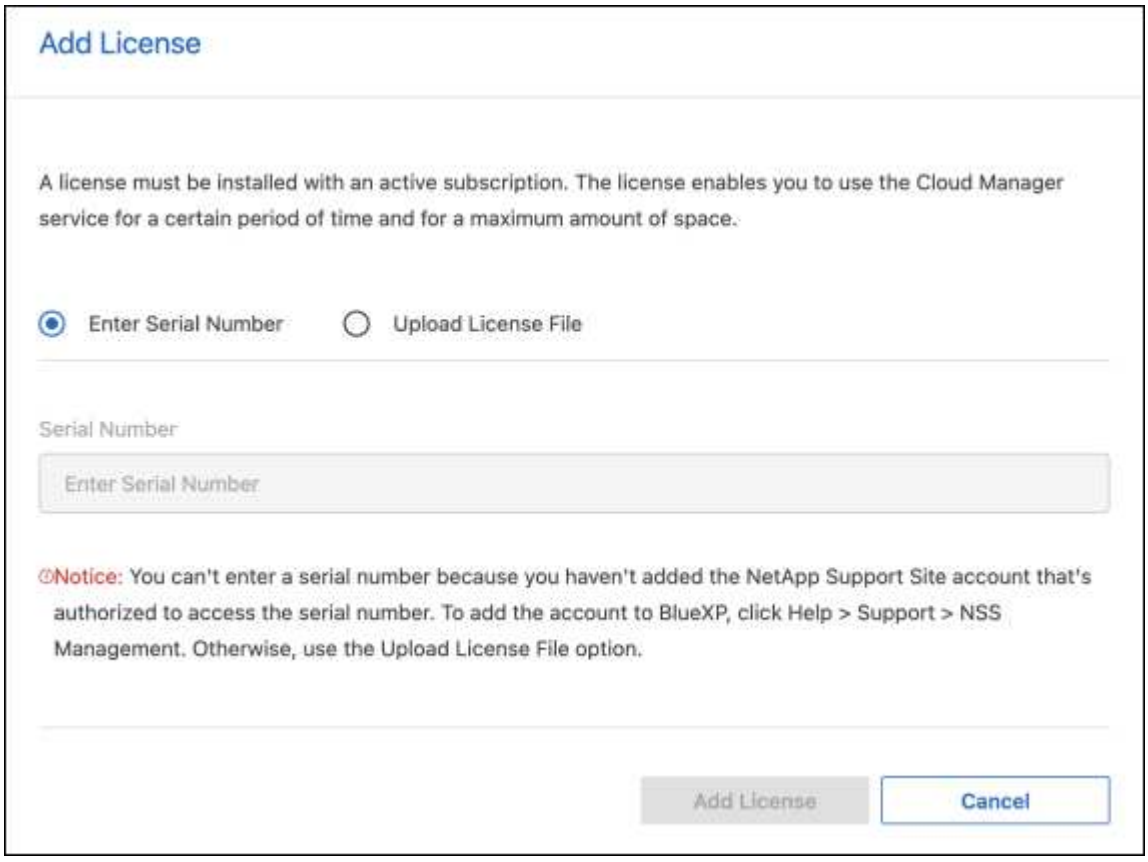
1. 在「勒索軟體復原」中，執行以下操作之一：
   - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。
   - 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」**Amazon Web Services**。
3. 在 AWS Marketplace 中，選擇 查看購買選項。
4. 使用 AWS Marketplace 訂閱 * NetApp Intelligent Services* 和 * 勒索軟體復原能力 *。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。

> 系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示您已在 AWS Marketplace 中訂閱 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 透過選擇「新增許可證」將許可證新增至控制台。



8. 在新增許可證頁面中，選擇*輸入序號*，輸入發送給您的電子郵件中包含的序號，然後選擇*新增許可證*。
9. 要查看許可證詳細信息，請從控制台左側導航中選擇“管理”>“**Licenses and subscriptions**”。
   - 若要查看訂閱訊息，請選擇*訂閱*。
   - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

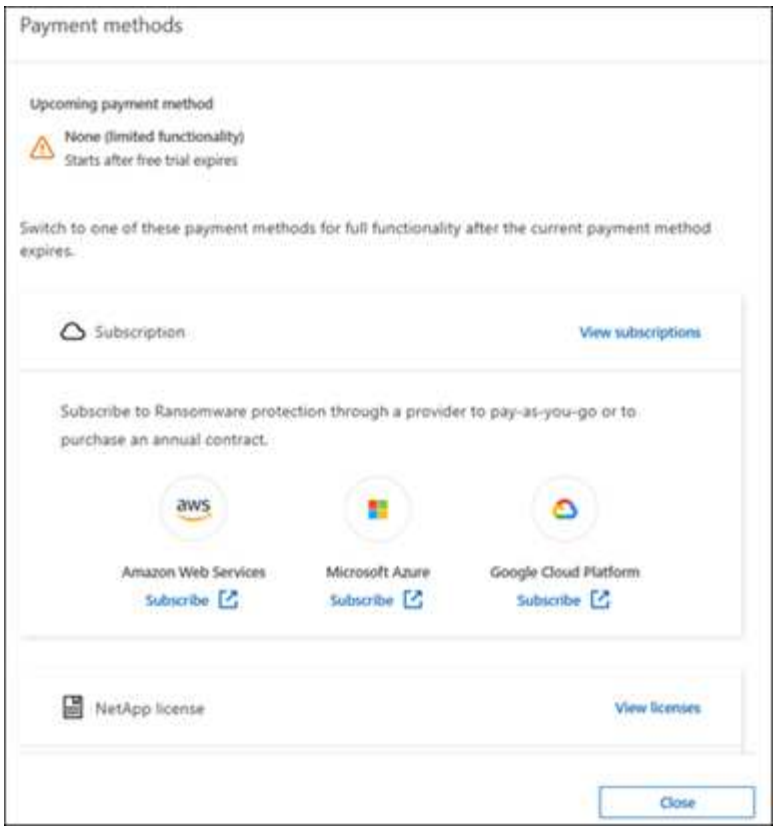
    一則訊息確認許可證已新增。

透過 **Microsoft Azure Marketplace** 訂閱

此流程提供如何在 Azure 市場中直接訂閱的高級概述。

步驟

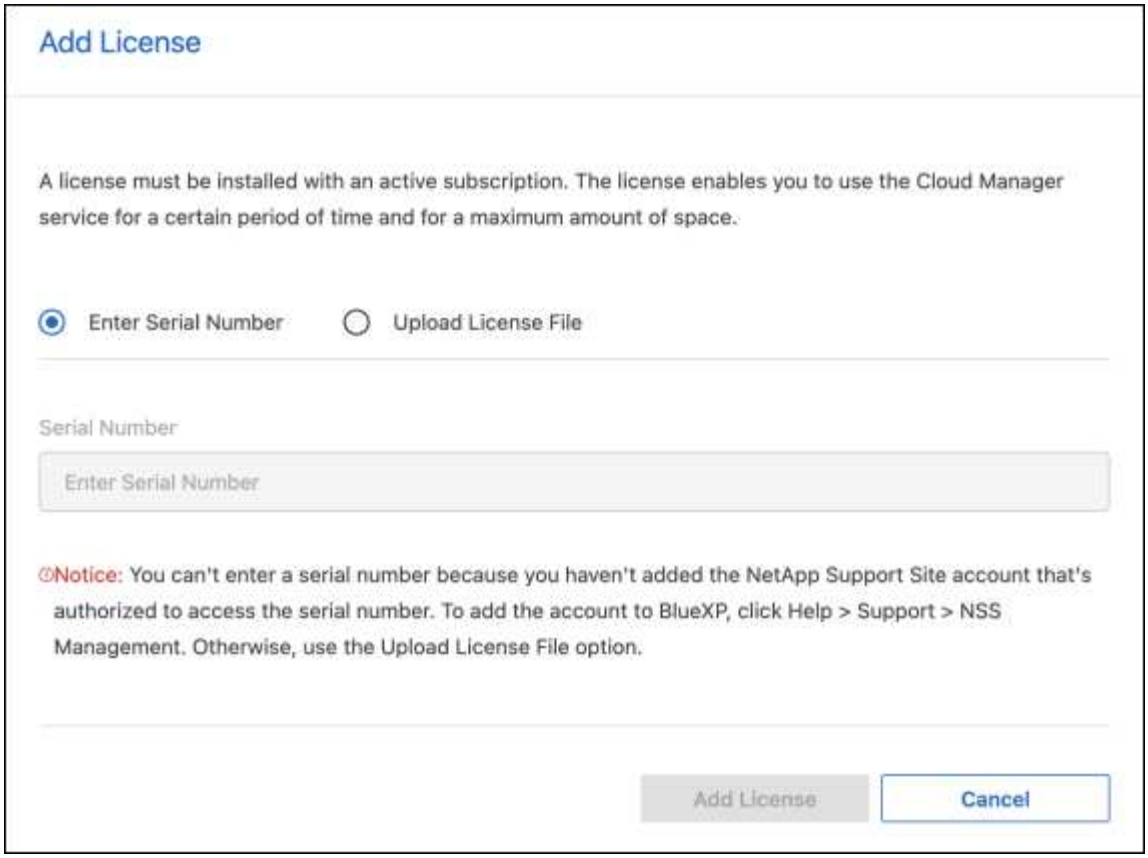
1. 在「勒索軟體復原」中，執行以下操作之一：
   - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。
   - 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」**Microsoft Azure Marketplace**。
3. 在 Azure 市場中，選擇「查看購買選項」。
4. 使用 Azure Marketplace 訂閱 * NetApp Intelligent Services* 和 * 勒索軟體復原能力 *。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。

> 系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示已在 Azure 市集訂閱 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 若要新增許可證，請選擇*新增許可證*。



8. 在新增許可證頁面中，選擇*輸入序號*，然後輸入發送給您的電子郵件中的序號。選擇*新增許可證*。
9. 要查看Licenses and subscriptions中的許可證詳細信息，請從控制台左側導航中選擇“治理”>“Licenses and subscriptions”。
   - 若要查看訂閱訊息，請選擇*訂閱*。
   - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

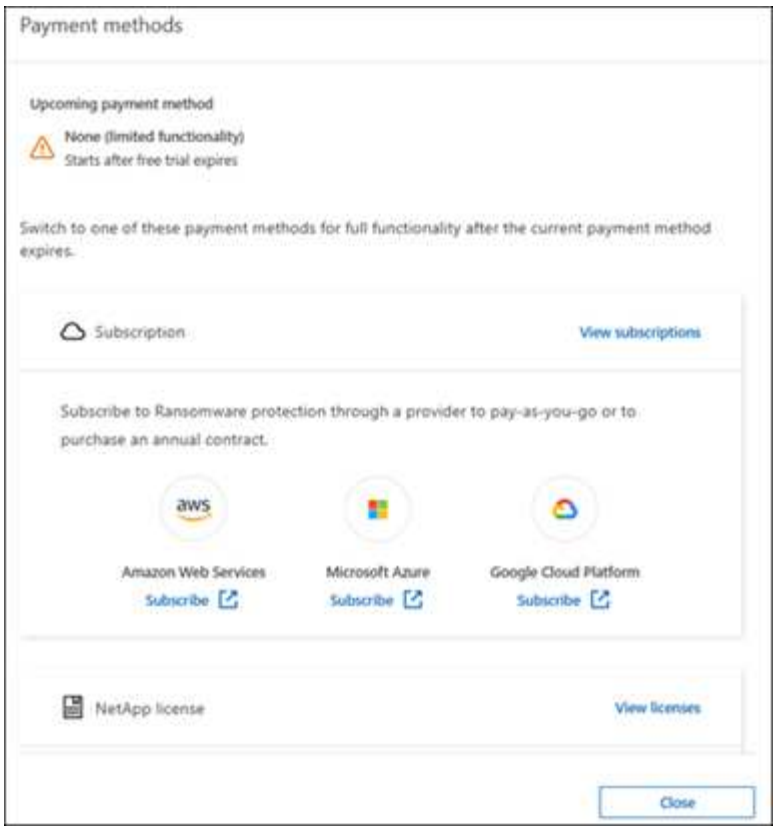
    出現一則訊息，表示已新增許可證。

透過 Google Cloud Platform Marketplace 訂閱

此流程概述如何在 Google Cloud Platform Marketplace 中直接訂閱。

步驟

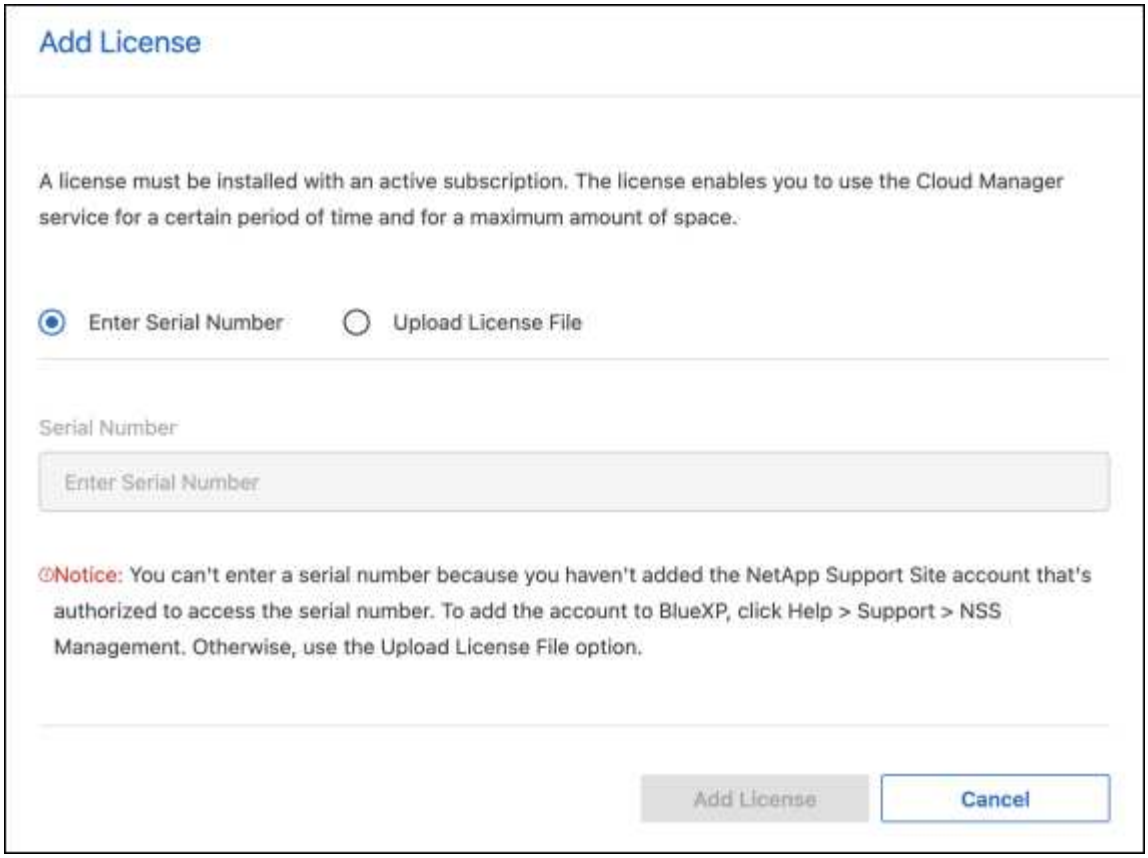
1. 在勒索軟體復原中，執行以下操作之一：
   - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。
   - 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」Google Cloud Platform Marketplace*。
3. 在 Google Cloud Platform Marketplace 中，選擇 訂閱。
4. 使用 Google Cloud Platform Marketplace 訂閱 * NetApp Intelligent Services* 和 * Ransomware Resilience *。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。

> 系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示您已在 Google Cloud Platform Marketplace 中訂閱了 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 若要將許可證新增至控制台，請選擇「新增許可證」。



8. 在新增許可證頁面中，選擇*輸入序號*。輸入發送給您的電子郵件中的序號。選擇*新增許可證*。
9. 要查看許可證詳細信息，請從控制台左側導航中選擇“治理”>“**Licenses and subscriptions**”。
   - 若要查看訂閱訊息，請選擇*訂閱*。
   - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

    出現一則訊息，表示已新增許可證。

自帶授權 (BYOL)

