Use Ransomware Resilience

NetApp Ransomware Resilience

NetApp
February 11, 2026

Table of Contents

Use Ransomware Resilience

Monitor workload health using the NetApp Ransomware Resilience Dashboard

The NetApp Ransomware Resilience Dashboard provides at-a-glance information about the protection health of your workloads. You can quickly determine workloads that are at risk or protected, identify workloads impacted by an incident or in recovery, and gauge the extent of protection by looking at how much storage is protected or at risk.

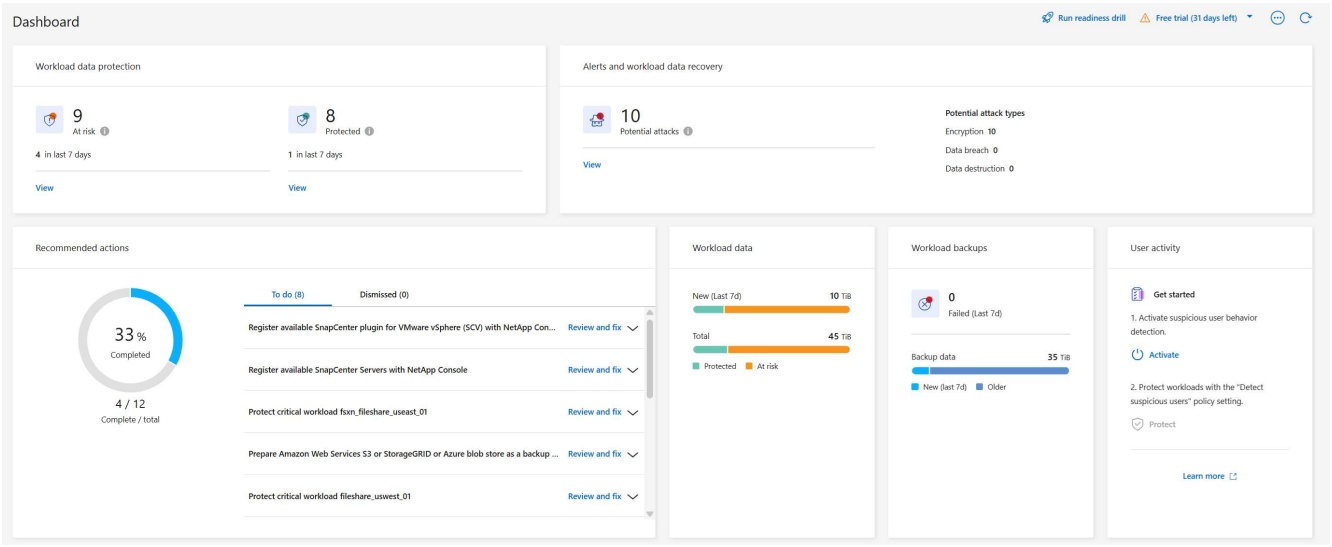
Use the Dashboard to review protection suggestions, change settings, and download reports.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

Review workload health using the Dashboard

Steps

1. After the Console discovers your workloads, the Ransomware Resilience dashboard displays workload data protection health.



2. From the Dashboard, you can do the following actions in each of the panes:
   - **Workload data protection**: Select **View all** to see all workloads that are at risk or protected on the Protection page. Workloads are at risk when protection levels don't match a protection policy. Refer to Protect workloads.

     Select the "i" icon to see tips on this data. To increase the workload limit, select **Increase workload limit** inside this i note. Selecting this takes you to the Console Support page where you can create a case ticket.

   - **Alerts and workload data recovery**: Select **View all** to see active incidents that have impacted your workload, are ready for recovery after incidents are neutralized, or are in recovery. Refer to Respond to

a detected alert.

- An incident is categorized in one of the following states:
  - New
  - Dismissed
  - Dismissing
  - Resolved
- An alert can have one of the following statuses:
  - New
  - Inactive
- A workload can have one of the following restore statuses:
  - Restore needed
  - In progress
  - Restored
  - Failed

◦ **Recommended actions**: To increase protection, review each recommendation then select **Review and fix**.

See Review protection suggestions on the Dashboard or Protect workloads.

Ransomware Resilience displays new recommendations since your last visit to the Dashboard with the "New" tag for 24 hours. Actions appear in priority order, with the most important at the top. Review, act on, or dismiss each recommendation.

The total number of actions does not include actions you dismissed.

◦ **Workload data**: Monitor changes in protection coverage over the last 7 days.

◦ **Workload backups**: Monitor changes in workload backups created by Ransomware Resilience that failed or completed successfully in the last 7 days.

Review protection recommendations on the Dashboard

Ransomware Resilience assesses the protection on your workloads and recommends actions to improve that protection.

You can review a recommendation and act on it, which changes the recommendation status to Complete. Or, if you want to act on it later, you can dismiss it. Dismissing an action moves the recommendation to a list of dismissed actions, which you can review later.

Here is a sampling of the recommendations that Ransomware Resilience offers.

Recommendation	Description	How to resolve
Add a ransomware protection policy.	The workload is currently not protected.	Assign a policy to the workload. Refer to Protect workloads against ransomware attacks.

Recommendation	Description	How to resolve
Connect to SIEM for threat reporting.	Send data to a security and event management system (SIEM) for threat analysis and detection.	Enter SIEM/XDR server details to enable threat detection. Refer to Configure protection settings.
Enable workload-consistent protection for applications or VMware.	These workloads are not managed by SnapCenter Software or SnapCenter Plug-in for VMware vSphere.	To have them managed by SnapCenter, enable workload-consistent protection. Refer to Protect workload against ransomware attacks.
Improve security posture for system	NetApp Digital Advisor has identified at least one high or critical security risk.	Review all security risks in NetApp Digital Advisor. Refer to Digital Advisor documentation.
Make a policy stronger.	Some workloads might not have enough protection. Strengthen protection on workloads with a policy.	Increase retention, add backups, enforce immutable backups, block suspicious file extensions, enable detection on secondary storage and more. Refer to Protect workloads against ransomware attacks.
Prepare <backup provider> as a backup destination to back up your workload data.	The workload does not currently have any backup destinations.	Add backup destinations to this workload to protect it. Refer to Configure protection settings.
Protect critical or highly important application workloads against ransomware.	The Protect page displays critical or highly important (based on the Priority level assigned) application workloads that are not protected.	Assign a policy to these workloads. Refer to Protect workloads against ransomware attacks.
Protect critical or highly important file share workloads against ransomware.	The Protection page displays critical or highly important workloads of the type File Share or Datastore that are not protected.	Assign a policy to each of the workloads. Refer to Protect workloads against ransomware attacks.
Register available SnapCenter plugin for VMware vSphere (SCV) with the Console	A VM workload is not protected.	Assign VM-consistent protection to the VM workload by enabling the SnapCenter Plugin for VMware vSphere. Refer to Protect workloads against ransomware attacks.
Register available SnapCenter Server with the Console	An application is not protected.	Assign application-consistent protection to the workload by enabling SnapCenter Server. Refer to Protect workloads against ransomware attacks.
Review new alerts.	New alerts exist.	Review the new alerts. Refer to Respond to a detected ransomware alert.

Steps

1. From the Recommended actions pane in Ransomware Resilience, select a recommendation then **Review and fix**.
2. To dismiss the action until later, select **Dismiss**.

   The recommendation clears from the To Do list and appears on the Dismissed list.

   You can later change a dismissed item to a To Do item. When you mark an item as completed or you change a dismissed item to a To Do action, the Total actions count increases by 1.

3. To review information on how to act on the recommendations, select the **information** icon.

Export protection data to CSV files

You can export data and download CSV files that show details of protection, alerts, and recovery.

You can download CSV files from any of the main menu options:

- **Protection**: Contains the status and details of all workloads, including the total number of workloads that Ransomware Resilience marks as protected or at risk.
- **Alerts**: Includes the status and details of all alerts, including the total number of alerts and automated snapshots.
- **Recovery**: Includes the status and details of all workloads that need to be restored, including the total number of workloads that Ransomware Resilience marks as "Restore needed", "In progress," "Restore failed," and "Successfully restored."

Downloading a CSV file from a page includes only the data from that page.

The CSV files include data for all workloads on all Console systems.

Steps

1. From the Ransomware Resilience dashboard, select the **Refresh** option in the upper right to refresh the data that will appear in the files.
2. Do one of the following:
   - From the page, select the **Download** option.
   - From the Ransomware Resilience menu, select **Reports**.
3. If you selected the **Reports** option, select one of the preconfigured named files then select **Download (CSV)** or **Download (JSON)**.

Access technical documentation

You can access Ransomware Resilience technical documentation from docs.netapp.com or from inside Ransomware Resilience.

Steps

1. From the Ransomware Resilience dashboard, select the vertical **Actions** option.

2. Select one of these options:
    - **What's new** to view information about the features in the current or previous releases in the Release Notes.
    - **Documentation** to view the Ransomware Resilience documentation Home page and this documentation.

Protect workloads

Protect workloads with NetApp Ransomware Resilience protection strategies

You can protect workloads against ransomware attacks by enabling workload-consistent protection or creating ransomware protection strategies in NetApp Ransomware Resilience.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Understand ransomware protection strategies

Ransomware protection strategies encompass *detection*, *protection*, and *replication* policies.

- **Detection policies** identify ransomware threats
- **Protection policies** include snapshot and backup policies. Detection and snapshot policies are required in a protection strategy. Backup policies are optional.

  If you're using other NetApp products to protect your workload, Ransomware Resilience discovers those and provides the option to either:

    - use a ransomware detection policy and continue to use the snapshot and backup policies created by other NetApp tools, or
    - use Ransomware Resilience to manage detection, snapshots, and backups.
- **Replication policies** enable you to replicate snapshots from Ransomware Resilience to a secondary site. Replication schedules can be set to hourly, daily, weekly, or monthly frequencies.

  Currently, you can only replicate snapshots to on-premises ONTAP storage.

For enhanced management and protection of your data estate, you can create group file shares to collectively protect volumes under one strategy.

Protection policies with other NetApp-managed services

Beyond Ransomware Resilience, the following services can be used to manage protection:

- NetApp Backup and Recovery for file shares, VM file shares
- SnapCenter for VMware for VM datastores
- SnapCenter for Oracle

Protection information from these services appears in Ransomware Resilience. You can add detection policies

to these services with Ransomware Resilience. Adding a protection policy with Ransomware Resilience replaces the existing protection policies.

If a ransomware detection policy is being managed by Autonomous Ransomware Protection (ARP or ARP/AI, depending on the ONTAP version) and FPolicy in ONTAP, those workloads are protected and will continue to be managed by ARP and FPolicy.

> Backup destinations are not available for workloads in Amazon FSx for NetApp ONTAP. Perform backup operations using the FSx for ONTAP backup service. You set backup policies for workloads in FSx for ONTAP in AWS, not in Ransomware Resilience. The backup policies appear in Ransomware Resilience and remain unchanged from AWS.

Protection policies for workloads not protected by NetApp applications

If your workload isn't managed by Backup and Recovery, Ransomware Resilience, SnapCenter, or SnapCenter Plug-in for VMware vSphere, it may have snapshots taken as part of ONTAP or other products. If ONTAP FPolicy protection is in place, you can change the FPolicy protection using ONTAP.

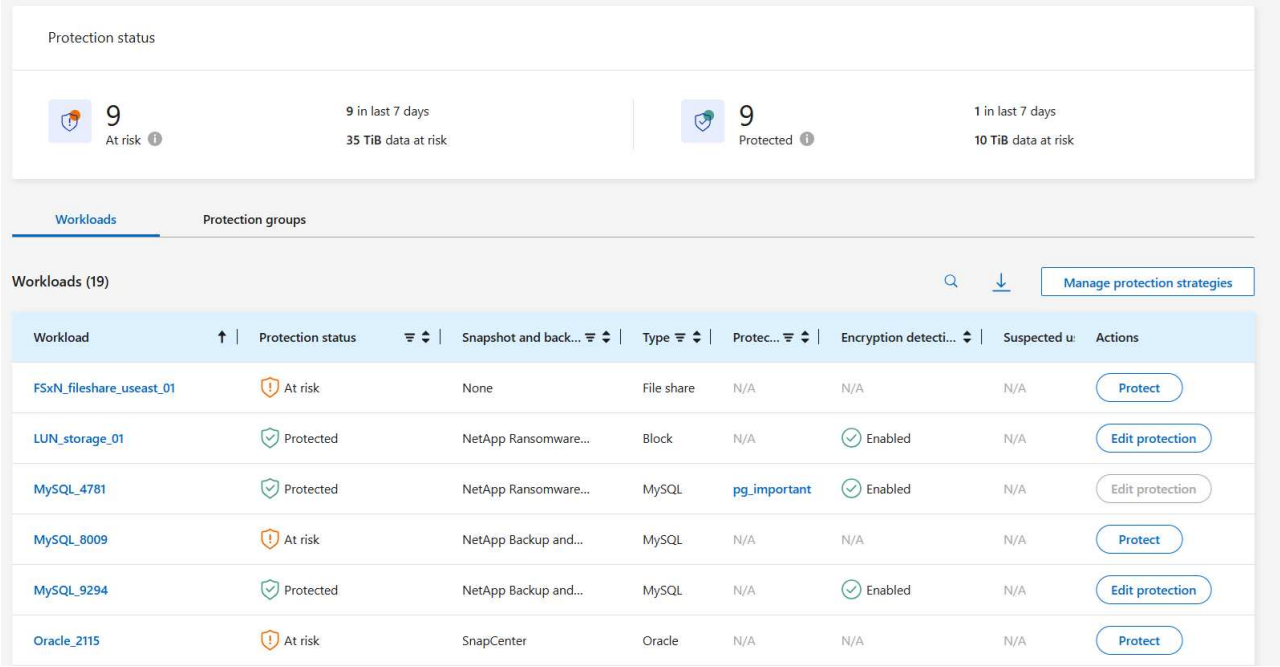
View ransomware protection on a workload

One of the first steps in protecting workloads is viewing your current workloads and their protection status. You can see the following types of workloads:

- Application workloads
- Block workloads
- File share workloads
- VM workloads

Steps

1. From the Console's left navigation, select **Protection** > **Ransomware Resilience**.
2. Do one of the following:
    - From the Data Protection pane on the Dashboard, select **View all**.
    - From the menu, select **Protection**.



3. From this page, you can view and change protection details for the workload.

See Add a ransomware protection strategy to learn about using Ransomware Resilience when there's an existing protection policy with SnapCenter or Backup and Recovery.

Understand the Protection page

The Protection page shows the following information about workload protection:

Protection status: A workload can show one of the following protection statuses to indicate whether a policy is applied or not:

- **Protected**: A policy is applied. ARP (or ARP/AI depending on the ONTAP version) is enabled on all volumes related to the workload.
- **At risk**: No policy is applied. If a workload does not have a primary detection policy enabled, it is "at risk" even if it has a snapshot and backup policy enabled.
- **In progress**: A policy is being applied but not completed yet.
- **Failed**: A policy is applied but is not working.

Detection status: A workload can have one of the following ransomware detection statuses:

- **Learning**: A ransomware detection policy was recently assigned to the workload and Ransomware Resilience is scanning workloads.
- **Active**: A ransomware detection protection policy is assigned.
- **Not set**: A ransomware detection protection policy is not assigned.
- **Error**: A ransomware detection policy was assigned, but Ransomware Resilience has encountered an error.

When protection is enabled in Ransomware Resilience, alert detection and reporting begins after the ransomware detection policy status changes from Learning mode to Active mode.

Suspicious user behavior activity and FPolicy (suspicious file extension) activity are listed separately from detection status.

Detection policy: The name of the ransomware detection policy appears, if one has been assigned. If the detection policy has not been assigned, "N/A" appears.

Replication destination: If you've configured snapshot replication, the names of the destination storage VMs and systems are listed. If there's no replication, this field displays "None."

Snapshot and backup policies: This column shows the snapshot and backup policies applied to the workload and the product or service that is managing those policies.

- Managed by SnapCenter
- Managed by SnapCenter Plug-in for VMware vSphere
- Managed by Backup and Recovery
- Name of ransomware protection policy that governs snapshots and backups
- None

Workload importance

Ransomware Resilience assigns an importance or priority to each workload during discovery based on an analysis of each workload. The workload importance is determined by the following snapshot frequencies:

- **Critical**: More than one snapshot copy is taken per hour (highly aggressive protection schedule)
- **Important**: Snapshots copies are created less frequently than every hour but more frequently than every day
- **Standard**: Snapshot copies are taken more than once per day

Predefined detection policies

You can choose one of the following Ransomware Resilience predefined policies, which are aligned with workload importance.

The **Encryption user extension** policy is the only predefined policy that supports suspicious user behavior detection.

+
The **Critical replication policy** is the only predefined policy that supports replicating snapshots to ONTAP.

Policy level	Snapshot	Frequency	Retention (days)	Number of snapshot copies	Maximum number of snapshot copies
Critical workload policy	Quarter hourly	Every 15 min	3	288	309
	Daily	Every 1 day	14	14	309
	Weekly	Every 1 week	35	5	309
	Monthly	Every 30 days	60	2	309
Important workload policy	Quarter hourly	Every 30 mins	3	144	165
	Daily	Every 1 day	14	14	165
	Weekly	Every 1 week	35	5	165
	Monthly	Every 30 days	60	2	165
Standard workload policy	Quarter hourly	Every 30 min	3	72	93
	Daily	Every 1 day	14	14	93
	Weekly	Every 1 week	35	5	93
	Monthly	Every 30 days	60	2	93
Encryption user extension	Quarter hourly	Every 30 min	3	72	93
	Daily	Every 1 day	14	14	93
	Weekly	Every 1 week	35	5	93
	Monthly	Every 30 days	60	2	93
Encryption user extension	Quarter hourly	Every 30 min	3	72	93
	Daily	Every 1 day	14	14	93
	Weekly	Every 1 week	35	5	93
	Monthly	Every 30 days	60	2	93

Policy level	Snapshot	Frequency	Retention (days)	Number of snapshot copies	Maximum number of snapshot copies
Critical replication policy	Quarter hourly	Every 15 min	3	288	309
	Daily	Every 1 day	14	14	309
	Weekly	Every 1 week	35	5	309
	Monthly	Every 30 days	60	2	309

Enable application- or VM-consistent protection with SnapCenter

Enabling application- or VM-consistent protection helps you protect your application or VM workloads in a consistent manner, achieving a quiescent and consistent state to avoid potential data loss later if recovery is needed.

This process initiates registering SnapCenter Software Server for applications or SnapCenter Plug-in for VMware vSphere for VMs using Backup and Recovery.

After you enable workload-consistent protection, you can manage protection strategies in Ransomware Resilience. The protection strategy includes the snapshot and backup policies managed elsewhere along with a ransomware detection policy managed in Ransomware Resilience.