如果您想自備許可證 (BYOL)，則需要購買許可證，取得NetApp許可證文件 (NLF)，然後將許可證新增至控制台。

將您的許可證文件新增至控制台

從NetApp銷售代表購買勒索軟體恢復許可證後，您可以透過輸入勒索軟體恢復序號和NetApp支援網站 (NSS) 帳戶資訊來啟動授權。

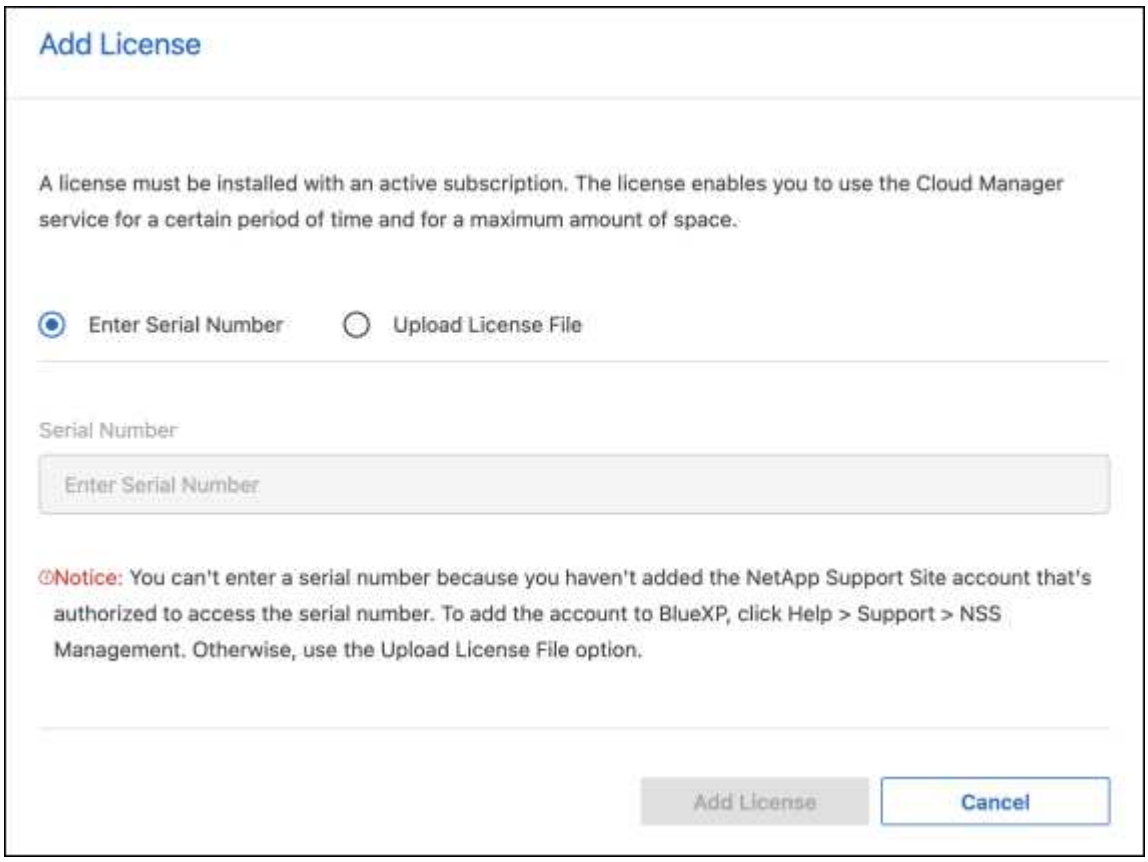
開始之前

您需要 Ransomware Resilience 序號。從您的銷售訂單中找到此號碼，或聯絡客戶團隊以取得此資訊。

步驟

1. 取得授權後，返回 Ransomware Resilience。選擇右上角的*查看付款方式*選項。或者，在免費試用即將到期的訊息中，選擇*訂閱或購買授權*。

2. 選擇「新增許可證」到控制台許可證和訂閱頁面。
3. 從「資料服務許可證」標籤中，選擇「新增許可證」。



4. 在「新增許可證」頁面中，輸入序號和NetApp支援網站帳戶資訊。
   - 如果您有控制台許可證序號並知道您的 NSS 帳戶，請選擇 輸入序號 選項並輸入該資訊。

     如果您的NetApp支援網站帳號未從下拉清單中找到， "將 NSS 帳戶新增至控制台" 。
   - 如果您有 zvondolr 授權檔案（在暗站安裝時需要），請選擇 上傳授權檔案 選項並依照指示附加檔案。
5. 選擇*新增許可證*。

結果

Licenses and subscriptions頁面顯示 Ransomware Resilience 已取得授權。

控制台許可證到期後請更新

如果您的許可期限即將到期，或者您的許可容量已達到限制，您將在勒索軟體復原 UI 中收到通知。您可以在勒索軟體復原許可證到期之前進行更新，這樣您存取掃描資料的能力就不會受到干擾。

此訊息也出現在Licenses and subscriptions以及 "通知設定"。

步驟

1. 您可以發送電子郵件給支援人員以要求更新您的許可證。

在您支付許可證費用並在NetApp支援網站註冊後，控制台會自動更新許可證。數據服務許可證頁面將在 5 到 10 分鐘內反映變更。

2. 如果控制台無法自動更新許可證，則需要手動上傳許可證文件。
   a. 您可以從NetApp支援網站取得許可證文件。
   b. 在控制台中，選擇管理 > **Licenses and subscriptions**。
   c. 選擇“資料服務許可證”選項卡，選擇要更新的序號的“操作...”圖標，然後選擇“更新許可證”。

結束 **PAYGO** 訂閱

如果您想終止 PAYGO 訂閱，您可以隨時終止。

步驟

1. 在 Ransomware Resilience 中，在右上角選擇授權選項。
2. 選擇*查看付款方式*。
3. 在下拉詳細資料中，取消勾選「目前付款方式過期後使用」方塊。
4. 選擇*儲存*。

更多資訊

- "NetApp Console授權和訂閱文檔"

發現NetApp Ransomware Resilience中的工作負載

在使用NetApp Ransomware Resilience之前，它首先需要發現工作負載資料。在發現過程中，勒索軟體復原力會分析組織內所有控制台代理程式和專案系統中的所有捲和檔案。

在「發現」儀表板中，「勒索軟體復原能力」顯示受支援且不受支援的系統配置。勒索軟體復原能力評估 Oracle 應用程式、VMware 資料儲存、檔案共用和區塊儲存。

勒索軟體復原能力無法發現使用FlexGroup 的磁碟區的工作負載。

勒索軟體復原能力會檢查您目前的備份保護、快照副本和NetApp自主勒索軟體保護選項。勒索軟體復原能力還可以偵測來自SnapCenter for VMware（用於 VM 資料儲存）、 SnapCenter for Oracle 和NetApp Backup and Recovery （用於檔案共用和 VM 檔案共用）的保護資訊。然後它會推薦一些改善勒索軟體防護的方法。

雖然 Ransomware Resilience 可以識別來自 SnapCenter 的原則，但您無法透過 SnapCenter 使用 Ransomware Resilience 執行還原。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

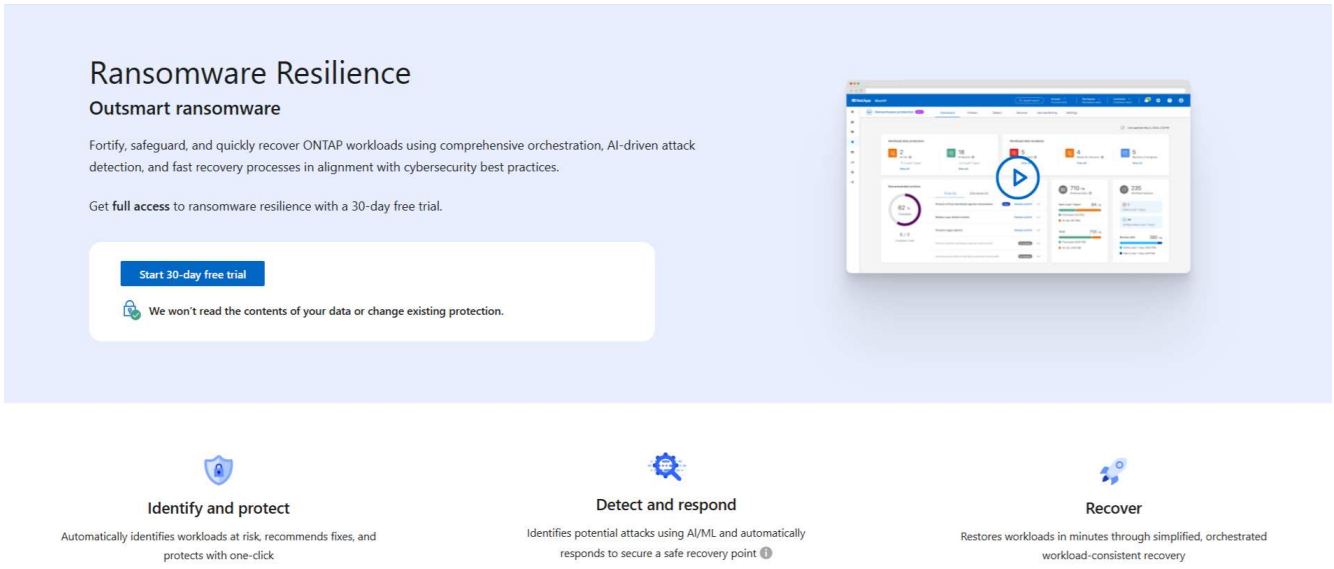
選擇要發現和保護的工作負載

在每個控制台代理程式中，選擇您想要發現工作負載的系統。

步驟

1. 從NetApp Console中，選擇 保護 > 勒索軟體保護。

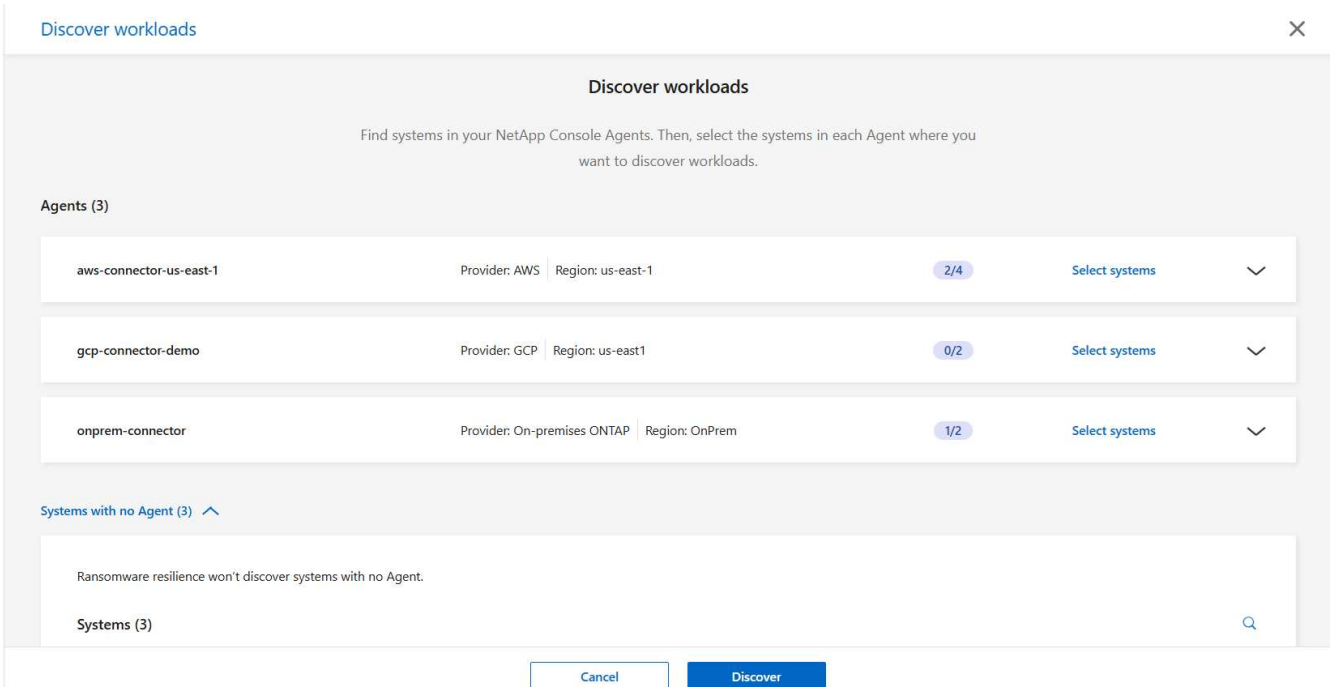
   如果這是您的第一次登錄，則會出現登入頁面。



   如果您開始免費試用，開始 **30** 天免費試用*按鈕標籤將更改為*透過發現工作負載開始。

2. 從初始登入頁面，選擇*從發現工作負載開始*。

   勒索軟體復原力可發現受支援和不受支援的系統。此過程可能需要幾分鐘。



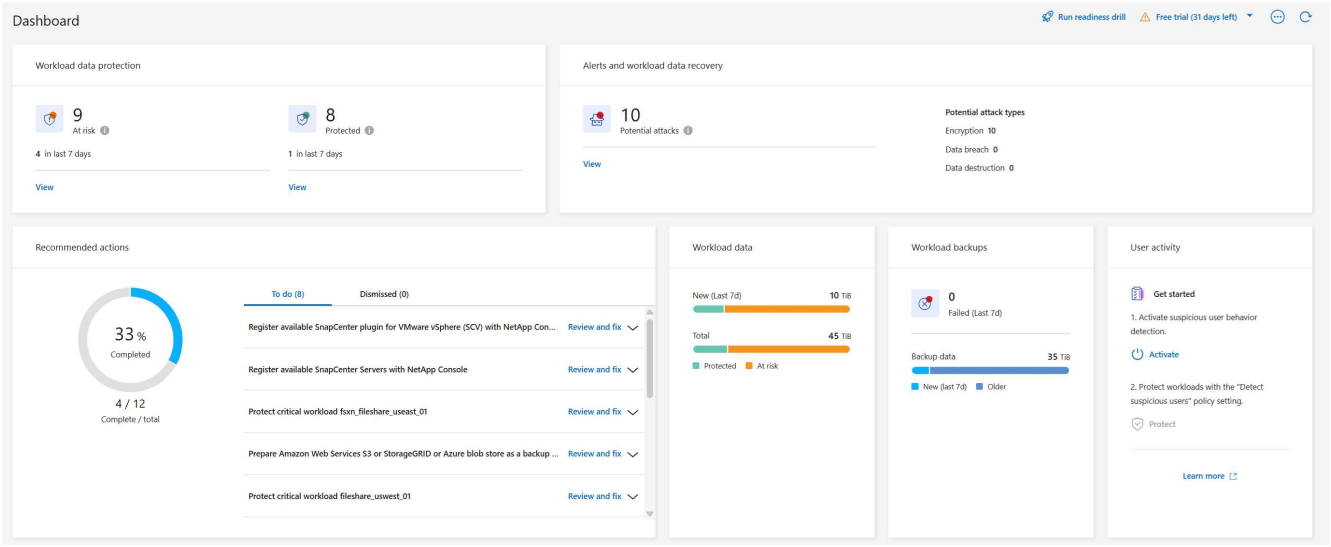
3. 若要發現特定控制台代理程式的工作負載，請選擇要發現工作負載的控制台代理旁邊的「選擇系統」。
4. 選擇您想要發現工作負載的系統。

5. 選擇*發現*。

   勒索軟體復原能力僅在選擇系統時才會發現工作負載資料。發現過程可能需要幾分鐘。

6. 若要下載已發現的工作負載列表，請選擇*下載結果*。
7. 若要顯示勒索軟體恢復儀表板，請選擇「前往儀表板」。

   儀表板顯示資料保護健康狀況。隨著新工作負載的發現，處於危險中或受保護的工作負載的數量會更新。



"了解儀表板向您顯示的內容。"

發現先前選定的系統新建立的工作負載

如果您已向先前發現的系統新增了工作負載，則需要重新啟動發現以保護新的工作負載。

步驟

1. 要確定上次發現的時間，請查看勒索軟體恢復儀表板右上角「刷新」圖示旁的日期和時間戳記。
2. 在控制台中，選擇“刷新”圖示以尋找新的工作負載。

> 如果您發現已發現的系統中存在未顯示的捲，則這些卷可能不受支援。若要尋找不支援的磁碟區列表，請前往「設定」選單，然後選擇「工作負載發現」卡中的操作選單，下載支援和不支援的磁碟區的 JSON 報表。

發現新系統

如果您已經發現了系統，您可以找到新的或以前未選擇的系統。

步驟

1. 從「勒索軟體復原」選單中，選擇垂直方向 右上角的“category='inline-code'/> 選項。從下拉式選單中選擇“設定”。
2. 在工作負載發現卡中，選擇*發現工作負載*。發現過程可能需要幾分鐘。載入圖示顯示進度。
3. 勒索軟體復原力可以發現受支援和不受支援的系統。如果系統的ONTAP版本低於所需版本，則不支援該系