To learn about registering SnapCenter or SnapCenter Plug-in for VMware vSphere using Backup and Recovery, refer to the following information:

- Register SnapCenter Server Software
- Register SnapCenter Plug-in for VMware vSphere

Steps

1. From the Ransomware Resilience menu, select **Dashboard**.
2. From the Recommendations pane, locate one of the following recommendations and select **Review and fix**:
   - Register available SnapCenter Server with the NetApp Console
   - Register available SnapCenter Plug-in for VMware vSphere (SCV) with the NetApp Console
3. Follow the information to register the SnapCenter or SnapCenter Plug-in for VMware vSphere host using Backup and Recovery.
4. Return to Ransomware Resilience.
5. From Ransomware Resilience, navigate to the Dashboard and initiate the discovery process again.
6. From Ransomware Resilience, select **Protection** to view the Protection page.
7. Review details in the snapshot and backup policies column on the Protection page to see that the policies are managed elsewhere.

Add a ransomware protection strategy

There are three approaches to adding a ransomware protection strategy:

- **Create a ransomware protection strategy if you have no snapshot or backup policies.**

  The ransomware protection strategy includes:

  - Snapshot policy
  - Ransomware detection policy
  - Backup policy

- **Replace the existing snapshot or backup policies from SnapCenter or Backup and Recovery protection with protection strategies managed by Ransomware Resilience.**

  The ransomware protection strategy includes:

  - Snapshot policy
  - Ransomware detection policy
  - Backup policy

- **Create a detection policy for workloads with existing snapshot and backup policies managed in other NetApp products or services.**

  The detection policy does not change the policies managed in other products.

  The detection policy enables Autonomous Ransomware Protection and FPolicy protection if they are already activated in other services. Learn more about Autonomous Ransomware Protection, Backup and Recovery, and ONTAP FPolicy.

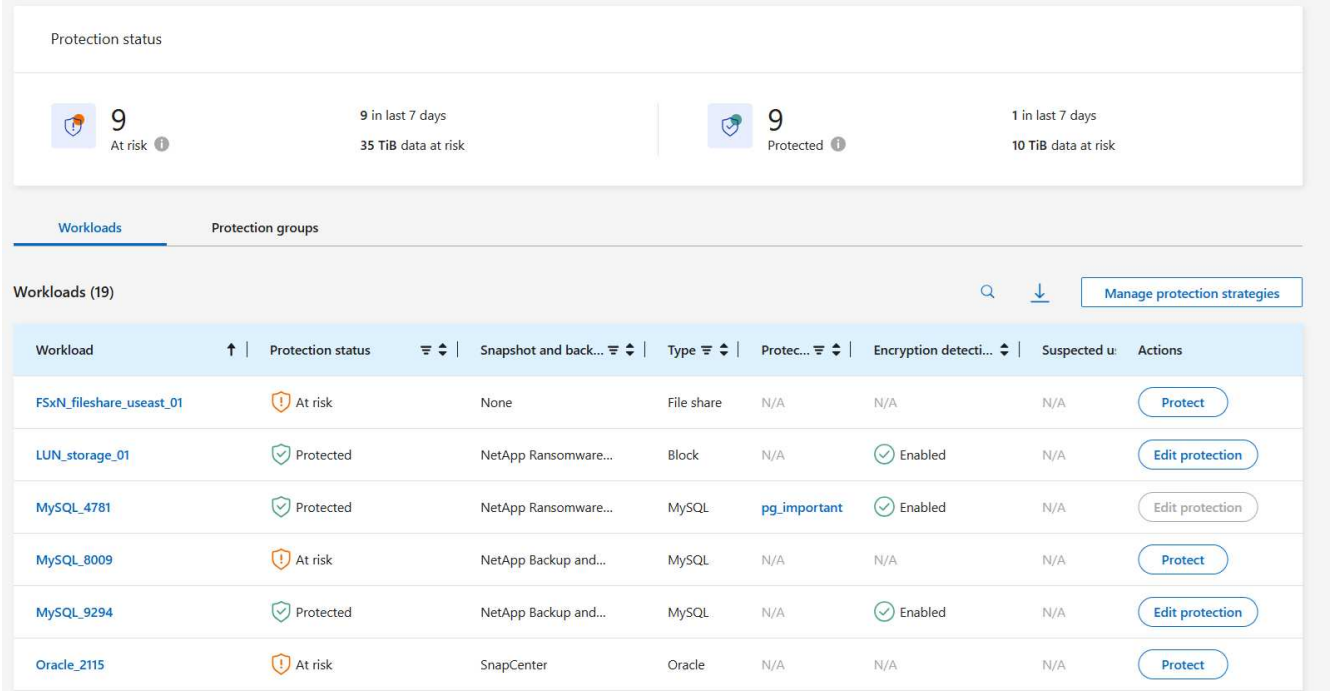
Create a ransomware protection strategy (if you have no snapshot or backup policies)

If snapshot or backup policies do not exist on the workload, you can create a ransomware protection strategy, which can include the following policies that you create in Ransomware Resilience:

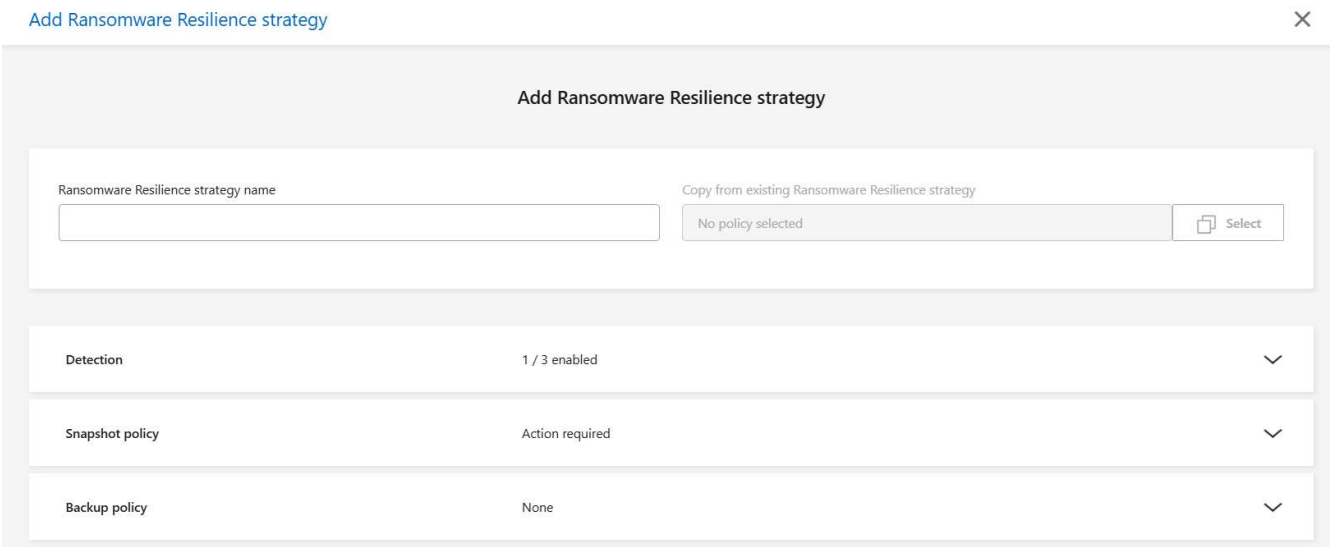
- Snapshot policy
- Backup policy
- Ransomware detection policy
- Secondary replication to ONTAP

Steps to create a ransomware protection strategy

1. From the Ransomware Resilience menu, select **Protection**.



2. From the Protection page, select a workload then **Protect**.
3. From the Ransomware protection strategies page, select **Add**.



4. Enter a new strategy name, or enter an existing name to copy it. If you enter an existing name, choose which one to copy and select **Copy**.

> If you choose to copy and modify an existing strategy, Ransomware Resilience appends "_copy" to the original name. You should change the name and at least one setting to make it unique.

5. For each item, select the **Down arrow**.
   - **Detection policy**:
     - **Policy**: Choose one of the predesigned detection policies.
     - **Primary detection**: Enable Ransomware Resilience to detect potential ransomware attacks.

- **Suspicious user behavior detection**: Enable user behavior detection to transmit user activity events to Ransomware Resilience and detect suspicious events, such as data breaches.
- **Block file extensions**: Enable Ransomware Resilience to block known suspicious file extensions. Ransomware Resilience takes automated snapshot copies when Primary detection is enabled.

  If you want to change the blocked file extensions, edit them in System Manager.

◦ **Snapshot policy**:

- **Snapshot policy base name**: Select a policy or select **Create** and enter a name for the snapshot policy.
- **Snapshot locking**: Enable this to lock the snapshot copies on primary storage so that they cannot be modified or deleted for a certain period of time even if a ransomware attack manages its way to the backup storage destination. This is also called *immutable storage*. This enables quicker restore time.

  When a snapshot is locked, the volume expiration time is set to the expiration time of the snapshot copy.

  Snapshot copy locking is available with ONTAP 9.12.1 and later. To learn more about SnapLock, refer to SnapLock in ONTAP.

- **Snapshot schedules**: Choose schedule options, the number of snapshot copies to keep, and select to enable the schedule.

◦ **Replication policy**:

- **Replication policy basename**: Enter a new name or choose an existing one. The basename is the prefix appended to all snapshots.
- **Replication schedules**: Toggle the frequencies you want to enable (hourly, daily, weekly, or monthly) and set the retention value (the number of replicated snapshots to keep) for each schedule you enable.

◦ **Backup policy**:

- **Backup policy basename**: Enter a new or choose an existing name.
- **Backup schedules**: Choose schedule options for secondary storage and enable the schedule.

  To enable backup locking on secondary storage, configure your backup destinations using the **Settings** option. For details, see Configure settings.

6. Select **Add**.

Add a detection policy to workloads with existing snapshot and backup policies managed by SnapCenter or Backup and Recovery

Ransomware Resilience enables you to assign either a detection policy or a protection policy to workloads with existing snapshot and backup protection managed in other NetApp products or services. Other services, such as Backup and Recovery and SnapCenter, use policies that govern snapshots, replication to secondary storage, or backups to object storage.

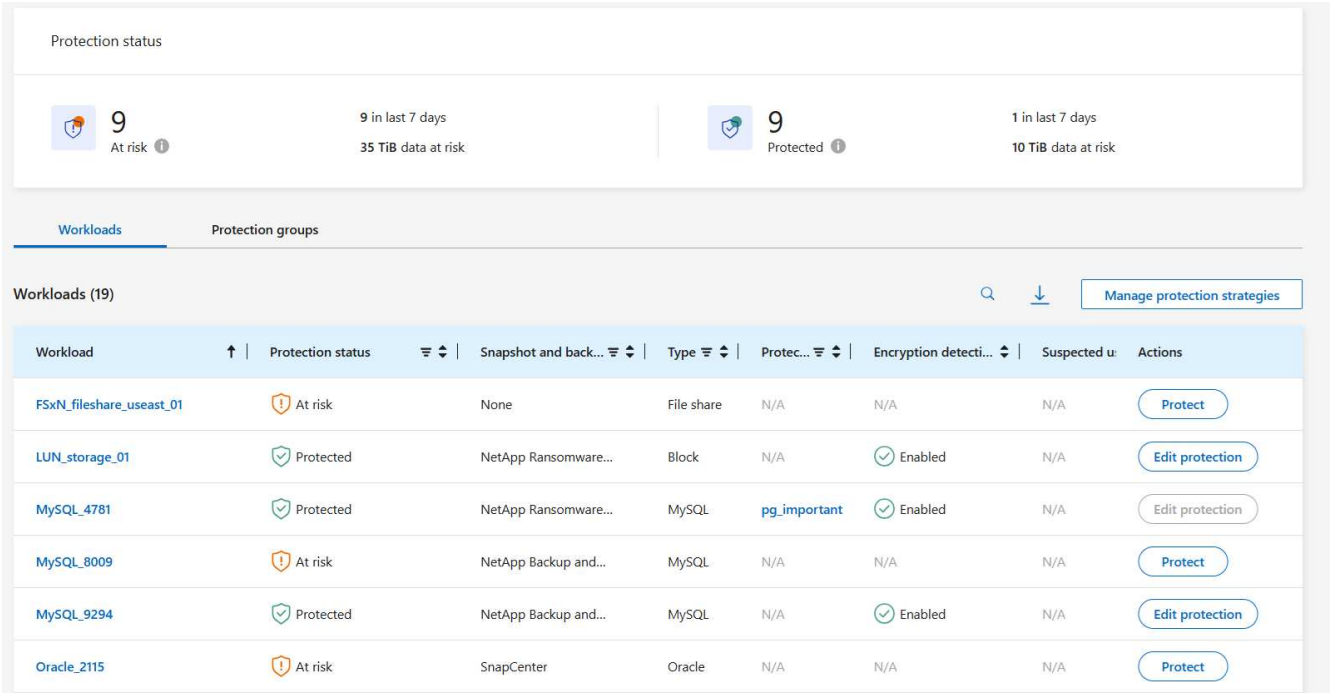
Add a detection policy to workloads with existing backup or snapshot policies

If you have existing snapshot or backup policies with Backup and Recovery or SnapCenter, you can add a policy to detect ransomware attacks. To manage protection and detection with Ransomware Resilience, see

Protect with Ransomware Resilience.

Steps

1. From the Ransomware Resilience menu, select **Protection**.



2. From the Protection page, select a workload then select **Protect**.
3. Ransomware Resilience detects if there are existing active SnapCenter or Backup and Recovery policies.
4. To leave your existing Backup and Recovery or SnapCenter policies in place and only apply a *detection* policy, leave the **Replace existing policies** box unchecked.
5. To see details of the SnapCenter policies, select the **Down arrow**.
6. Select the detection settings you want:
   Encryption detection
   Suspicious user behavior detection
   Block suspicious file extensions
7. Select **Next**.
8. If you selected **Suspicious user behavior detection** as a detection setting, select the User activity agent or or create one.

   The user activity agent hosts the new data collectors. Ransomware Resilience creates the data collector automatically to transmit user activity events to Ransomware Resilience to detect anomalous user behavior.

9. Select **Next**.
10. Review your choices. Select **Create** to activate detection.
11. On the Protection page, review the **Detection status** to confirm detection is Active.

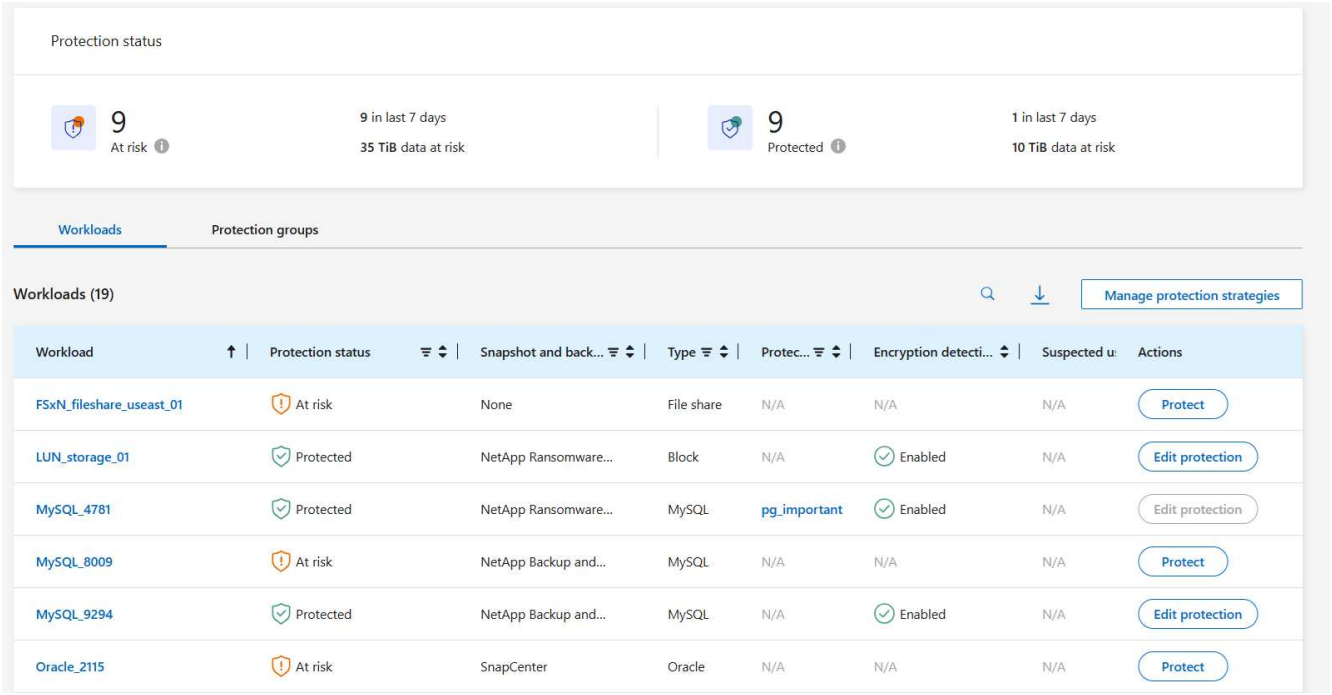
Replace existing backup or snapshot policies with a ransomware protection strategy

You can replace your existing backup or snapshot policies with a ransomware protection strategy. This approach removes your externally managed protection and configures detection and protection in

Ransomware Resilience.

Steps

1. From the Ransomware Resilience menu, select **Protection**.



2. From the Protection page, select a workload then select **Protect**.
3. Ransomware Resilience detects if there are existing active Backup and Recovery or SnapCenter policies. To replace the existing Backup and Recovery or SnapCenter policies, select the **Replace existing policies** box. When you select the box, Ransomware Resilience replaces the list of detection policies with detection policies.
4. Choose a protection policy. If no protection policy exists, select **Add** to create a new policy. For information about creating a policy, see Create a protection policy. Select **Next**.
5. If your strategy includes replication, select the **Destination system** and **Destination storage VM**. Select **Next**.
6. Select a backup destination or create a new one. Select **Next**.
   a. If your protection strategy includes user behavior detection, select a User activity agent in your environment to host the new data collectors. Ransomware Resilience creates the data collector automatically to transmit user activity events to Ransomware Resilience to detect anomalous user behavior.
7. Review the new protection strategy then select **Protect** to apply it.
8. On the Protection page, review the **Detection status** to confirm detection is Active.

Assign a different policy

You can replace the existing policy with a different one.

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, on the workload row, select **Edit protection**.

3. If the workload has an existing Backup and Recovery or SnapCenter policy that you want to maintain, uncheck **Replace existing policies**. To replace the existing policies, check **Replace existing policies**.
4. In the Policies page, select the down arrow for the policy you want to assign to review the details.
5. Select the policy you want to assign.
6. Select **Protect** to complete the change.