統。當您將滑鼠停留在某個不支援的系統上時，工具提示會顯示原因。選擇您想要發現工作負載的系統。

4. 選擇*發現*。

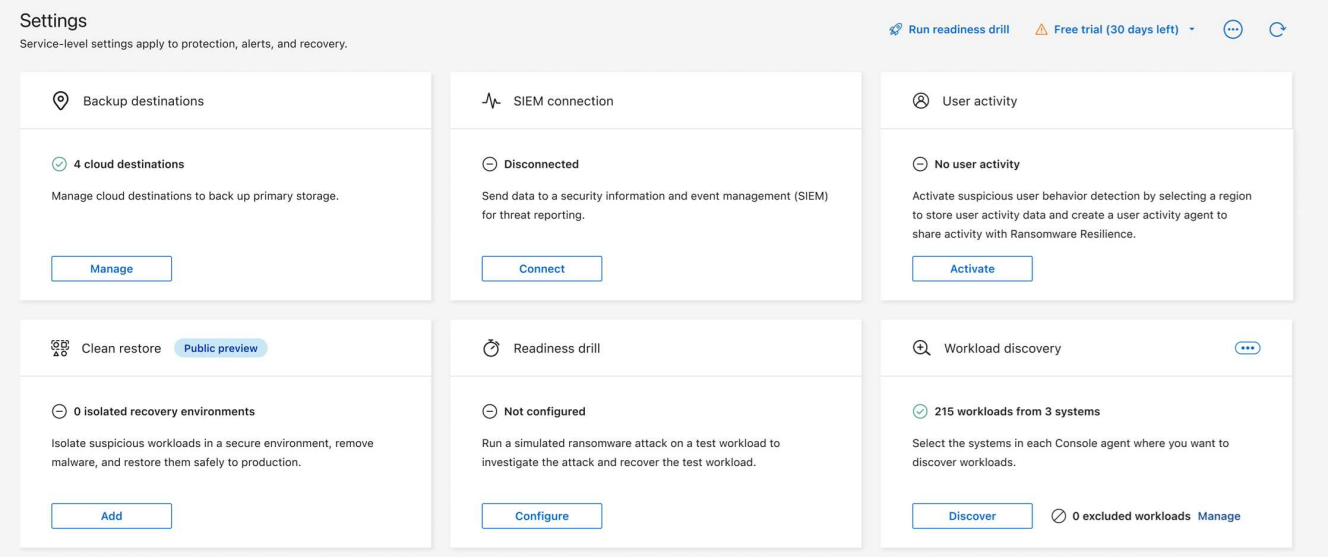
排除工作負載

勒索軟體復原功能可讓您將系統中的特定工作負載排除在勒索軟體保護和偵測之外。

您只能排除受支援且已成功發現的工作負載。您可以隨時修改已排除的工作負載清單。對於未納入勒索軟體復原功能的工作負載，您無需付費。

將工作負載新增至排除的工作負載清單中

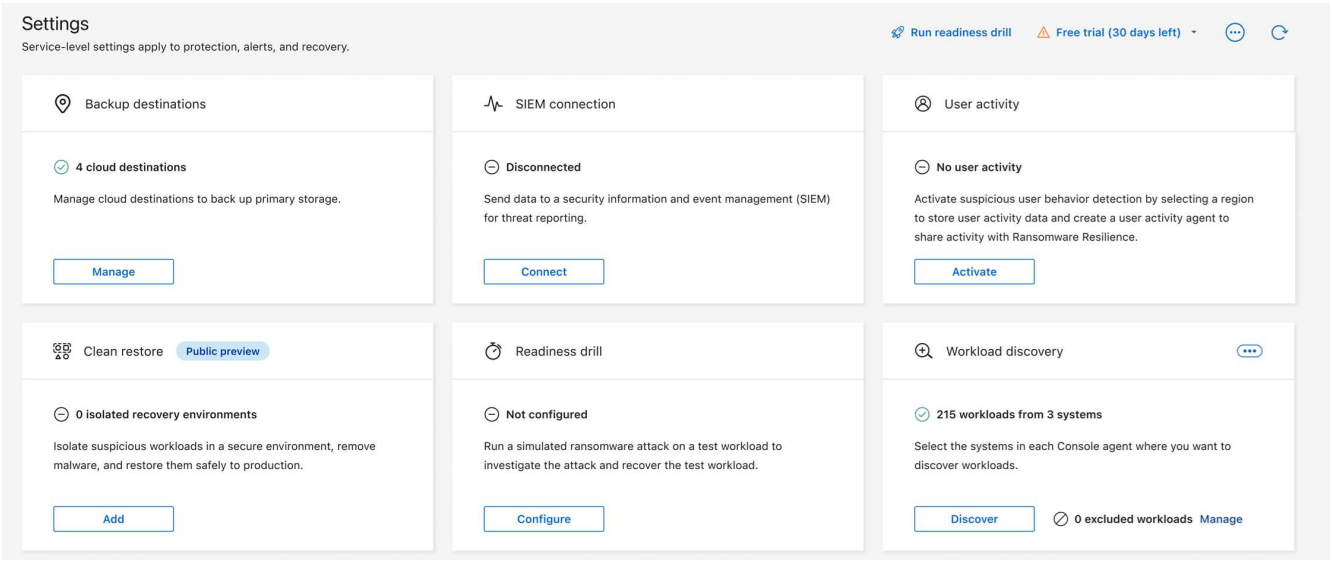
1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表板中，找到「工作負載發現」儀表板。該卡片標明了已排除的工作負載數量。若要新增工作負載，請在排除的工作負載旁邊選擇管理。



3. 在「排除的工作負載」頁面中，選擇新增。
4. 選擇要排除的工作負載，然後按一下新增。
5. 請查看「已排除的工作負載」頁面，以了解已排除的工作負載。新增工作負載時，其名稱旁會顯示進度指示器。如果工作負載未成功排除，則不會顯示在頁面上。

從排除的工作負載清單中移除工作負載

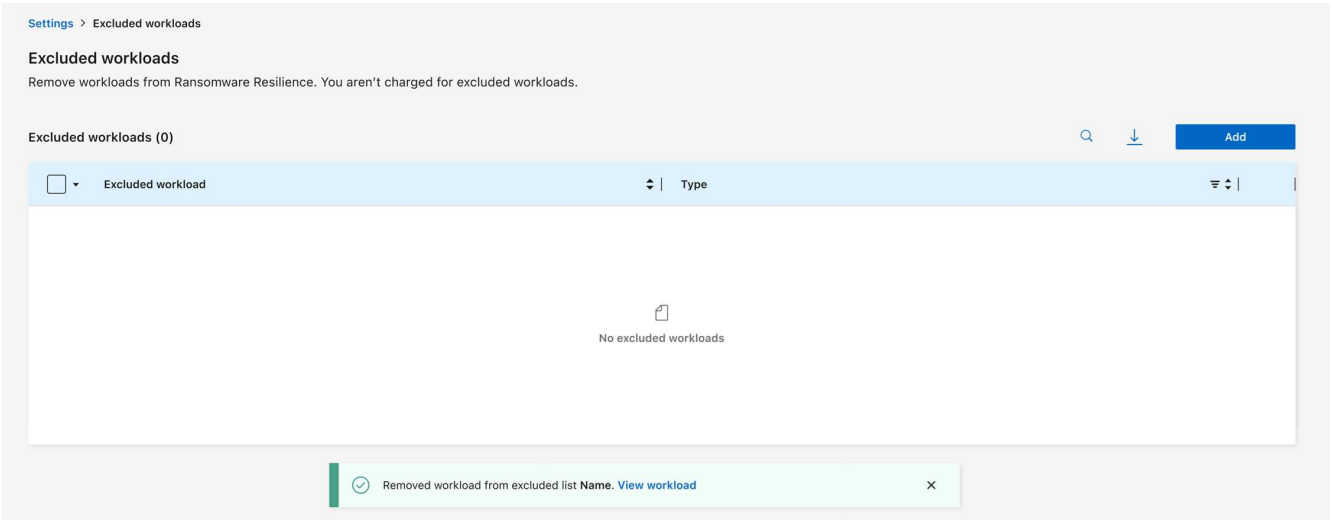
1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表板中，找到「工作負載發現」儀表板。該卡片標明了已排除的工作負載數量。在排除的工作負載旁邊，選擇管理。



3. 若要從排除清單中刪除單一工作負載，請選擇要刪除的工作負載的操作功能表。

   若要刪除多個工作負載，請選取要刪除的工作負載旁的複選框，然後選擇從排除清單中刪除。

4. 在對話方塊中，選擇「刪除」以確認要從排除清單中刪除工作負載。
5. 如果成功從排除的工作負載清單中刪除工作負載，則「排除的工作負載」頁面上將顯示成功訊息，且該工作負載將不再出現在已排除的工作負載清單中。如果操作失敗，將顯示錯誤訊息；請重試該操作。



在NetApp Ransomware Resilience中進行勒索軟體攻擊準備演練

透過模擬對新樣本工作負載的攻擊來運行勒索軟體攻擊準備演習。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。根據需要經常進行演練。

您的實際工作量資料不會受到影響。

您可以對 NFS 和 CIFS (SMB) 工作負載進行準備情況演練。

配置勒索軟體攻擊準備演習

在執行模擬之前，請在「設定」頁面上設定演練。從頂部選單中的操作選項存取設定頁面。

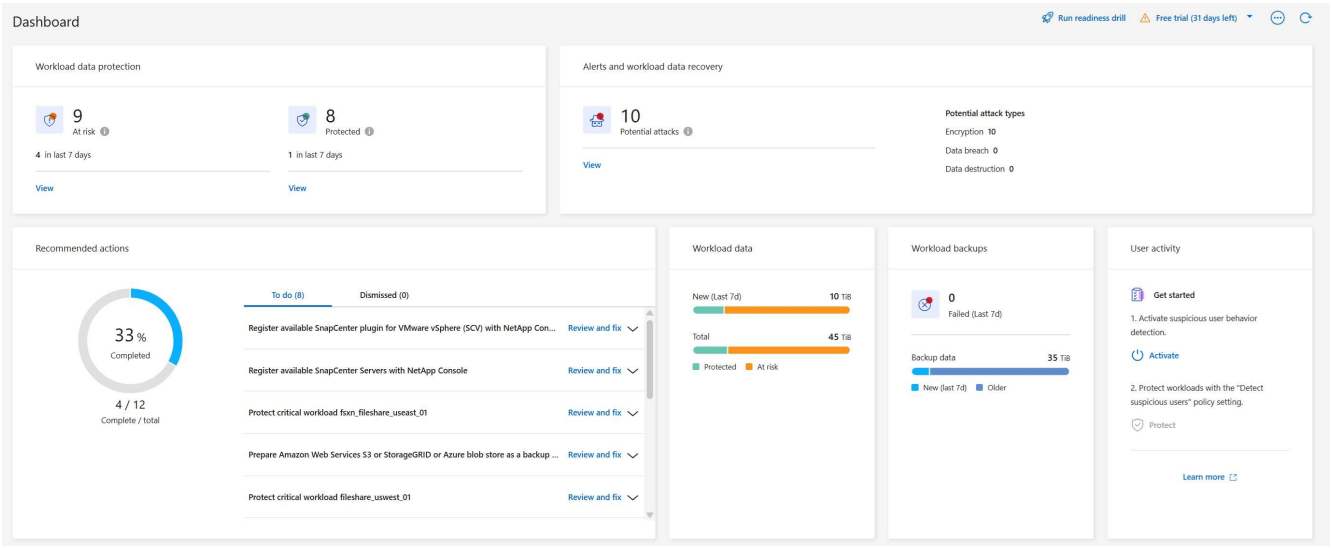
以下情況需要輸入使用者名稱和密碼：

- 如果先前選擇的儲存虛擬機器的使用者名稱或密碼發生更改
- 如果您選擇不同的 CIFS (SMB) 儲存體 VM
- 如果您輸入不同的測試工作負載名稱

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

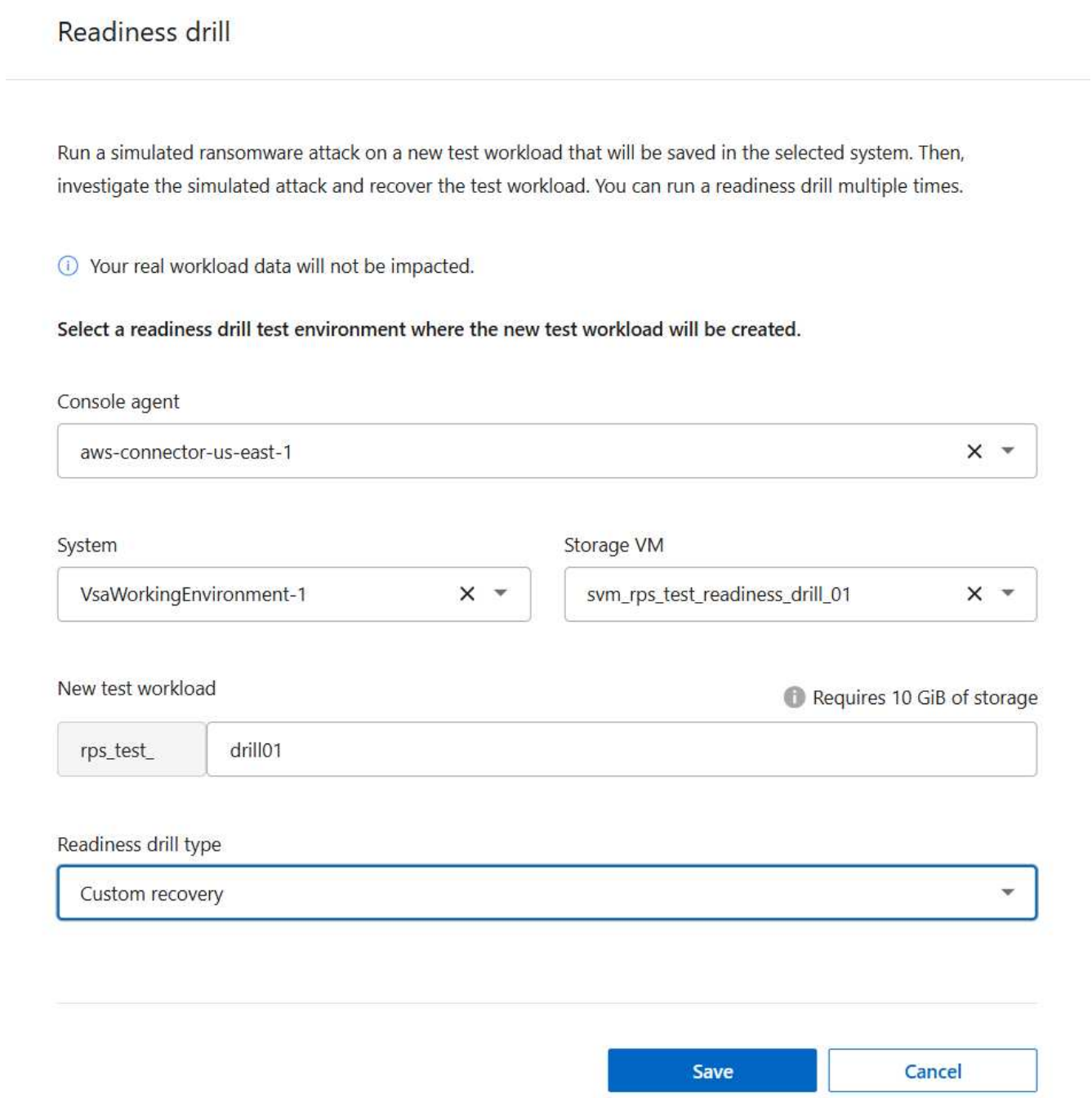
步驟

1. 從NetApp Ransomware Resilience選單中，選擇右上角的 執行準備演練 按鈕。



2. 在設定頁面的準備練習卡中，選擇*配置*。

   控制台顯示配置準備度演練頁面。



3. 執行以下操作：
   a. 選擇您想要用於準備情境演練的控制台代理程式。
   b. 選擇一個測試系統。
   c. 選擇測試儲存 SVM。
   d. 如果您選擇了 CIFS (SMB) 儲存虛擬機，則會出現使用者名稱和密碼欄位。輸入儲存虛擬機器的使用者名稱和密碼。
   e. 選擇準備演習類型。若要從加密資料外洩手動恢復，請選擇自訂恢復。若要從可疑用戶活動中恢復，請選擇資料外洩。
   f. 輸入要建立的新測試工作負載的名稱。名稱中不要包含破折號。