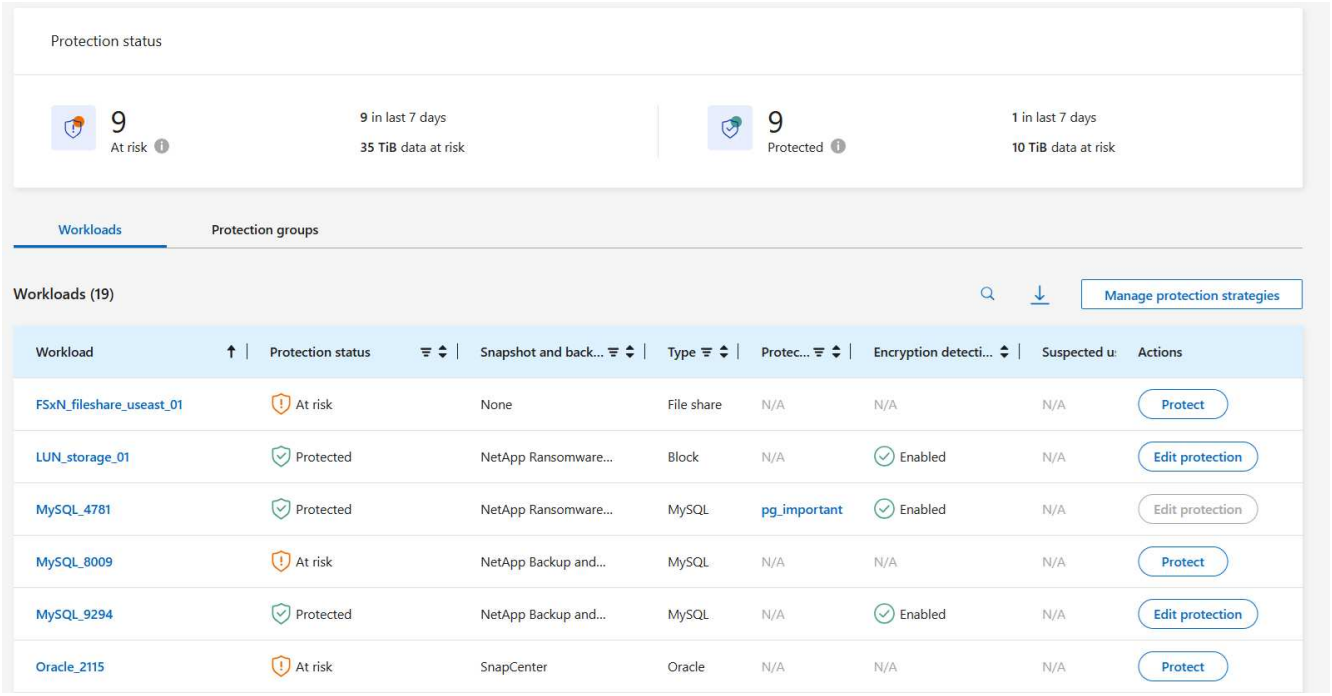
Create a protection group

Grouping file shares in a protection group makes it easier to protect your data estate. Ransomware Resilience can protect all volumes in a group at the same time rather than protecting each volume separately.

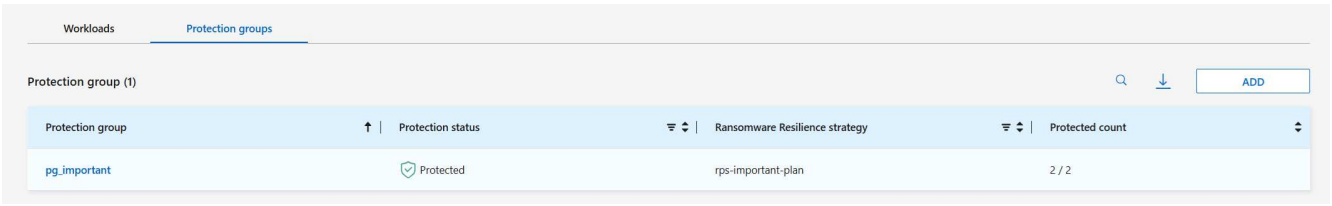
You can create groups regardless of their protection status (that is, groups not protected and groups that are protected). When you add a protection policy to a protection group, the new protection policy replaces any existing policy, including policies managed by SnapCenter and NetApp Backup and Recovery.

Steps

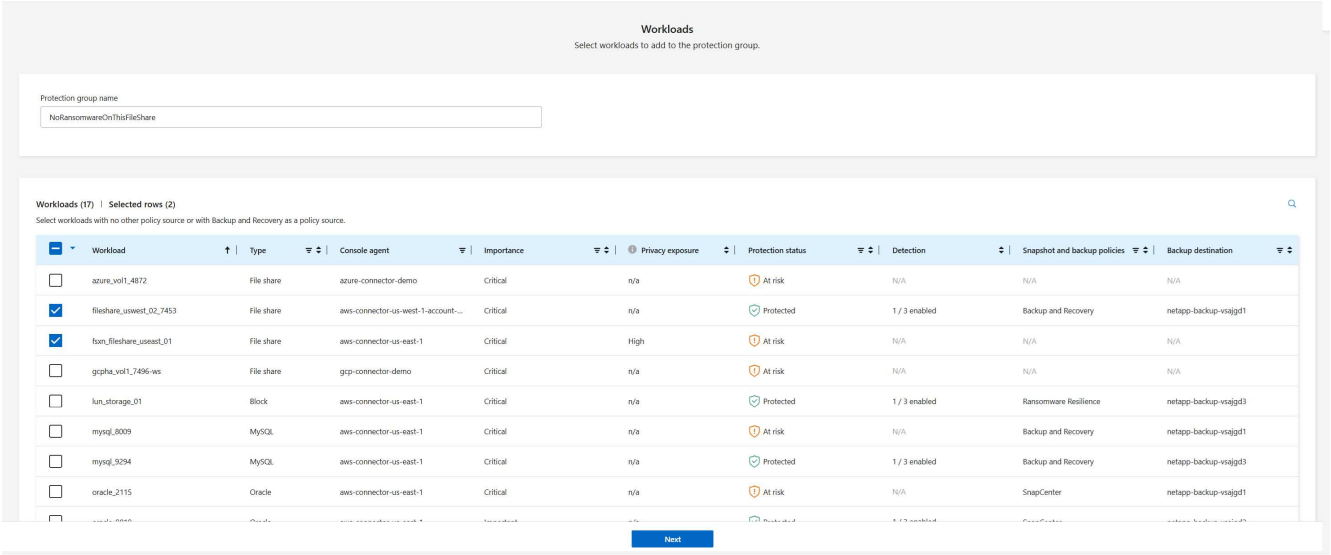
1. From the Ransomware Resilience menu, select **Protection**.



2. From the Protection page, select the **Protection groups** tab.



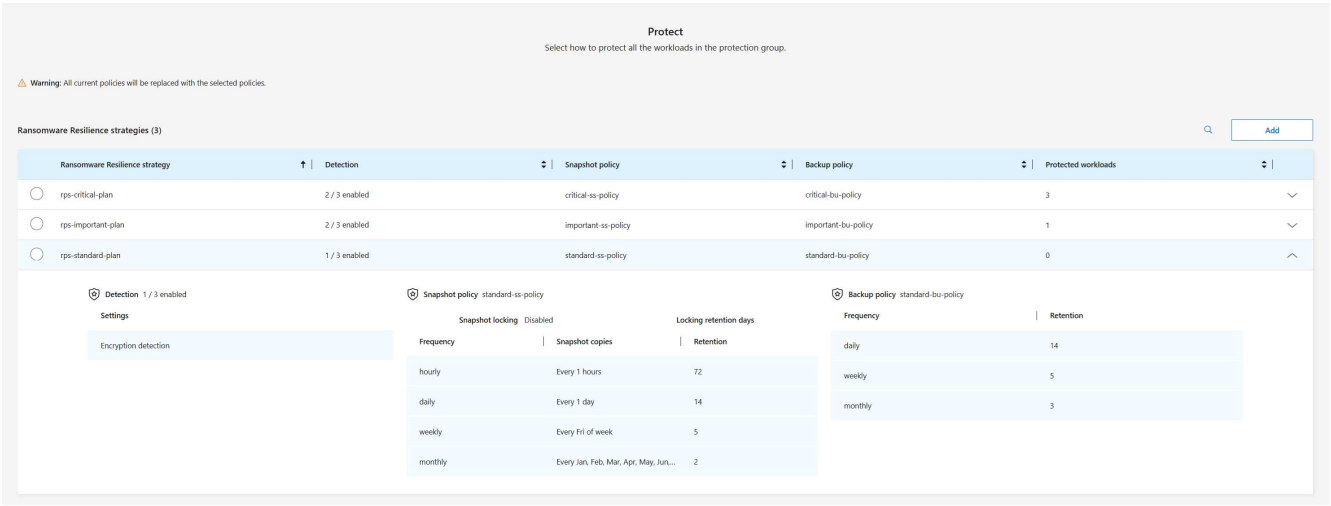
3. Select **Add**.



4. Enter a name for the protection group.
5. Select the workloads to add to the group.

   To see more details on the workloads, scroll to the right.