4. 選擇*儲存*。

您可以稍後使用「設定」頁面編輯準備演練配置。

開始準備演習

配置準備狀況演練後，即可開始演練。

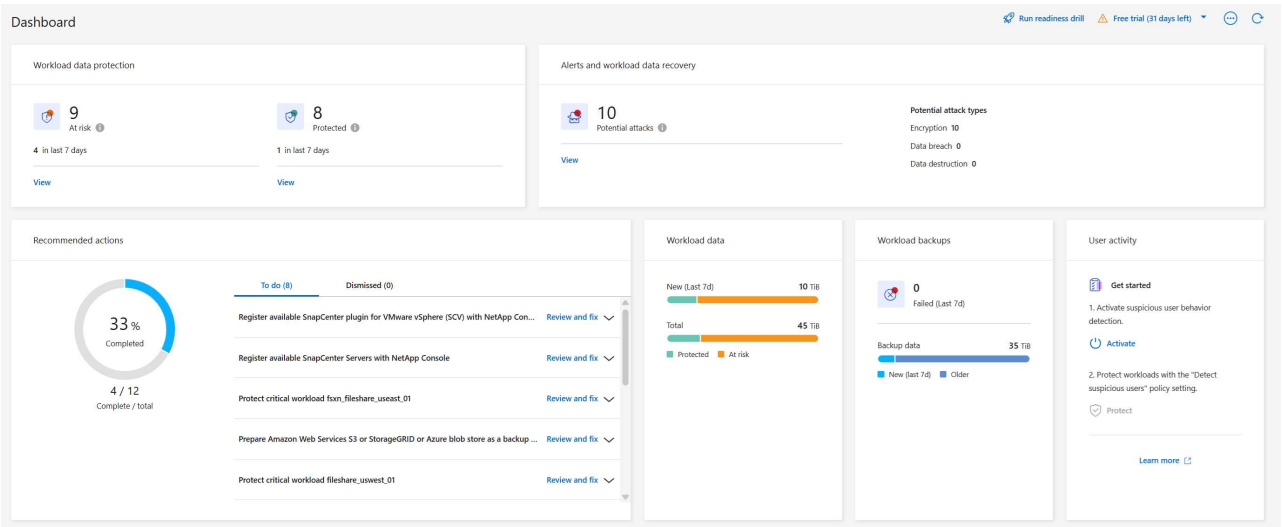
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

當您開始準備演習時，勒索軟體復原力會跳過學習模式並以主動模式開始演習。工作負載的偵測狀態為「活動」。

當最近分配了檢測策略並且勒索軟體恢復掃描工作負載時，工作負載可以具有勒索軟體檢測*學習模式*狀態。

步驟

1. 執行下列操作之一：
   - 從勒索軟體復原選單中，選擇右上角的「運行準備演練」按鈕。



   - 或者，從「設定」頁面的「準備好練習卡」中選擇「開始」。

演練運行時，您無法編輯準備演練配置。您可以重置鑽孔機以停止它並修改配置。

響應戰備演習警報

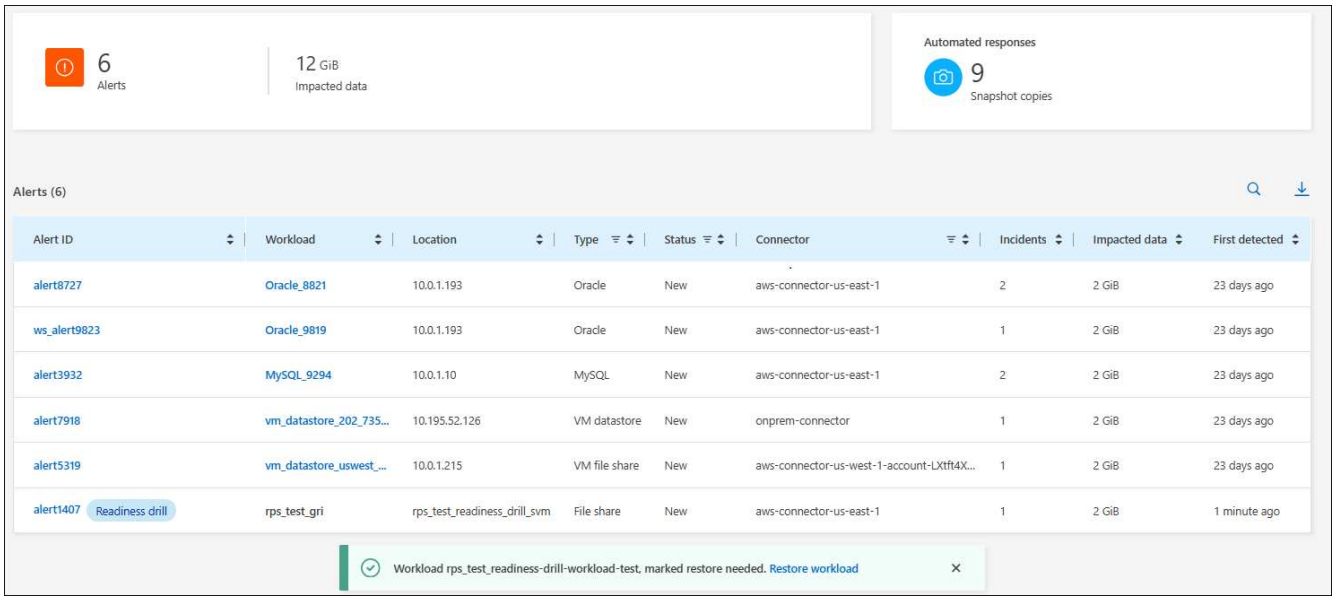
透過回應準備演習警報來測試您的準備。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

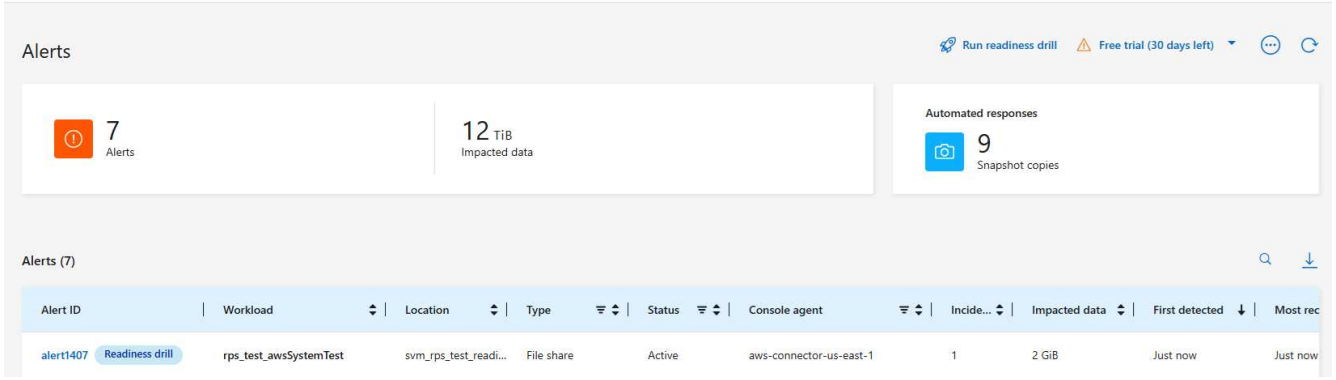
步驟

1. 從勒索軟體恢復選單中，選擇*警報*。

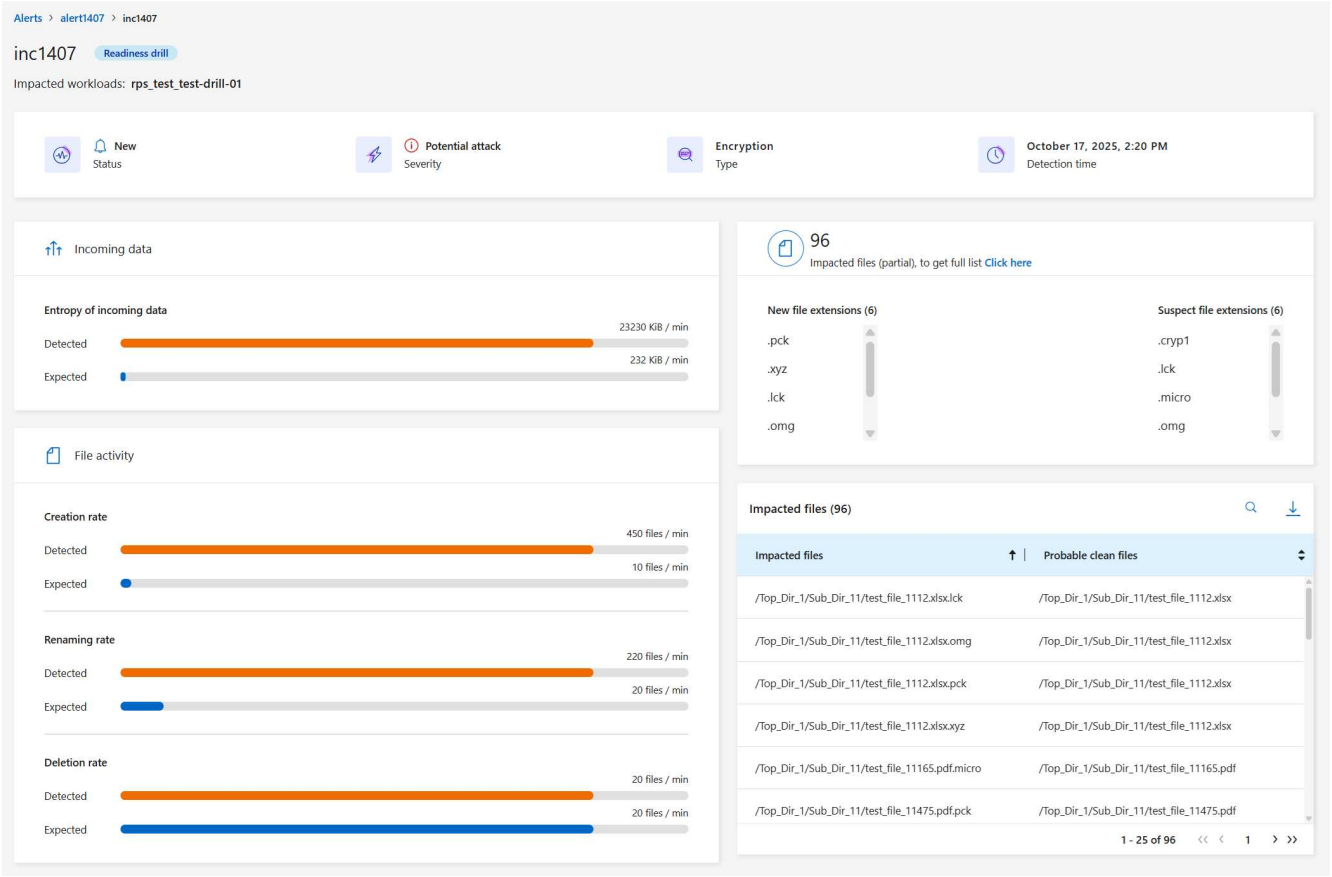
   控制台顯示警報頁面。在警報 ID 欄位中，您會在 ID 旁看到「準備好演練」。



2. 選擇帶有「準備演習」指示的警報。事件警報清單出現在警報詳細資訊頁面。



3. 查看警報事件。
4. 選擇一個警報事件。



以下是需要注意的一些事項：

- 查看潛在攻擊的嚴重性。

  如果嚴重性表明使用者涉嫌惡意活動，請檢查使用者名稱。您還可以"封鎖該用戶。"

- 查看文件活動和可疑進程：
  - 查看傳入的檢測數據與預期數據的比較。
  - 查看偵測到的文件的建立率與預期率的比較。
  - 查看偵測到的檔案重新命名率與預期率的比較。
  - 查看刪除率與預期刪除率的比較。
- 查看受影響文件的清單。查看可能導致攻擊的擴展。
- 透過查看受影響的檔案和目錄的數量來確定攻擊的影響和廣度。

恢復測試工作負載

審查準備情況演習警報後，如有必要，恢復測試工作量。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

步驟

1. 返回警報詳細資訊頁面。

2. 如果需要恢復測試工作負載，請執行下列操作：
   - 選擇*標記需要恢復*。
   - 查看確認訊息，然後在確認框中選擇*標記需要恢復*。
     - 從勒索軟體恢復選單中，選擇*恢復*。
     - 選擇要復原的標示為「準備演練」的測試工作負載。
     - 選擇*恢復*。
     - 在「還原」頁面中，提供還原的資訊：
   - 選擇來源快照副本。
   - 選擇目標磁碟區。
3. 在恢復審核頁面中，選擇*恢復*。

   控制台在恢復頁面上顯示準備演練恢復的狀態為「進行中」。

   恢復完成後，控制台將工作負載的狀態變更為*已復原*。

4. 查看恢復的工作負載。

有關恢復過程的詳細信息，請參閱"從勒索軟體攻擊中恢復（事件被消除後）"。

準備演練後更改警報狀態

審查準備情況演習警報並恢復工作量後，根據需要變更警報狀態。

需要控制台角色 組織管理員、資料夾或專案管理員或勒索軟體復原管理員。 "了解所有服務的控制台存取角色"。

步驟

1. 返回警報詳細資訊頁面。
2. 再次選擇警報。
3. 透過選擇*編輯狀態*來指示狀態，並將狀態變更為以下之一：
   - 已解除：如果您懷疑該活動不是勒索軟體攻擊，請將狀態變更為已解除。

     解除攻擊後，您將無法將其改回。如果您解除工作負載，則為應對潛在勒索軟體攻擊而自動取得的所有快照副本都將永久刪除。如果您解除警報，則準備演習即視為完成。

   - 已解決：事件已得到緩解。

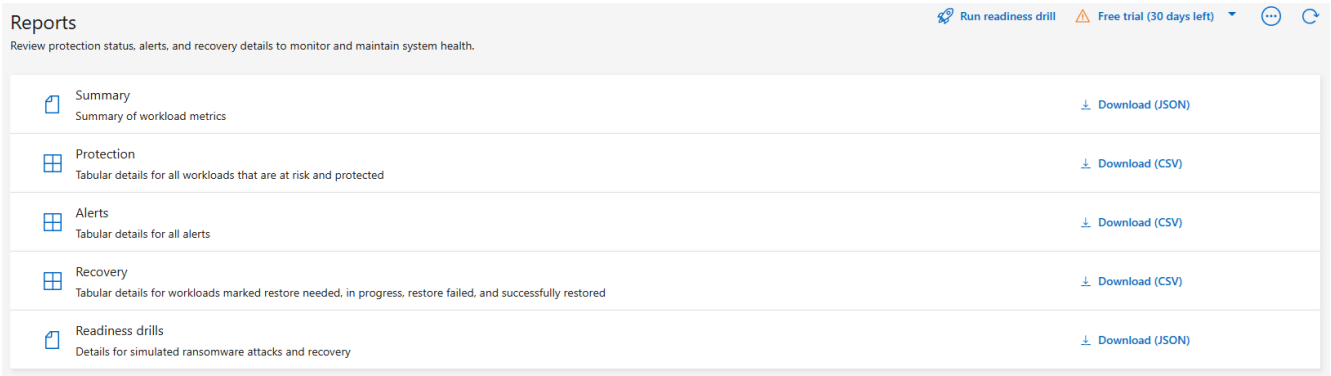
審查準備演習報告

準備演習完成後，您可能需要查看並儲存演習報告。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"了解NetApp Console的勒索軟體復原角色"。

步驟

1. 從勒索軟體恢復選單中，選擇*報告*。



2. 選擇*準備演習*和*下載*以下載準備演習報告。

在NetApp Ransomware Resilience中配置保護設置

在 NetApp Ransomware Resilience 設定標籤中，您可以設定備份目的地、執行攻擊準備演練、設定工作負載偵測，或設定可疑使用者活動偵測。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

*您可以在「設定」頁面做什麼？ *在「設定」頁面中，您可以執行以下操作：

- 透過進行準備演習來模擬勒索軟體攻擊，並對模擬勒索軟體警報做出回應。有關詳細信息，請參閱"進行勒索軟體攻擊準備演習" 。
- 配置工作負載發現。
- 配置可疑用戶活動報告。如需詳細資訊，請參閱 "可疑的用戶活動"。
- 新增備份目的地。
- 連接您的安全資訊和事件管理系統（SIEM）以進行威脅分析和偵測。啟用威脅偵測後，系統會自動將資料傳送到您的 SIEM 進行威脅分析。如需詳細資訊，請參閱 "將 NetApp Ransomware Resilience 連接到 SIEM"。

直接存取設定頁面

您可以從頂部選單附近的“操作”選項輕鬆存取“設定”頁面。

1. 從勒索軟體復原能力中，選擇垂直 ⋮ …右上角的選項。
2. 從下拉式選單中選擇*設定*。

模擬勒索軟體攻擊

透過模擬對新建立的範例工作負載的勒索軟體攻擊來進行勒索軟體準備演習。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。您可以多次執行勒索軟體準備演習。

有關詳細信息，請參閱"進行勒索軟體攻擊準備演習"。

配置工作負載發現

您可以設定工作負載發現來自動發現環境中的新工作負載。

1. 在「設定」頁面中，找到「工作負載發現」圖塊。
2. 在「工作負載發現」圖塊中，選擇「發現工作負載*」。

   此頁面顯示先前未選擇的系統的控制台代理、新可用的控制台代理程式和新可用的系統。此頁面不顯示先前選擇的系統。

3. 選擇您想要發現工作負載的控制台代理程式。
4. 查看系統清單。
5. 勾選您想要發現工作負載的系統，或選擇表格頂部的方塊以發現所有已發現工作負載環境中的工作負載。
6. 根據需要對其他系統執行此操作。
7. 選擇「發現」使勒索軟體復原功能自動發現所選控制台代理程式中的新工作負載。