6. Select **Next**.



7. Select the policy to govern the protection for this group. To confirm, select **Next**.
8. If the protection strategy includes replication, review the replication settings.
   a. To replicate all snapshots to the same destination, check **Use same destination for each workload**. Choose a **Destination system** and **Destination storage VM** for the workloads under the Console agent section. + To use different destinations, uncheck that box. Review each workloads under each Console agent and assign a **Destination system** and **Destination storage VM** for each workload. Select **Next**.
9. To configure a backup policy, choose one then select **Next**.
10. If your detection policy includes user behavior detection, select the data collector you want to use then **Next**.
11. Review the selections for the protection group.

12. To finalize creation of the protection group, select **Add**.

Edit group protection

You can change the detection policy on an existing group.

Steps

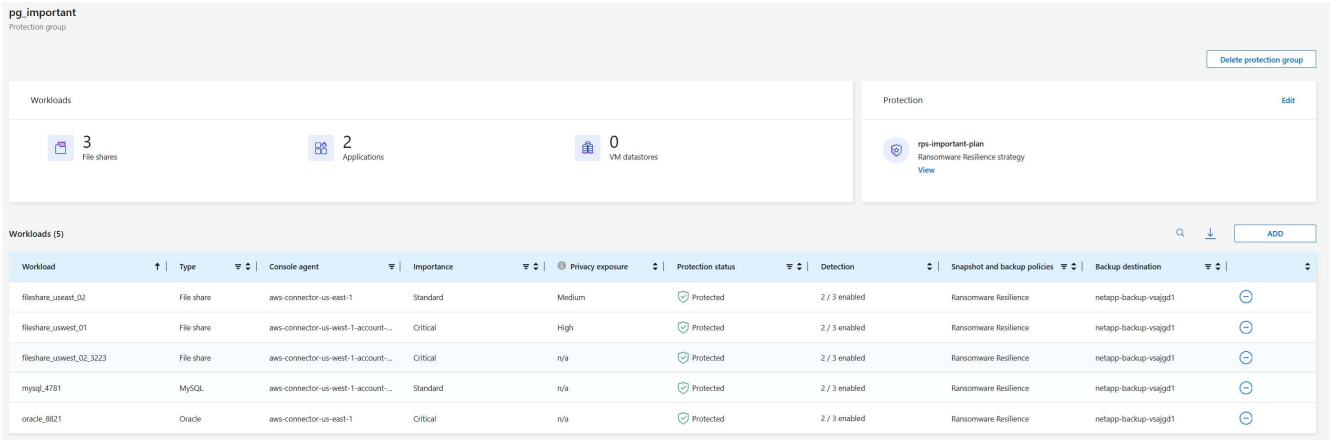
1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select the **Protection groups** tab then select the group whose policy you want to modify.
3. From protection group's overview page, select **Edit protection**.
4. Select an existing protection policy to apply or select **Add** to create a new protection policy. For more information about adding a protection policy see, Create a protection policy. Then select **Save**.
5. In the backup destination overview, select an existing backup destination or **Add a new backup destination**.
6. Select **Next** to review your changes.

Remove workloads from a group

You might later need to remove workloads from an existing group.

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select the **Protection groups** tab.
3. Select the group from which you want to remove one or more workloads.



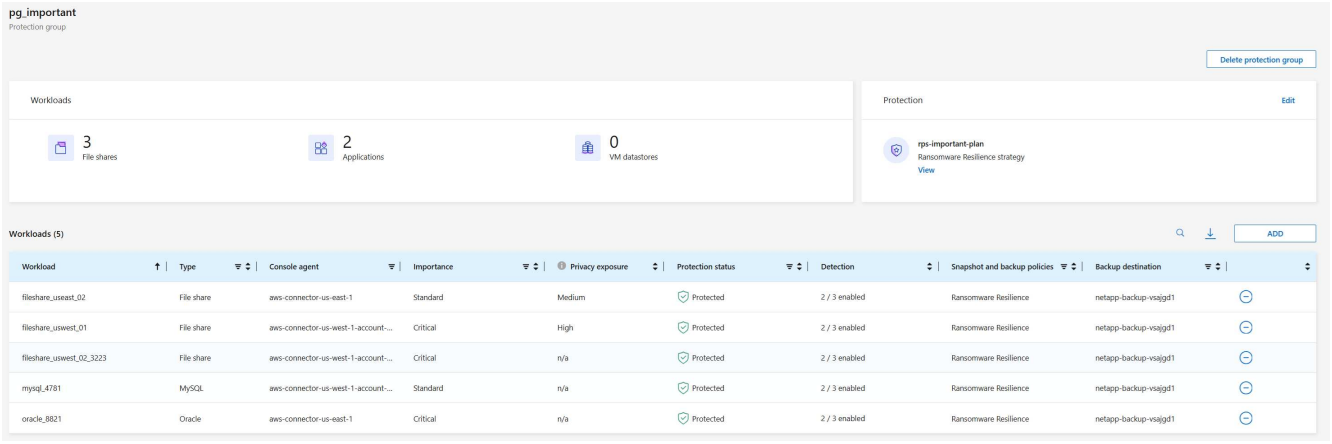
4. From the selected protection group page, select the workload you want to remove from the group and select the **Actions** ••• option.
5. From the Actions menu, select **Remove workload**.
6. Confirm that you want to remove the workload and select **Remove**.

Delete the protection group

Deleting the protection group removes the group and its protection but doesn't remove the individual workloads.

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select the **Protection groups** tab.
3. Select the group from which you want to remove one or more workloads.



4. From the selected protection group page, at the top right, select **Delete protection group**.
5. Confirm that you want to delete the group and select **Delete**.

Manage ransomware protection strategies

You can delete a ransomware strategy.

View workloads protected by a ransomware protection strategy

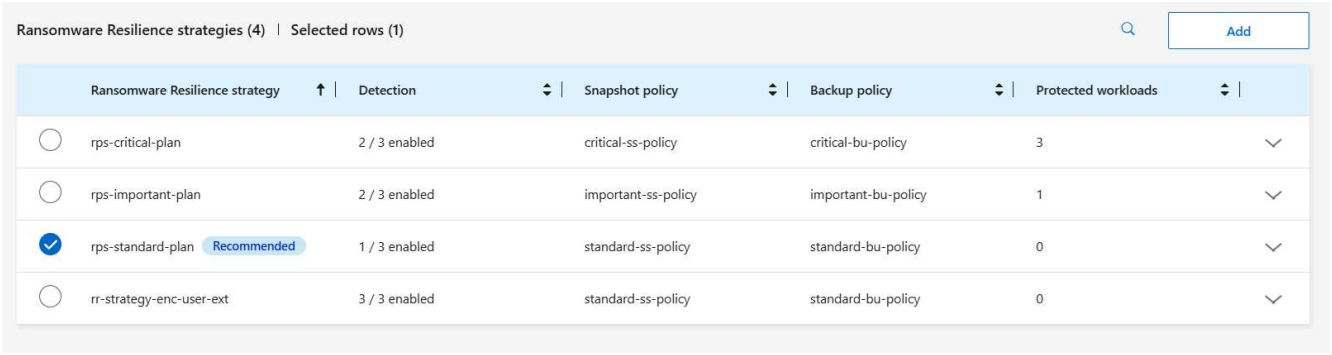
Before you delete a ransomware protection strategy, you might want to view which workloads are protected by that strategy.

You can view the workloads from the list of strategies or when you are editing a specific strategy.

Steps to view strategies

1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select **Manage protection strategies**.

   The Ransomware protection strategies page displays a list of strategies.



3. On the Ransomware protection strategies page in the Protected workloads column, select the down arrow at the end of the row.

Delete a ransomware protection strategy

You can delete a protection strategy that is not currently associated with any workloads.

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select **Manage protection strategies**.
3. In the Manage strategies page, select the **Actions** ••• option for the strategy you want to delete.
4. From the Actions menu, select **Delete policy**.

Scan for personally identifiable information with NetApp Data Classification in Ransomware Resilience

Within NetApp Ransomware Resilience, you can use NetApp Data Classification to scan and classify the data in a file share workload. Classifying data helps you determine whether the dataset includes personally identifiable information (PII), which can increase security risks. Data Classification is a core component of the NetApp Console and is available at no additional cost.

Data Classification utilizes AI-driven natural language processing for contextual data analysis and categorization, providing actionable insights into your data to address compliance requirements, detect security vulnerabilities, optimize costs, and accelerate migration.

This process can impact workload importance to help ensure you have the appropriate protection.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Identify privacy exposure with Data Classification

Before you use Data Classification within Ransomware Resilience, you need to enable Data Classification to scan your data.

You can deploy Data Classification within the Protection page of Ransomware Resilience. Follow the procedure to identify the privacy exposure. When you select **Identify exposure**, if you haven't already deployed Data Classification, a dialog enables you to enable Data Classification.