在「設定」中的「工作負載發現」卡片中，選擇操作選單 ... 然後下載報告（**JSON**）以查看系統中支援和不支援的工作負載清單。

新增備份目標

勒索軟體復原能力可以識別尚未有任何備份的工作負載以及尚未分配任何備份目標的工作負載。

為了保護這些工作負載，您應該新增備份目標。您可以選擇以下備份目標之一：

- NetAppStorageGRID
- 亞馬遜網路服務（AWS）
- 谷歌雲端平台
- 微軟 Azure

Amazon FSx for NetApp ONTAP 和 Azure NetApp Files 中的工作負載無法使用備份目標。請使用原生備份解決方案執行備份作業：FSx for ONTAP 備份服務或 Azure NetApp Files 備份服務。

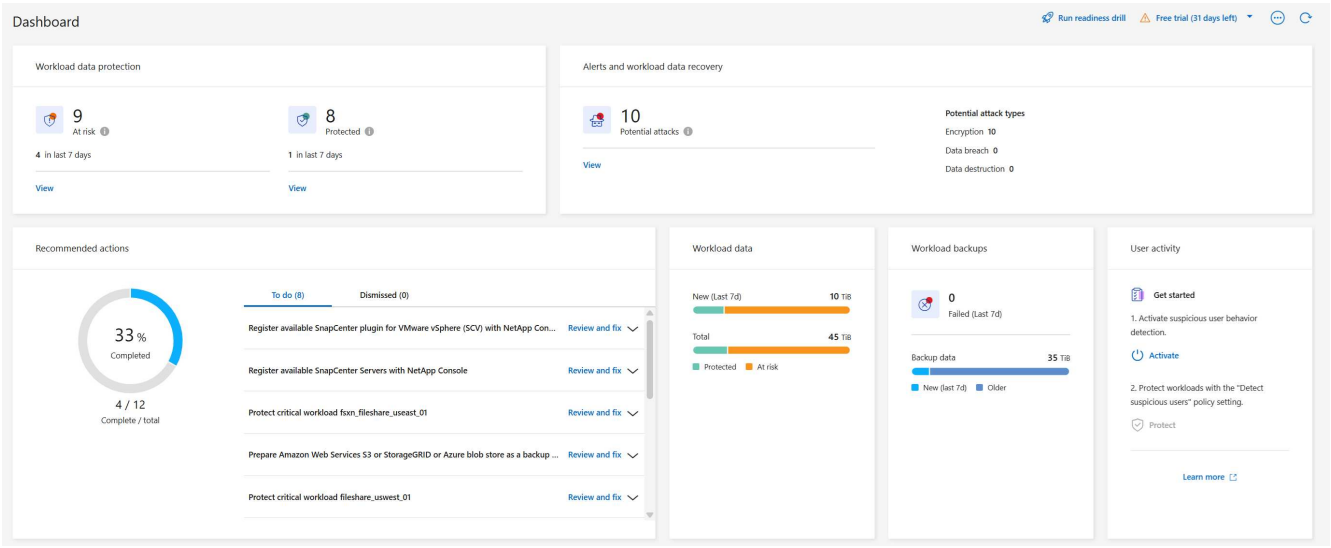
您可以根據儀表板中的建議操作或存取功能表上的「設定」選項來新增備份目標。

從儀表板的建議操作存取備份目標選項

儀表板提供了許多建議。一個建議可能是配置備份目標。

步驟

1. 在勒索軟體恢復儀表板中，請查看「建議的動作」窗格。



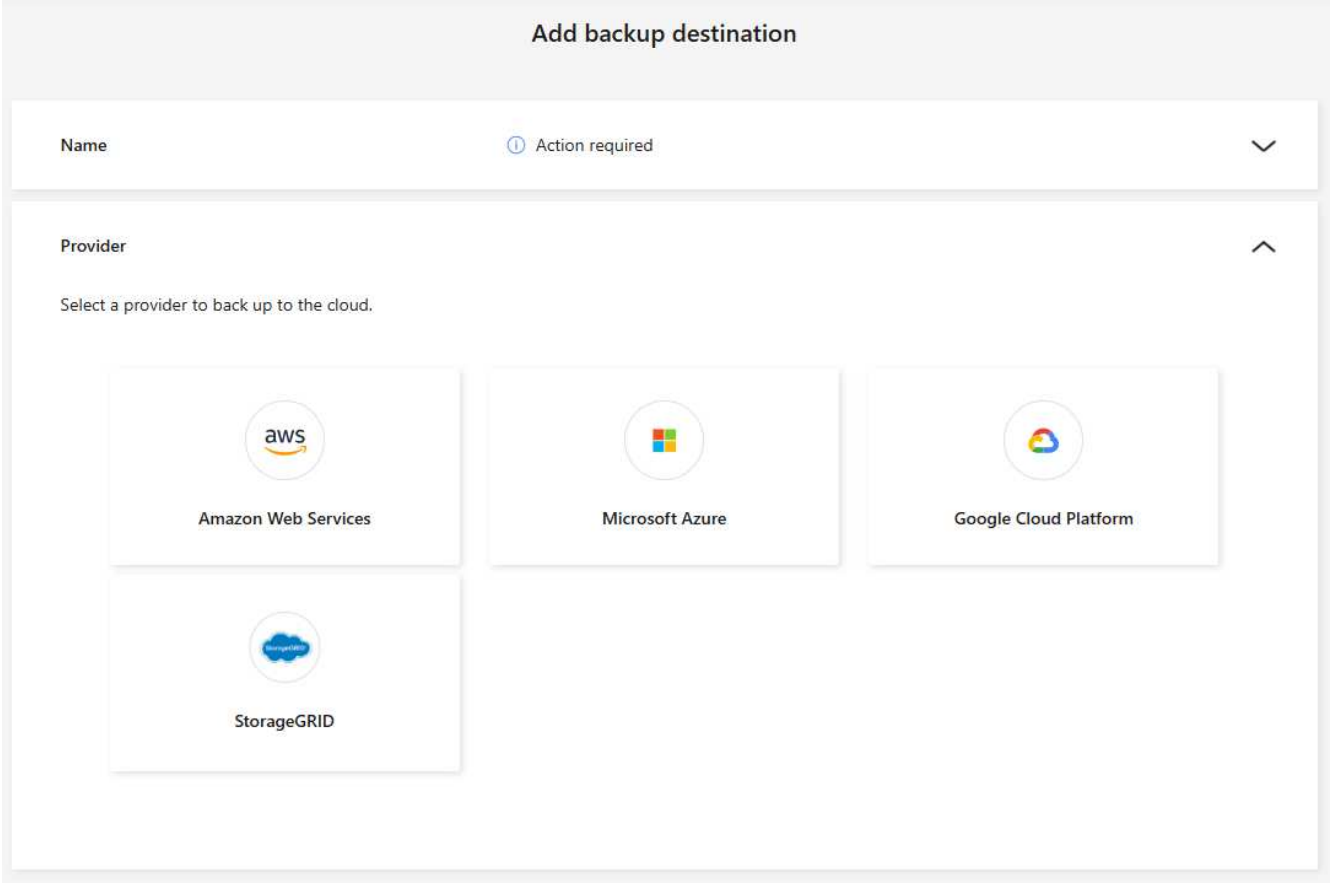
2. 從儀表板中，選擇「準備<備份提供者>作為備份目標」的建議的*審查和修復*。
3. 根據備份提供者的指示繼續操作。

新增**StorageGRID**作為備份目標

若要將NetApp StorageGRID設定為備份目標，請輸入下列資訊。

步驟

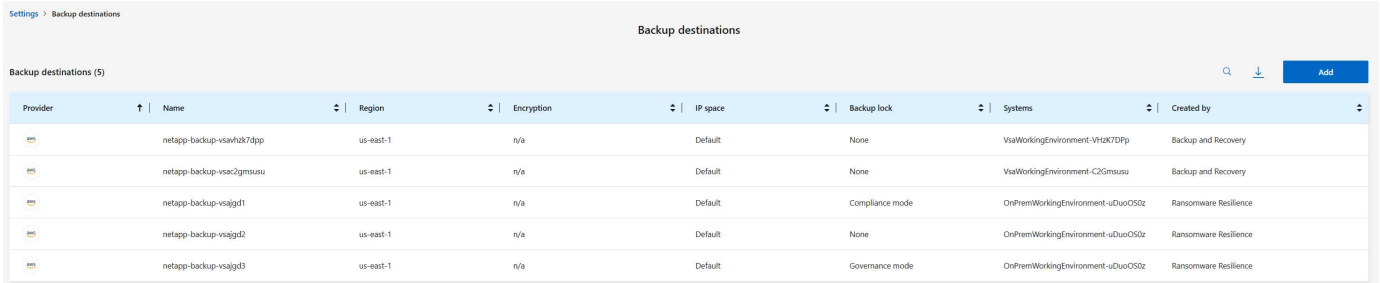
1. 在*設定 > 備份目標*頁面中，選擇*新增*。
2. 輸入備份目標的名稱。



3. 選擇* StorageGRID*。
4. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：
   - 提供者設定：
     - 建立一個新的儲存桶或自帶儲存桶來儲存備份。
     - StorageGRID網關完全限定網域名稱、連接埠、 StorageGRID存取金鑰和金鑰憑證。
   - 網路：選擇 IP 空間。
     - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
5. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。



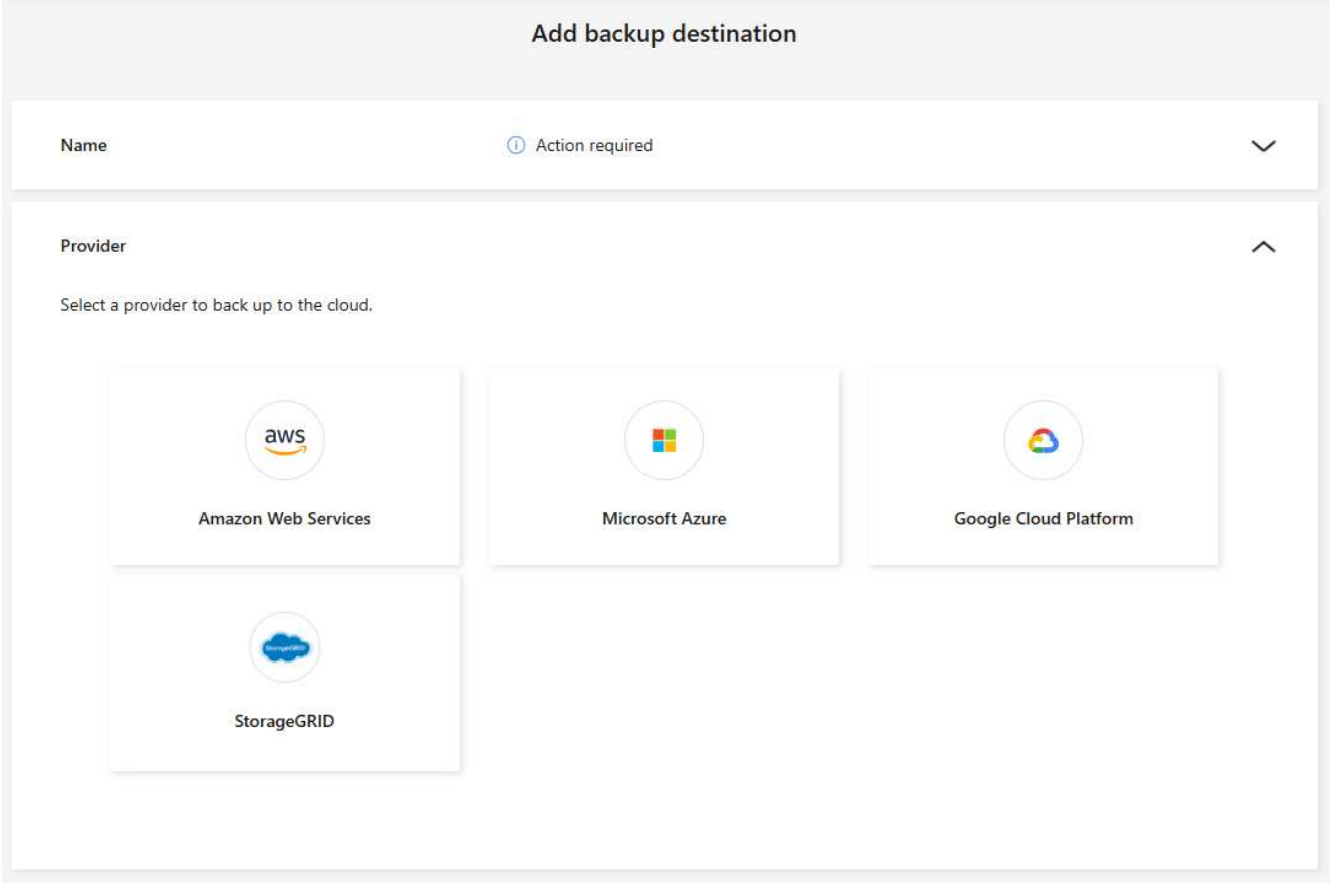
新增 **Amazon Web Services** 作為備份目標

若要將 AWS 設定為備份目標，請輸入以下資訊。

有關在控制台中管理 AWS 存儲的詳細信息，請參閱 "管理您的 Amazon S3 儲存桶"。

步驟

1. 在*設定 > 備份目標*頁面中，選擇*新增*。
2. 輸入備份目標的名稱。



3. 選擇*Amazon Web Services*。
4. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：
   - 提供者設定：
     - 建立一個新的儲存桶，如果控制台中已經存在儲存桶，請選擇一個現有儲存桶，或使用您自己的儲存桶來儲存備份。
     - AWS 帳戶、區域、AWS 憑證的存取金鑰和金鑰

       "如果您想要自備儲存桶，請參閱新增 S3 儲存桶" 。
   - 加密：如果您正在建立新的 S3 儲存桶，請輸入提供者提供給您的加密金鑰資訊。如果您選擇現有儲存桶，加密資訊已經可用。

     預設情況下，儲存桶中的資料使用 AWS 管理的金鑰加密。您可以繼續使用 AWS 管理的金鑰，也可以使用您自己的金鑰管理資料的加密。

- 網路：選擇 IP 空間以及是否使用私有端點。
  - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
  - 或者，選擇是否使用您先前配置的 AWS 私人終端節點 (PrivateLink)。

    如果您想使用 AWS PrivateLink，請參閱 "適用於 Amazon S3 的 AWS PrivateLink"。
- 備份鎖定：選擇是否希望勒索軟體復原功能保護備份不被修改或刪除。此選項使用NetApp DataLock 技術。每個備份將在保留期內鎖定，或至少 30 天，再加上最多 14 天的緩衝期。

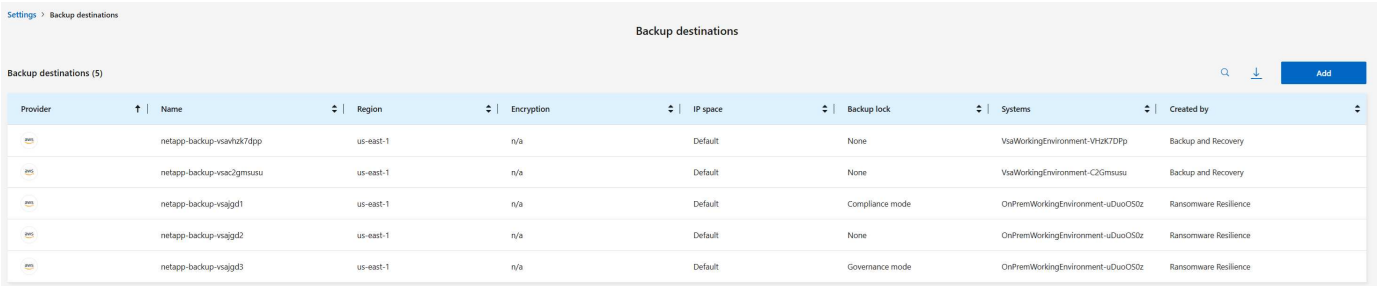
  如果您現在配置備份鎖定設置，則在配置備份目標後您將無法變更該設定。

  - 治理模式：特定使用者（具有 s3:BypassGovernanceRetention 權限）可以在保留期間內覆寫或刪除受保護的檔案。
  - 合規模式：使用者在保留期間內無法覆寫或刪除受保護的備份檔案。

5. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。



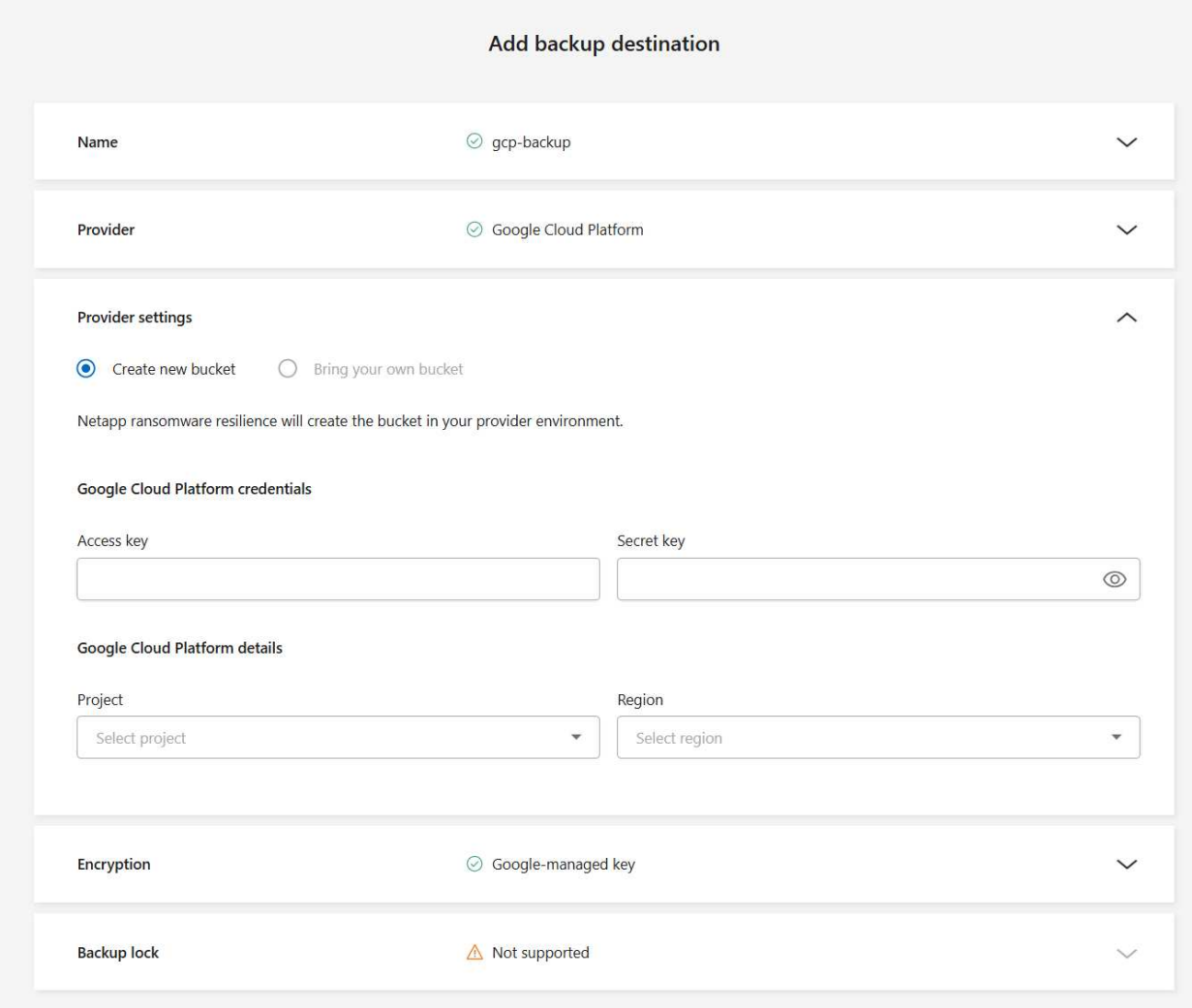
新增 **Google Cloud Platform** 作為備份目標

若要將 Google Cloud Platform (GCP) 設定為備份目標，請輸入以下資訊。

有關在控制台中管理 GCP 存儲的詳細信息，請參閱 "Google Cloud 中的控制台代理安裝選項"。

步驟

1. 在*設定 > 備份目標*頁面中，選擇*新增*。
2. 輸入備份目標的名稱。
3. 選擇*Google Cloud Platform*。
4. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：
   - 提供者設定：
     - 建立一個新的儲存桶。輸入存取密鑰和密鑰。
     - 輸入或選擇您的 Google Cloud Platform 專案和區域。



- 加密：如果您正在建立新的儲存桶，請輸入提供者提供給您的加密金鑰資訊。如果您選擇現有儲存桶，加密資訊已經可用。

  預設情況下，儲存桶中的資料使用 Google 管理的金鑰加密。您可以繼續使用 Google 管理的金鑰。

- 網路：選擇 IP 空間以及是否使用私有端點。
  - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
  - 或者，選擇是否使用您先前設定的 GCP 專用端點 (PrivateLink)。

5. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。

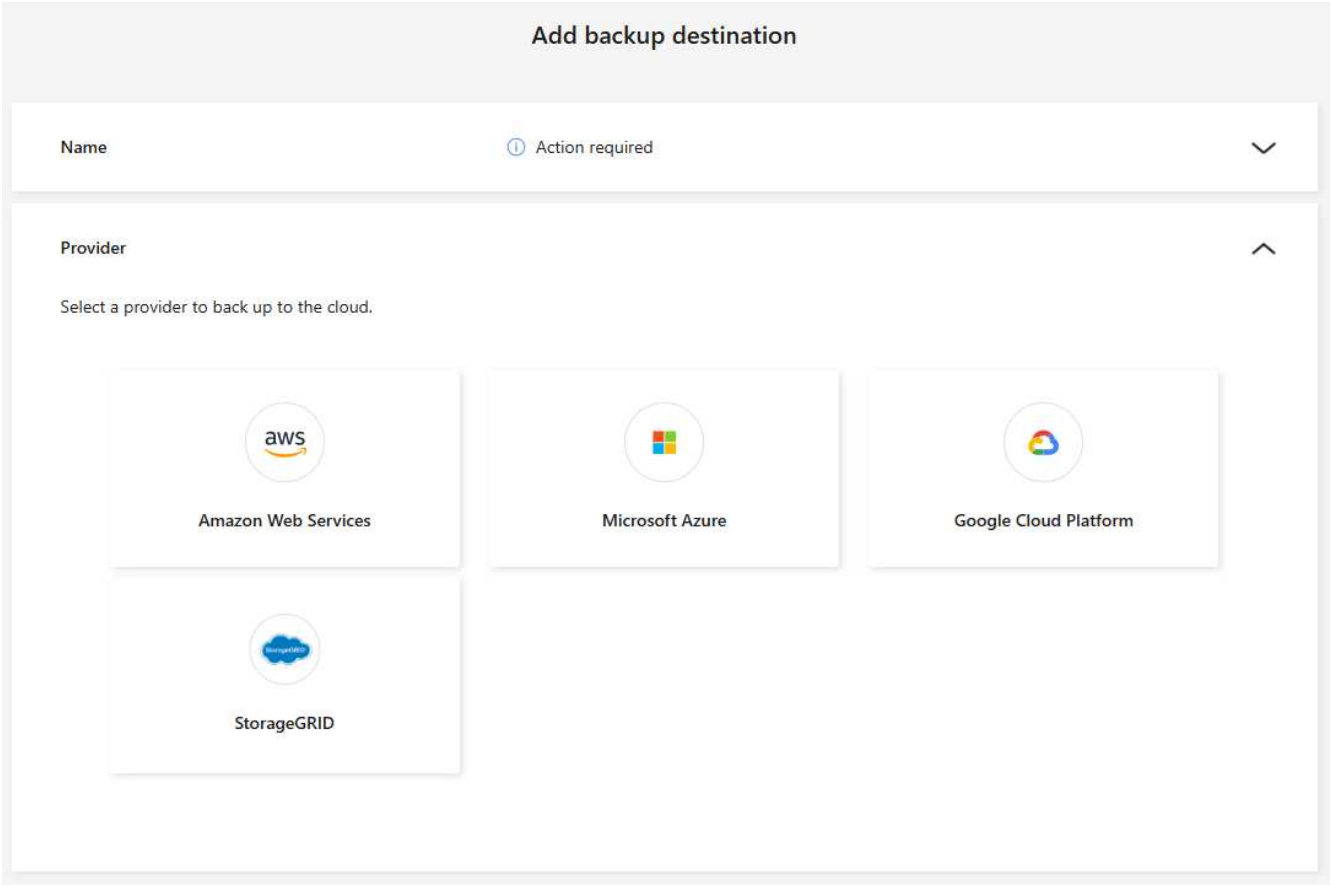
新增 **Microsoft Azure** 作為備份目標

若要將 Azure 設定為備份目標，請輸入以下資訊。

有關在控制台中管理 Azure 憑證和市場訂閱的詳細信息，請參閱 "管理 Azure 憑證和市集訂閱"。

步驟

1. 在*設定 > 備份目標*頁面中，選擇*新增*。
2. 輸入備份目標的名稱。



3. 選擇“**Azure**”。
4. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：
   - 提供者設定：
     - 建立一個新的儲存帳戶，如果控制台中已經存在，請選擇一個現有的儲存帳戶，或使用您自己的儲存帳戶來儲存備份。
     - Azure 憑證的 Azure 訂閱、區域和資源群組

     "如果您想自備儲存帳戶，請參閱新增 Azure Blob 儲存體帳戶" 。
   - 加密：如果您正在建立新的儲存帳戶，請輸入提供者提供給您的加密金鑰資訊。如果您選擇現有帳戶，加密資訊已經可用。

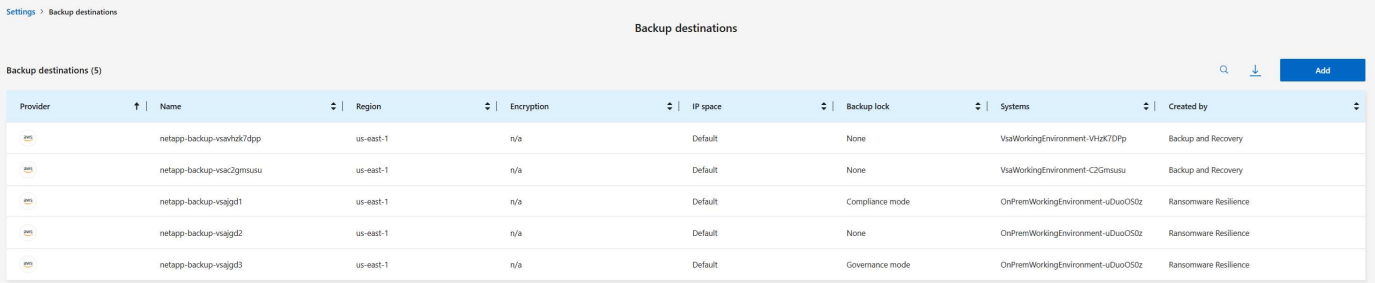
     預設情況下，帳戶中的資料會使用 Microsoft 管理的金鑰加密。您可以繼續使用 Microsoft 管理的金鑰，也可以使用您自己的金鑰管理資料的加密。
   - 網路：選擇 IP 空間以及是否使用私有端點。
     - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
     - 或者，選擇是否使用先前設定的 Azure 專用終端點。

     如果您想使用 Azure PrivateLink，請參閱 "Azure PrivateLink"。

5. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。



將 NetApp Ransomware Resilience 連接到安全性與事件管理系統（SIEM），以進行威脅分析與偵測

您可以自動將資料從 NetApp Ransomware Resilience 傳送到您的安全性與事件管理系統（SIEM），以進行威脅分析與偵測。

Ransomware Resilience 支援下列 SIEM ：

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

在 Ransomware Resilience 中啟用 SIEM 之前，您需要設定您的 SIEM 系統。

傳送至 **SIEM** 的事件資料

Ransomware Resilience 可以將以下事件資料傳送到您的 SIEM 系統：

- 情境:
  - **os**：這是一個具有ONTAP值的常數。
  - **os_version**：系統上執行的ONTAP版本。
  - **connector_id**：管理系統的控制台代理的 ID。
  - **cluster_id**： ONTAP為系統報告的叢集 ID。
  - **svm_name**：發現警報的 SVM 的名稱。
  - **volume_name**：發現警報的磁碟區的名稱。
  - **volume_id**： ONTAP為系統報告的磁碟區的 ID。
- 事件：
  - **incident_id**：勒索軟體復原力針對勒索軟體復原力中受到攻擊的捲所產生的事件 ID。
  - **alert_id**：勒索軟體復原能力為工作負載產生的 ID。

- 嚴重性：以下警報等級之一：「嚴重」、「高」、「中」、「低」。
- 描述：有關檢測到的警報的詳細信息，例如“在工作負載 arp_learning_mode_test_2630 上檢測到潛在的勒索軟體攻擊”

設定 **AWS Security Hub** 進行威脅偵測

在 Ransomware Resilience 中啟用 AWS Security Hub 之前，您需要在 AWS Security Hub 中執行以下幾個主要步驟：

- 在 AWS Security Hub 中設定權限。
- 在 AWS Security Hub 中設定身份驗證存取金鑰和金鑰。 （此處未提供這些步驟。）

在 **AWS Security Hub** 中設定權限的步驟

1. 前往 **AWS IAM** 控制台。
2. 選擇*政策*。
3. 使用以下 JSON 格式的程式碼建立策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

設定 **Microsoft Sentinel** 進行威脅偵測

在 Ransomware Resilience 中啟用 Microsoft Sentinel 之前、您需要在 Microsoft Sentinel 中執行下列高階步驟：

- 先決條件
  - 啟用 Microsoft Sentinel。
  - 在 Microsoft Sentinel 中建立自訂角色。

- 登記
  - 註冊 Ransomware Resilience 以接收來自 Microsoft Sentinel 的事件。
  - 為註冊創建一個秘密。
- 權限：為應用程式指派權限。
- 身份驗證：輸入應用程式的身份驗證憑證。

啟用 **Microsoft Sentinel** 的步驟

1. 前往 Microsoft Sentinel。
2. 建立*Log Analytics 工作區*。
3. 啟用 Microsoft Sentinel 以使用您剛剛建立的 Log Analytics 工作區。

在 **Microsoft Sentinel** 中建立自訂角色的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*訂閱* > 存取控制 **(IAM)**。
3. 輸入自訂角色名稱。使用名稱 **Ransomware Resilience Sentinel Configurator**。
4. 複製以下 JSON 並將其貼上到 **JSON** 標籤中。

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. 檢查並儲存您的設定。

註冊勒索軟體復原能力以接收來自 **Microsoft Sentinel** 的事件的步驟

1. 前往 Microsoft Sentinel。
2. 選擇 **Entra ID** > 應用程式 > 應用程式註冊。
3. 對於應用程式的*顯示名稱*，輸入「**Ransomware Resilience**」。
4. 在 支援的帳戶類型 欄位中，選擇 僅限此組織目錄中的帳戶。
5. 選擇將推送事件的*預設索引*。
6. 選擇*審核*。
7. 選擇*註冊*來儲存您的設定。

   註冊後，Microsoft Entra 管理中心將顯示應用程式概述窗格。

建立註冊密鑰的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*憑證和機密* > 客戶端機密 > 新客戶端機密。
3. 為您的應用程式機密新增描述。
4. 為秘密選擇一個*到期日*或指定自訂有效期限。

客戶端金鑰的有效期限限制為兩年（24 個月）或更短。 Microsoft 建議您設定小於 12 個月的到期值。

5. 選擇“新增”來建立您的秘密。
6. 記錄身份驗證步驟中使用的秘密。離開此頁面後，該秘密將不再顯示。

為應用程式指派權限的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*訂閱* > 存取控制 **(IAM)**。
3. 選擇*新增* > 新增角色分配。
4. 對於*特權管理員角色*字段，選擇*勒索軟體彈性哨兵配置器*。

這是您之前創建的自訂角色。

5. 選擇“下一步”。
6. 在*指派存取權限*欄位中，選擇*使用者、群組或服務主體*。
7. 選擇“選擇成員”。然後，選擇*Ransomware Resilience Sentinel Configurator*。
8. 選擇“下一步”。
9. 在*使用者可以做什麼*欄位中，選擇*允許使用者指派除特權管理員角色擁有者、UAA、RBAC（建議）之外的所有角色*。
10. 選擇“下一步”。
11. 選擇*審核並分配*來分配權限。

輸入應用程式驗證憑證的步驟

1. 前往 Microsoft Sentinel。
2. 輸入憑證：
   a. 輸入租用戶 ID、客戶端應用程式 ID 和客戶端應用程式金鑰。
   b. 按一下“驗證”。

認證成功後，會出現「已認證」的資訊。

3. 輸入應用程式的 Log Analytics 工作區詳細資訊。
   a. 選擇訂閱 ID、資源群組和 Log Analytics 工作區。

設定 **Splunk Cloud** 進行威脅偵測

在 Ransomware Resilience 中啟用 Splunk Cloud 之前，您需要在 Splunk Cloud 中執行下列進階步驟：

- 在 Splunk Cloud 中啟用 HTTP 事件收集器以透過 HTTP 或 HTTPS 從控制台接收事件資料。
- 在 Splunk Cloud 中建立事件收集器令牌。