For more information about Data Classification, see:

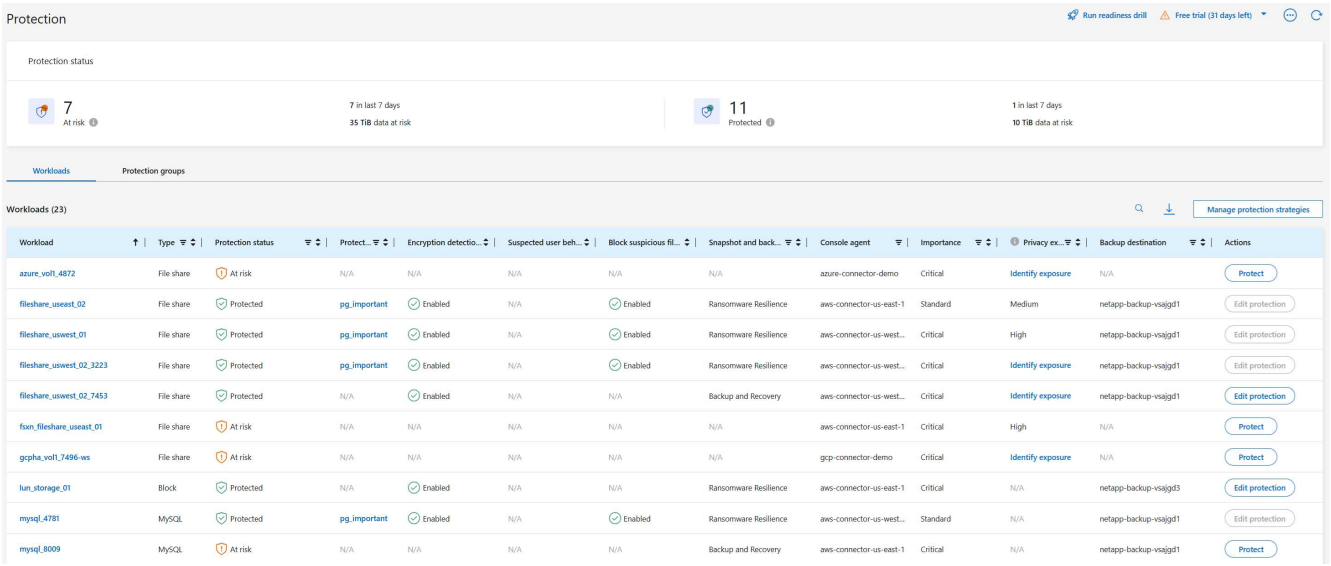
- Learn about Data Classification
- Categories of private data
- Investigate the data stored in your organization

Before you begin

Scanning for PII data in Ransomware Resilience is available if you've deployed Data Classification. Data Classification is available as part of the Console at no extra charge and can be deployed on-premises or in the customer cloud.

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. In the Protection page, locate a file share workload in the Workload column.



3. To enable Data Classification to scan your data for PII, in the **Privacy exposure** column, select **Identify exposure**.

> If you haven't deployed Data CCassification, selecting **Identify exposure** opens a dialog to deploy Data Classification. Select **Deploy**. After you've deployed Data Classification, you can return to the Protection page then select **Identify exposure**.

Result

Scanning can take several minutes depending on the size and number of the files. During the scan, the Protection page indicates it is identifying files and provides a file count. When scanning is complete, the Privacy exposure column rates the exposure level as Low, Medium, or High.

Review the privacy exposure

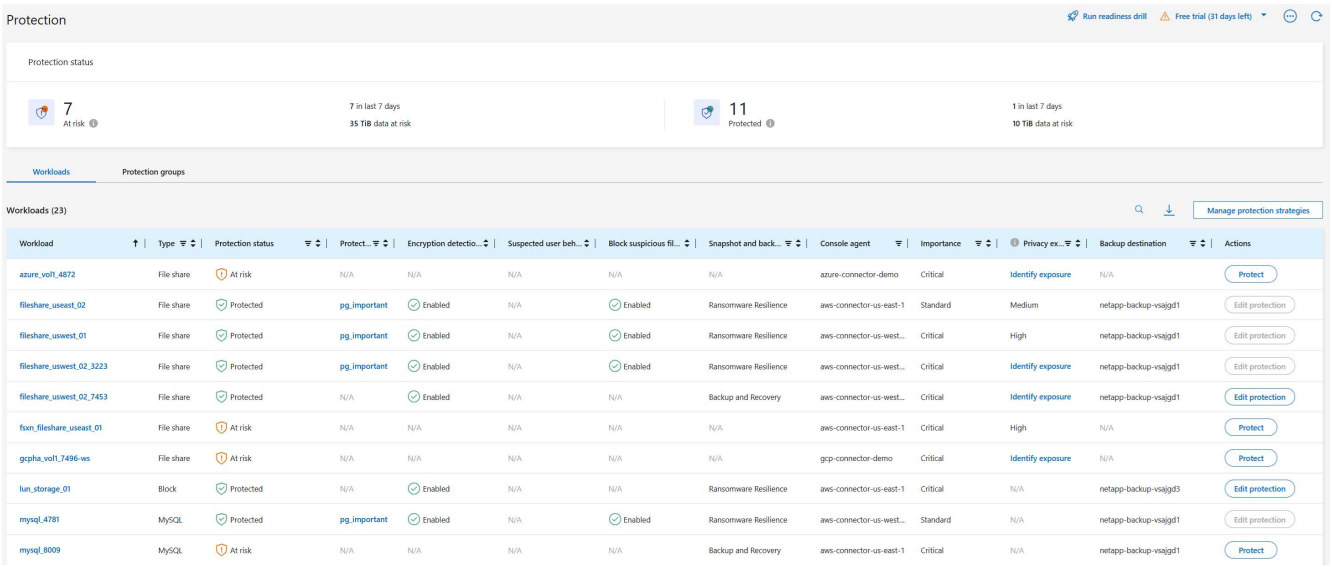
After Data Classification scans for PII, assess the risk.

PII data is classified into one of three designations:

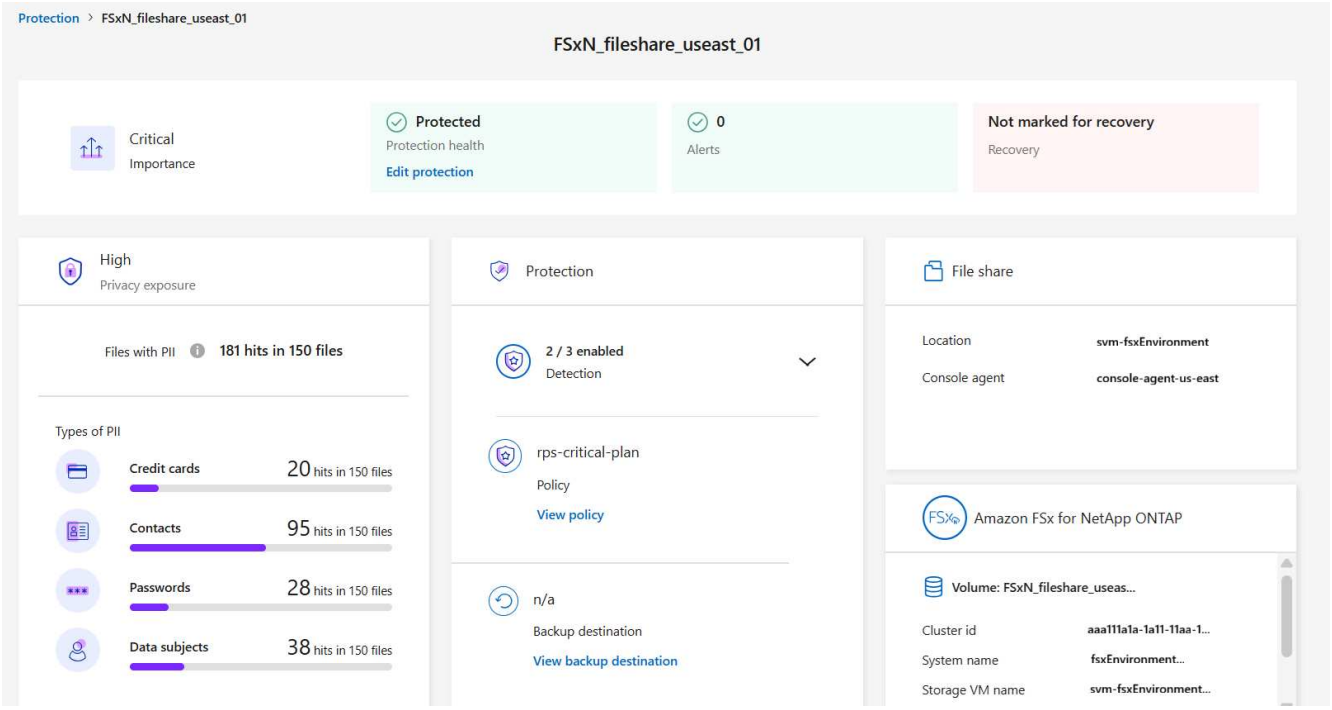
- **High**: Greater than 70% of files contain PII
- **Medium**: Greater than 30% and less than 70% of files contain PII
- **Low**: Greater than 0% and less than 30% of files contain PII

Steps

1. From the Ransomware Resilience menu, select **Protection**.
2. In the Protection page, locate the file share workload in the Workload column that shows a status in the Privacy exposure column.



3. Select the workload link in the Workload column to see workload details.



4. In the Workload details page, look at the details in the Privacy exposure tile.

Impact of privacy exposure on workload importance

Privacy exposure changes can impact the workload importance.

When privacy exposure:	From this privacy exposure:	To this privacy exposure:	Then, workload importance does this: .
Decreases	High, Medium, or Low	Medium, Low, or None	Remains the same
Increases	None	Low	Remains at Standard
	Low	Medium	Changes from Standard to Important
	Low or Medium	High	Changes from Standard or Important to Critical

For more information

For details about Data Classification, refer to the Data Classification documentation:

- Learn about Data Classification
- Categories of private data
- Investigate the data stored in your organization

Manage alerts in NetApp Ransomware Resilience

When NetApp Ransomware Resilience detects a possible attack, it displays an alert on the Dashboard and in the Notifications area. Ransomware Resilience immediately takes a snapshot. Review the potential risk in the Ransomware Resilience **Alerts** tab.