在 **Splunk** 中啟用 **HTTP** 事件收集器的步驟

1. 轉到 Splunk Cloud。
2. 選擇*設定* > 資料輸入。
3. 選擇 **HTTP** 事件收集器 > 全域設定。
4. 在所有令牌切換上，選擇*已啟用*。
5. 若要讓事件收集器透過 HTTPS 而不是 HTTP 進行監聽和通信，請選擇「啟用 SSL」。
6. 在「HTTP 連接埠號碼」中輸入 HTTP 事件收集器的連接埠。

在 **Splunk** 中建立事件收集器令牌的步驟

1. 轉到 Splunk Cloud。
2. 選擇*設定* > 新增資料。
3. 選擇*監控* > **HTTP** 事件收集器。
4. 輸入令牌的名稱並選擇*下一步*。
5. 選擇將推播事件的*預設索引*，然後選擇*審核*。
6. 確認端點的所有設定正確，然後選擇*提交*。
7. 複製令牌並將其貼上到另一個文件中，以準備進行身份驗證步驟。

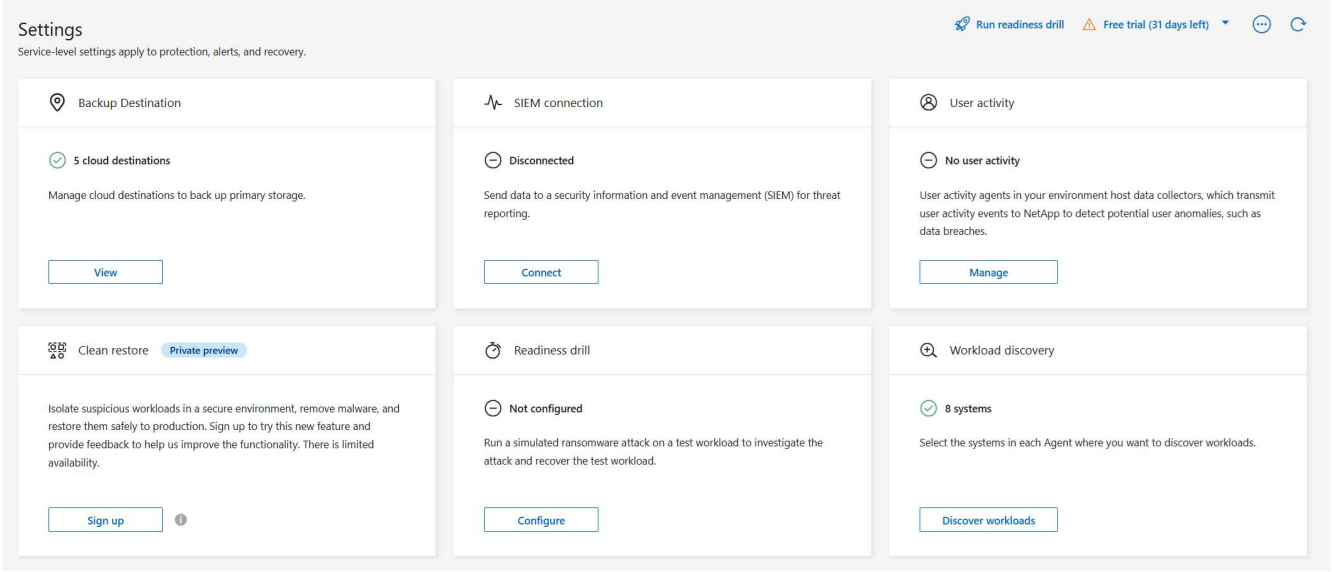
在勒索軟體防禦中連接 **SIEM**

啟用 SIEM 會將勒索軟體復原資料傳送到您的 SIEM 伺服器以進行威脅分析和報告。

步驟

1. 從控制台選單中，選擇*保護*>*勒索軟體恢復*。
2. 從勒索軟體恢復選單中，選擇垂直  …右上角的選項。
3. 選擇“設定”。

   出現「設定」頁面。



4. 在「設定」頁面中，選擇 SIEM 連線圖塊中的「連線」。

5. 選擇其中一個 SIEM 系統。
6. 輸入您在 AWS Security Hub 或 Splunk Cloud 中配置的令牌和驗證詳細資訊。

   您輸入的資訊取決於您選擇的 SIEM。

7. 選擇*啟用*。

   設定頁面顯示「已連線」。

設定使用者活動偵測

瞭解 **NetApp Ransomware Resilience** 中的使用者活動偵測

NetApp Ransomware Resilience 支援偵測可疑的使用者行為，讓您能夠在使用者層級處

理勒索軟體事件。

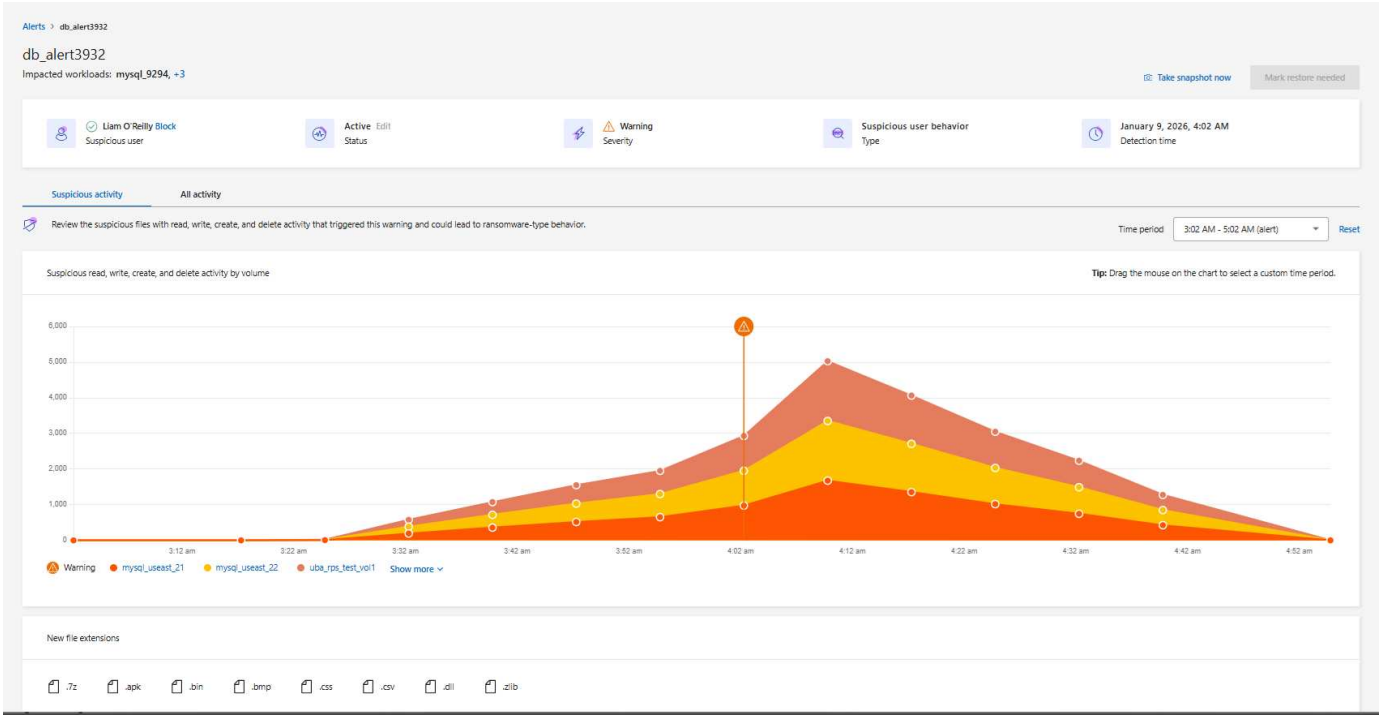
NetApp Ransomware Resilience 透過監控可疑的使用者活動，提供 AI 驅動的資料外洩偵測。讀取活動的急劇增加以及讀取活動的存取模式被用來判斷惡意意圖。一旦偵測到，Ransomware Resilience 會自動在 NetApp Console、電子郵件以及任何已設定的安全生態系統（例如 SIEM）中產生警示。

透過可疑使用者行為偵測和警示，NetApp Ransomware Resilience 會在發現可疑的資料外洩和破壞企圖及模式時發出警示。在每次警示中，NetApp Ransomware Resilience 都會識別出您可以封鎖的使用者。

勒索軟體彈性透過分析ONTAP中 FPolicy 產生的使用者活動事件來偵測可疑的使用者活動。要收集用戶活動數據，您需要部署一個或多個用戶活動代理程式。該代理程式是可連接到租用戶上的裝置的 Linux 伺服器或 VM。

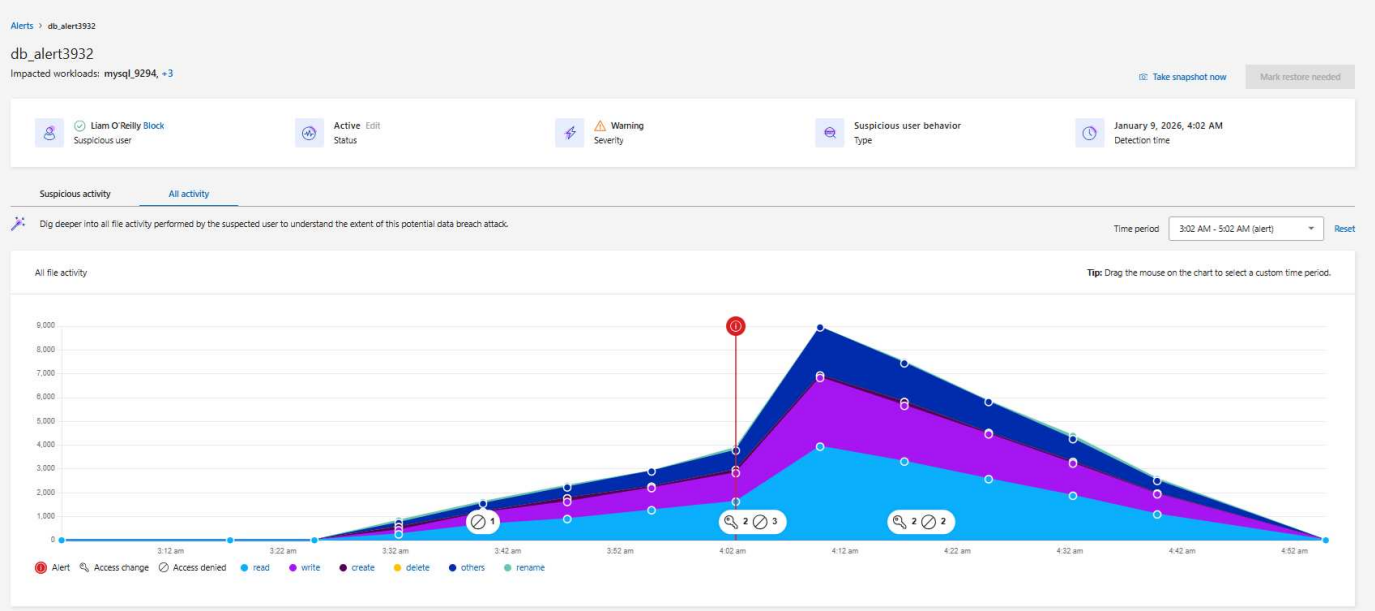
可疑使用者活動取證

Ransomware Resilience 提供使用者行為取證：透過清單和圖表顯示可疑活動發生的時間以及通知發送的時間。這些圖表詳細記錄了一段時間內檔案、目錄、磁碟區和工作負載上可疑活動的頻率，幫助您繪製事件圖。您也可以觀察新檔案副檔名的出現。



o

您可以將可疑活動與所有活動視圖進行比較。在所有活動視圖中，除了存取權限變更和存取被拒絕事件外，您還可以查看讀取、寫入、重新命名、移動、建立和刪除事件。



元件

Ransomware Resilience 可疑使用者行為活動偵測包含三個關鍵組成部分。

- 使用者活動代理程式是資料收集器的可執行環境。您必須設定使用者活動代理程式。
- 資料收集器會將使用者活動事件與 Ransomware Resilience 共用。當您啟用勒索軟體防護策略，並偵測可疑的使用者活動時，資料收集器會自動建立。
- 使用者目錄連接器能夠建立使用者名稱和使用者 ID 之間的映射關係，從而在應對可疑使用者行為時提供更清晰的線索。您必須配置使用者目錄連接器。

Ransomware Resilience 與 Data Infrastructure Insights

Ransomware Resilience 的可疑使用者行為偵測功能與 Data Infrastructure Insights（DII）Workload Security 整合，並使用"Data Infrastructure Insights 端點"。您無需任何 DII 組態即可在 Ransomware Resilience 中啟用使用者行為偵測。若要啟用使用者行為偵測，"建立所需的代理程式和收集器，並啟用適當的勒索軟體防護策略"。

如果您已在使用 NetApp Data Infrastructure Insights（DII）Workload Security、建議您將相同的 Workload Security 代理程式用於 Ransomware Resilience。您無需為 Ransomware Resilience 單獨部署 Workload Security 代理程式、但使用相同的 Workload Security 代理程式需要 Ransomware Resilience Console 組織與 DII Storage Workload Security 租戶建立配對關係。請聯絡您的客戶代表以啟用此配對。

後續步驟

- "使用者行為活動偵測的要求"
- "設定使用者行為活動代理程式和偵測器"

NetApp Ransomware Resilience 中的使用者行為偵測需求

在建立使用者活動代理程式和其他收集器之前、您必須確保符合所述的作業系統、伺服器和網路需求。

雲端供應商支援

雲端服務提供者支持

可疑用戶活動資料可以儲存在 AWS 和 Azure 的以下區域：

雲端提供者	地區
AWS	• 亞太地區（雪梨）（ap-southeast-2） • 歐洲（法蘭克福）(eu-central-1) • 美國東部（維吉尼亞北部）（us-east-1）
Azure	美國東部

作業系統要求

以下作業系統支援可疑使用者行為偵測：

作業系統	支援的版本
AlmaLinux	9.4（64 位元）至 9.5（64 位元）和 10（64 位元），包括 SELinux
CentOS	CentOS Stream 9（64 位元）
Debian	11（64 位元）、12（64 位元），包括 SELinux
OpenSUSE 飛躍	15.3（64 位）至 15.6（64 位）
Oracle Linux	8.10（64 位元）、9.1（64 位元）至 9.6（64 位元），包括 SELinux
紅帽	8.10（64 位元）、9.1（64 位元）至 9.6（64 位元）和 10（64 位元），包括 SELinux
洛基	Rocky 9.4 (64 位) 至 9.6 (64 位)，包括 SELinux
SUSE 企業 Linux	15 SP4（64 位元）至 15 SP6（64 位元），包括 SELinux
Ubuntu	20.04 LTS（64 位元）、22.04 LTS（64 位元）和 24.04 LTS（64 位元）

用于用户活动代理的计算机不应运行其他应用程序级别的软件。建議使用專用伺服器。

這 `unzip` 安裝需要該指令。這 `sudo su -` 該命令用於安裝、運行腳本和卸載。

伺服器要求

伺服器必須滿足以下最低要求：

- CPU：4 核
- 內存：16GB 內存

- 磁碟空間：36 GB 可用磁碟空間

伺服器建議

- 分配額外的磁碟空間以用於建立檔案系統。請確保檔案系統中至少有 35 GB 的可用空間。+ 如果 `/opt` 這是從 NAS 儲存裝置掛載的資料夾，本機使用者必須有權限存取此資料夾。如果本機使用者沒有必要的權限，則使用者活動代理程式建立可能會失敗。
- 建議您將使用者活動代理安裝在與 Ransomware Resilience 環境不同的系統上。如果確實要安裝在同一台機器上，則應預留 50 至 55 GB 的磁碟空間。對於 Linux 系統，請分配 25-30 GB 的空間至 `/opt/netapp`，並分配 25 GB 至 `var/log/netapp`。
- 建議您使用網路時間協定 (NTP) 或簡單網路時間協定 (SNTP) 同步ONTAP系統和使用者活動代理程式電腦上的時間。

雲端網路存取規則

查看您所在地區（亞太地區、歐洲或美國）的雲端網路存取規則。

在初始安裝期間，請將 `<site_name>` 替換為萬用字元 (* 權限。代理程式啟動並完全運作後，您可以將權限替換為網站名稱。請聯絡您的 NetApp 代表以取得網站名稱。

使用者活動代理程式使用 NetApp Data Infrastructure Insights 技術，因此需要使用 `cloudinsights`端點。如需詳細資訊，請參閱

基於亞太地區的使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS（TCP）	443	使用者活動代理	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	取得勒索軟體復原能力

歐洲使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS（TCP）	443	使用者活動代理	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	取得勒索軟體復原能力

美國使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS（TCP）	443	使用者活動代理	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	取得勒索軟體復原能力

網路內規則

協定	港口	來源	目的地	描述
TCP	389（LDAP） 636（LDAP/啟動-tls）	使用者活動代理	LDAP 伺服器 URL	連線到 LDAP
HTTPS（TCP）	443	使用者活動代理	叢集或SVM管理IP位址（取決於SVM收集器配置）	API 與ONTAP進行通信

協定	港口	來源	目的地	描述
TCP	35000 - 55000	SVM 資料 LIF IP 位址	使用者活動代理	ONTAP與使用者活動代理程式之間關於 Fpolicy 事件的通訊。為了讓ONTAP能夠向用戶活動代理發送事件，必須向其開放這些端口，包括用戶活動代理本身上的任何防火牆（如果存在）。+ 注意：您不需要預留*所有*這些端口，但您為此預留的端口必須在此範圍內。建議您先預留 100 個端口，如有必要再增加。
TCP	35000-55000	叢集管理IP	使用者活動代理	ONTAP叢集管理 IP 與使用者活動代理程式之間關於 **EMS** 事件 的通訊。為了讓ONTAP向用戶活動代理發送 EMS 事件，必須向用戶活動代理開放這些端口，包括用戶活動代理本身上的任何防火牆。+ 注意：您不需要預留*所有*這些端口，但您為此預留的端口必須在此範圍內。建議您先預留 100 個端口，如有必要再增加。
SSH	22	使用者活動代理	叢集管理	需要 CIFS/SMB 使用者阻止。

下一步

- "設定使用者活動代理程式和收集器"

在 **NetApp Ransomware Resilience** 中設定代理程式與收集器以偵測使用者活動

若要在 NetApp Ransomware Resilience 中啟用可疑使用者行為偵測功能，您必須至少安裝一個使用者活動代理程式。當您從 Ransomware Resilience 控制面板啟動可疑使用者活動功能時，需要提供使用者活動代理程式的主機資訊。

一個代理可以託管多個資料收集器。資料收集器將資料傳送到 SaaS 位置進行分析。有兩種類型的收集器：

- 資料收集器從ONTAP收集使用者活動資料。

- 使用者目錄連接器連接到您的目錄以將使用者 ID 對應到使用者名稱。

收集器在勒索軟體恢復設定中配置。

> 如果您已在使用 NetApp Data Infrastructure Insights（DII）Workload Security、建議您將相同的 Workload Security 代理程式用於 Ransomware Resilience。您無需為 Ransomware Resilience 單獨部署 Workload Security 代理程式、但使用相同的 Workload Security 代理程式需要 Ransomware Resilience Console 組織與 DII Storage Workload Security 租戶建立配對關係。請聯絡您的客戶代表以啟用此配對。

+ 如果您尚未使用 Data Infrastructure Insights，請按照此處的設定說明進行操作。

開始之前

- 確保您符合"作業系統、伺服器和網路要求"。

需要 **Console** 角色 若要啟用可疑使用者活動偵測，您需要 **Organization admin role**。針對後續的可疑使用者活動設定，您需要 **Ransomware Resilience user behavior admin role**。"了解NetApp Console的勒索軟體復原角色"。

確保每個角色都在組織層級套用。

建立使用者活動代理程式

使用者活動代理程式是 "資料收集器" 的可執行環境；資料收集器與 Ransomware Resilience 共用使用者活動事件。您必須建立至少一個使用者活動代理程式才能啟用可疑使用者活動偵測功能。

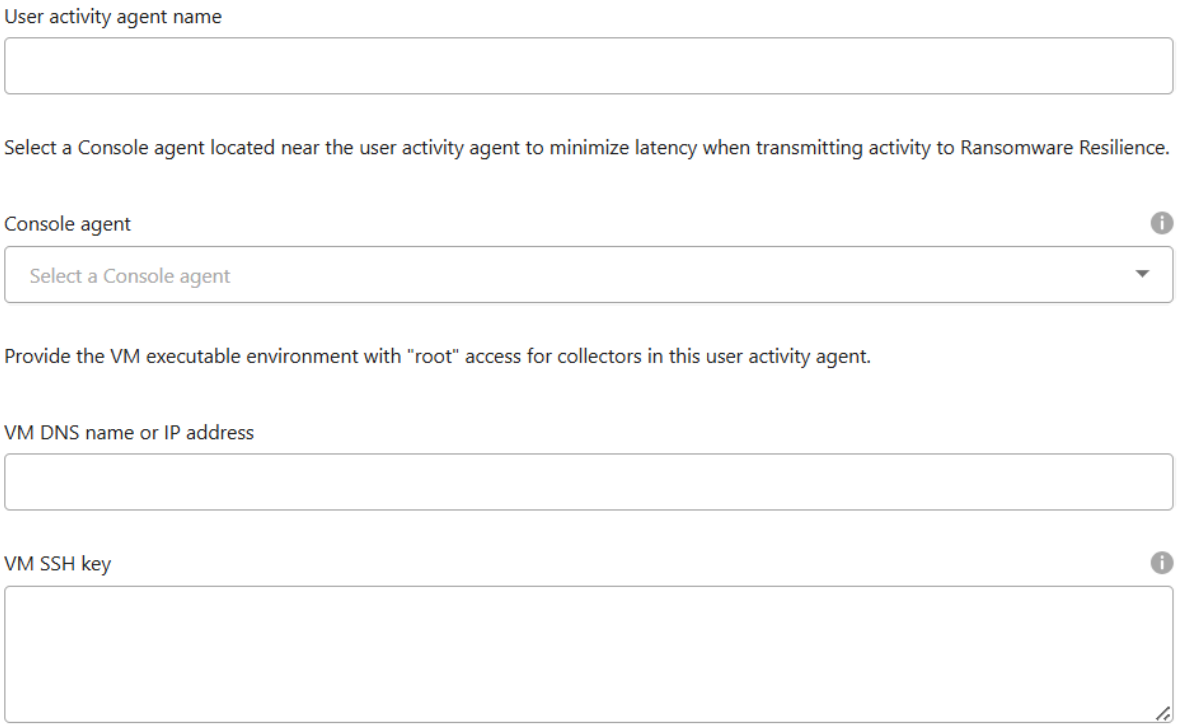
步驟

1. 如果這是您第一次建立使用者活動代理，請前往儀表板。在使用者活動圖塊中，選擇啟動。

   如果您要新增其他使用者活動代理，請前往*設定*，找到使用者活動圖塊，然後選擇管理。在使用者活動畫面上，選擇使用者活動代理選項卡，然後選擇新增。

2. 選擇雲端提供者，然後選擇區域。選擇下一步。
3. 提供用戶活動代理詳細資訊：
   - 使用者活動代理名稱
   - 控制台代理 - 控制台代理程式應與使用者活動代理程式位於同一網路中，並可透過 SSH 連線至使用者活動代理程式的 IP 位址。
   - **VM DNS** 名稱或 **IP** 位址
   - **VM SSH Key** - 請使用以下格式輸入 SSH 金鑰：

     ```
     -----BEGIN OPENSSH PRIVATE KEY-----
     private-key-contents
     -----END OPENSSH PRIVATE KEY-----
     ```



4. 選擇下一步。
5. 檢查您的設定。選擇*啟動*以完成新增使用者活動代理程式。
6. 確認使用者活動代理程式已成功建立。在「使用者活動」磁貼中，成功部署後會顯示為 **Running**。

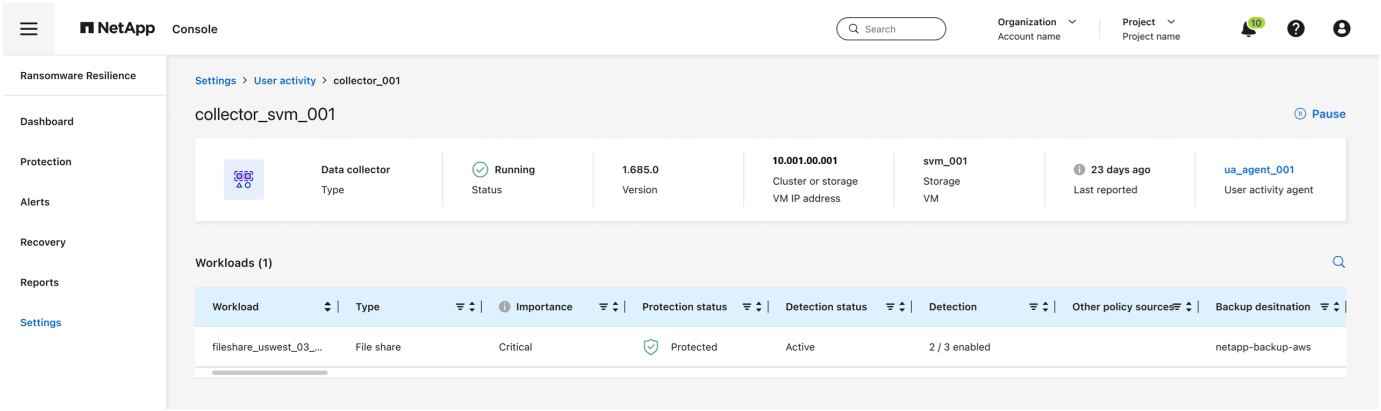
結果

使用者活動代理程式成功建立後、返回 **Settings** 功能表、然後在 User activity 磚中選取 **Manage** 。選取 **User activity agents** 索引標籤、然後選取使用者活動代理程式以檢視其詳細資料、包括資料收集器和使用者目錄連接器。

新增資料收集器

當您啟用具有可疑使用者活動偵測功能的勒索軟體保護策略時，資料收集器會自動建立。有關詳細信息，請參閱新增檢測策略。

您可以查看資料收集器的詳細資訊。從「設定」中，選擇「使用者活動」圖塊中的「管理」。選擇資料收集器選項卡，然後選擇資料收集器以查看其詳細資訊或暫停它。



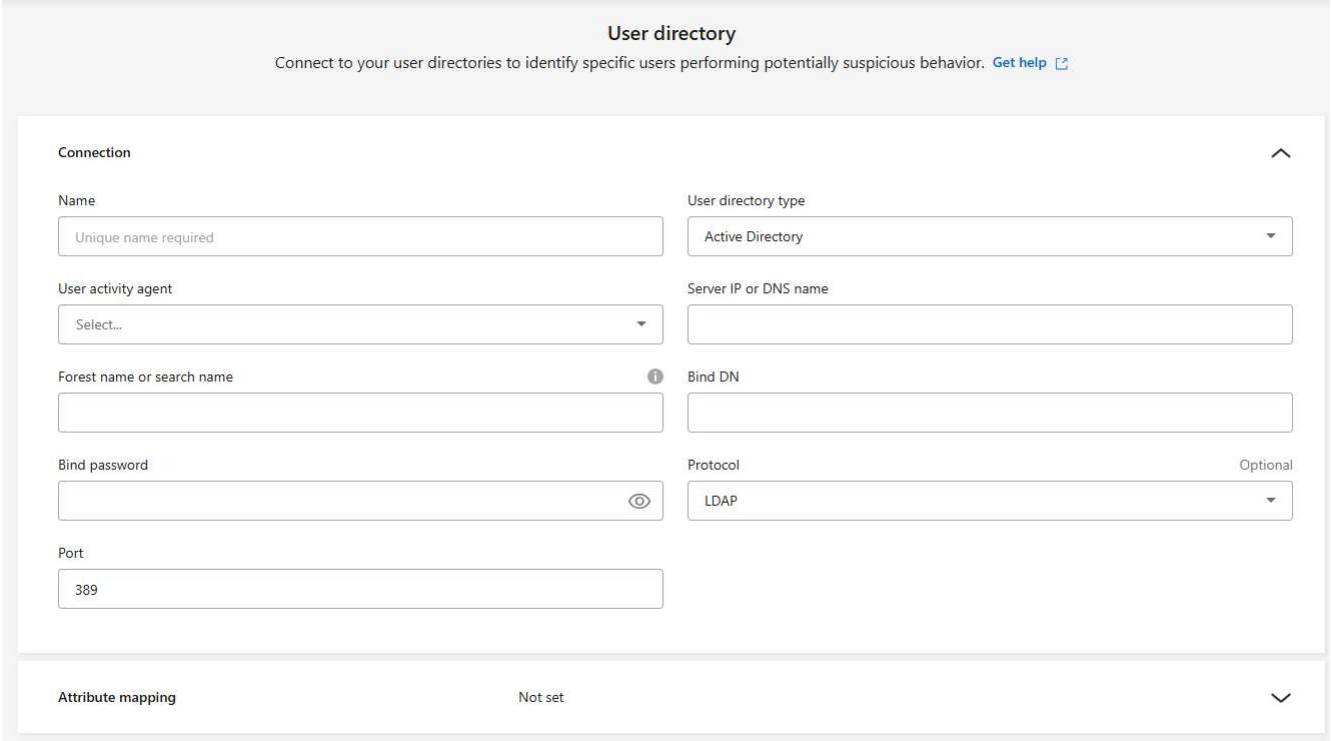
建立使用者目錄連接器

若要將使用者 ID 對應到使用者名，您必須建立使用者目錄連接器。

步驟

1. 在勒索軟體復原中，前往*設定*。
2. 在使用者活動圖塊中，選擇管理。
3. 選擇使用者目錄連接器選項卡，然後選擇新增。
4. 配置連接。請在每個欄位中填寫所需資訊。

場地	描述
姓名	請為使用者目錄連接器輸入一個唯一的名稱
使用者目錄類型	目錄類型
伺服器**IP**位址或網域名稱	連接所在伺服器的 IP 位址或完全限定網域名稱 (FQDN)
森林名稱或搜尋名稱	您可以將目錄結構的林級別指定為直接網域名稱（例如）。`unit.company.com`）或一組相對專有名詞（例如：`DC=unit,DC=company,DC=com`）。你也可以輸入一個 `OU` 按組織單元或 `CN` 僅限特定使用者（例如：`CN=user,OU=engineering,DC=unit,DC=company,DC=com`）。
綁定**DN**	BIND DN 是被允許搜尋目錄的使用者帳戶，例如 user@domain.com。使用者需要網域唯讀權限。
綁定密碼	BIND DN 中提供的使用者密碼
協定	協定字段為可選字段。您可以使用 LDAP、LDAPS 或基於 StartTLS 的 LDAP。
港口	請輸入您選擇的連接埠號



提供屬性映射詳細資訊：

- 顯示名稱
- **SID**（如果您使用 LDAP）
- 使用者名稱
- **Unix ID**（如果您使用 NFS）
- 如果您選擇"包含可選屬性"，您還可以新增電子郵件地址、電話號碼、角色、州/省、國家/地區、部門、照片、經理 DN 或群組。選擇"進階"以新增可選的搜尋查詢。

5. 選擇新增。
6. 傳回使用者目錄連接器標籤以檢查使用者目錄連接器的狀態。如果建立成功，使用者目錄連接器的狀態顯示為*正在執行*。

刪除使用者目錄連接器

步驟

1. 在勒索軟體復原中，前往*設定*。
2. 找到使用者活動圖塊，選擇管理。
3. 選擇使用者目錄連接器選項卡。
4. 確定要刪除的使用者目錄連接器。在行尾的操作選單中，選擇三個點 `...`然後刪除。
5. 在彈出的對話方塊中、選取 **Delete** 進行確認。

將使用者排除在警示範圍之外

如果某些受信任使用者的行為可能會觸發使用者行為警示，您可以將他們從警示中排除。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表板中，找到「使用者活動」卡片，然後選取 **Manage**。
3. 選擇 **Excluded users** 標籤。
4. 若要在使用者介面中檢閱個別使用者，請選擇 手動選取。若要上傳排除的使用者清單，請選取 上傳。
   a. 如果您選擇了 **Select manually**，請選取要排除的特定使用者名稱旁的核取方塊。
   b. 如果您選擇 **Upload**，則必須先下載包含所有使用者清單的 CSV 檔案。選擇 **Download** 即可存取該清單。

      檢閱 CSV 檔案。移除所有您想要維持偵測的使用者名稱。當清單僅包含您想要從偵測中排除的使用者名稱時，請儲存該清單。選取 **Upload** 以找到檔案，然後選擇該檔案。
5. 選擇 **Add** 以完成將使用者新增至排除清單的操作。
6. 在「已排除使用者」標籤中，現在會在儀表板中顯示已從使用者行為偵測警示中移除的使用者名稱。

您也可以直接將使用者從警示中排除。如需詳細資訊、請參閱 "回應勒索軟體警示"。

從排除使用者清單中移除使用者

之後您可以將使用者重新加入偵測。

步驟

1. 在「設定」儀表板中，找到「使用者活動」卡片，然後選取 **Manage**。
2. 選擇 **Excluded users** 標籤。
3. 從排除使用者清單中找到要移除的使用者名稱。在該使用者名稱所在的行選擇操作選單 (...) ，然後選擇移除。
4. 在對話方塊中、選取 **Remove** 以確認您要移除所選使用者。

回應可疑用戶活動警報

配置可疑使用者活動偵測後，您可以在警報頁面監控事件。如需詳細資訊，請參閱 "偵測惡意活動和可疑使用者行為"。