If Ransomware Resilience detects a possible attack, a notification appears in the Console Notification settings, and an email is sent to the configured addresses. The email includes information about the severity, the impacted workload, and a link to the alert in the Ransomware Resilience **Alerts** tab.

You can dismiss false positives or decide to recover your data immediately.

If you dismiss the alert, Ransomware Resilience learns this behavior, associates it with normal operations, and doesn't initiate an alert on it again.

To begin to recover your data, mark the alert as ready for recovery so that your storage administrator can begin the recovery process.

Each alert might include multiple incidents on different volumes and statuses. Review all incidents.

Ransomware Resilience provides information called *evidence* about what caused the alert to be issued, such as the following:

- File extensions were created or changed
- File creation with a comparison of detected versus expected rates

- File deletion with a comparison of detected versus expected rates
- When encryption is high, without file extension changes

An alert is classified as one of the following:

- **Potential attack**: An alert occurs when Autonomous Ransomware Protection detects a new extension and the occurrence is repeated more than 20 times in the last 24 hours (default behavior).
- **Warning**: A warning occurs based on the following behaviors:
  - Detection of a new extension has not been identified before and the same behavior does not repeat enough times to declare it as an attack.
  - High entropy is observed.
  - File read, write, rename, or delete activity doubled compared to normal levels.

For SAN environments, warnings are based on high entropy only.

Evidence is based on information from Autonomous Ransomware Protection in ONTAP. For details, refer to Autonomous Ransomware Protection overview.

An alert can have one of the following statuses:

- **New**
- **Inactive**

An alert incident can have the following states:

- **New**: All incidents are marked "new" when they are first identified.
- **In review**: You can mark an incident as in review while you evaluate it.
- **Dismissed**: If you suspect that the activity is not a ransomware attack, you can change the status to "Dismissed."

After you dismiss an attack, you can't revert its status. If you dismiss a workload, all snapshot copies taken automatically in response to the potential ransomware attack will be permanently deleted.

- **Dismissing**: The incident is in the process of being dismissed.
- **Resolved**: The incident has been fixed.
- **Auto Resolved**: For low priority alerts, the incident is automatically resolved if there has been no action taken on it within five days.

If you configured a security and event management system (SIEM) in Ransomware Resilience in the Settings page, Ransomware Resilience sends alert details to your SIEM system.

View alerts

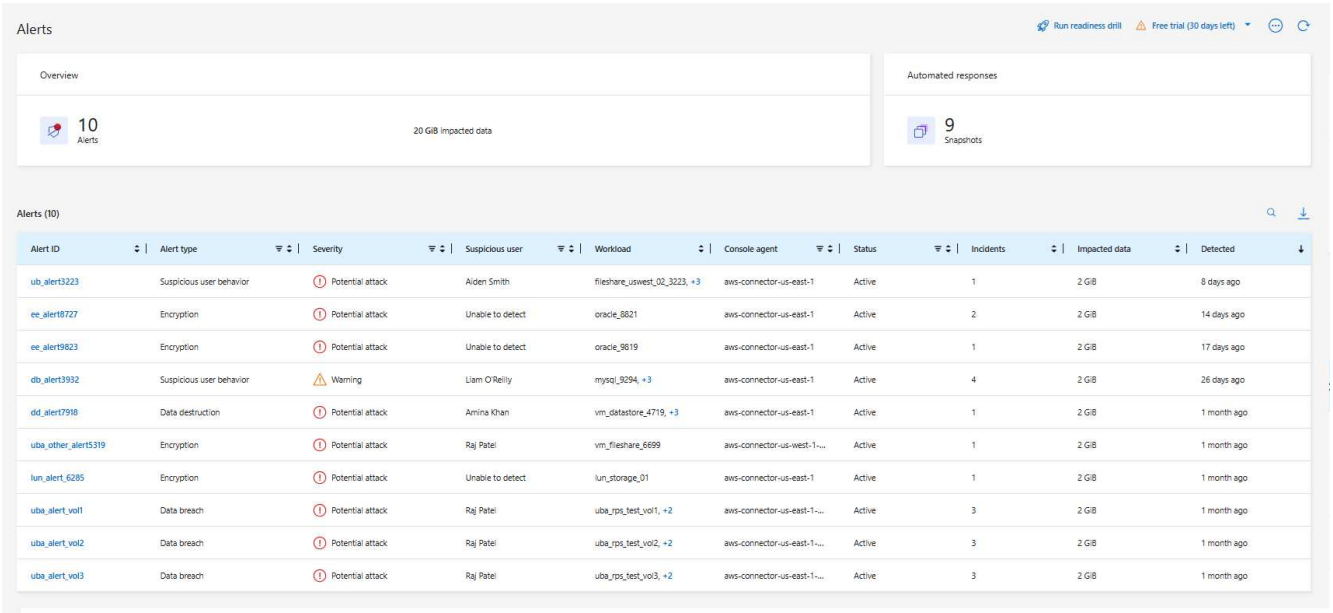
You can access alerts from the Ransomware Resilience Dashboard or from the **Alerts** tab.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience

admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. In the Ransomware Resilience Dashboard, review the Alerts pane.
2. Select **View all** under one of the statuses.
3. Select an alert to review all incidents on each volume for each alert.
4. To review additional alerts, select **Alert** in the breadcrumbs at the upper left.
5. Review the alerts on the Alerts page.



6. Continue with one of the following:
   - Detect malicious activity and anomalous user behavior.
   - Mark ransomware incidents as ready for recovery (after incidents are neutralized).
   - Dismiss incidents that are not potential attacks.

Respond to an alert email

When Ransomware Resilience detects a potential attack, it sends an email notification to the subscribed users based on their subscription notification preferences configured in the NetApp Console settings. The email contains information about the alert, including the severity and resources impacted.

To set up email notifications in the Console, see Set email notification settings.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. View the email.
2. In the email, select **View alert** and log in to Ransomware Resilience .

   The Alerts page appears.

3. Review all incidents on each volume for each alert.
4. To review additional alerts, click on **Alert** in the breadcrumbs at the upper left.
5. Continue with one of the following:
    - Detect malicious activity and anomalous user behavior.
    - Mark ransomware incidents as ready for recovery (after incidents are neutralized).
    - Dismiss incidents that are not potential attacks.

Detect malicious activity and anomalous user behavior

Looking at the Alerts tab, you can identify whether there is malicious activity or anomalous user behavior.

You must have configured a user activity agent and enabled a protection policy with user behavior detection to view user-level alerts. The **Suspicious user** column appears in the Alerts dashboard only when user behavior detection is enabled. To enable suspicious user detection, see Suspicious user activity.

View malicious activity

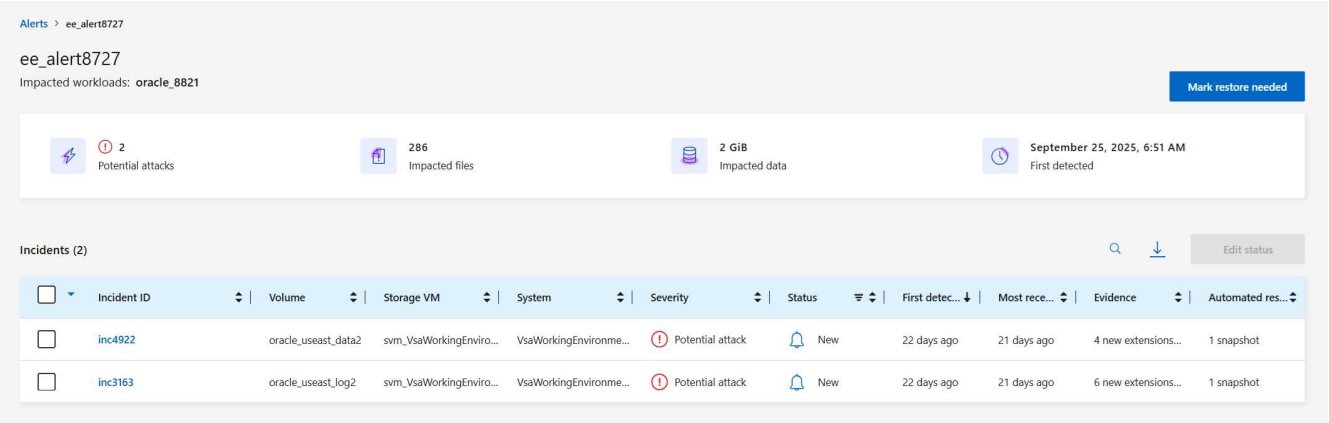
When Autonomous Ransomware Protection triggers an alert in Ransomware Resilience , you can view the following details:

- Entropy of incoming data
- Expected creation rate of new files compared to detected rate
- Expected deletion rate of files compared to detected rate
- Expected rename rate of files compared to detected rate
- Impacted files and directories

These details are viewable for NAS workloads. For SAN environments, only the entropy data is available.

Steps

1. From the Ransomware Resilience menu, select **Alerts**.
2. Select an alert.
3. Review the incidents in the alert.



4. Select an incident to review the details of the incident.

View anomalous user behavior

If you've configured suspicious user detection to view anomalous user behavior, you can view user-level data and block specific users. To enable suspicious user settings, see Configure Ransomware Resilience settings.

Steps

1. From the Ransomware Resilience menu, select **Alerts**.
2. Select an alert.
3. Review the incidents in the alert.
4. To block a suspected user in your environment, select **Block** under the user's name.

Mark ransomware incidents as ready for recovery (after incidents are neutralized)

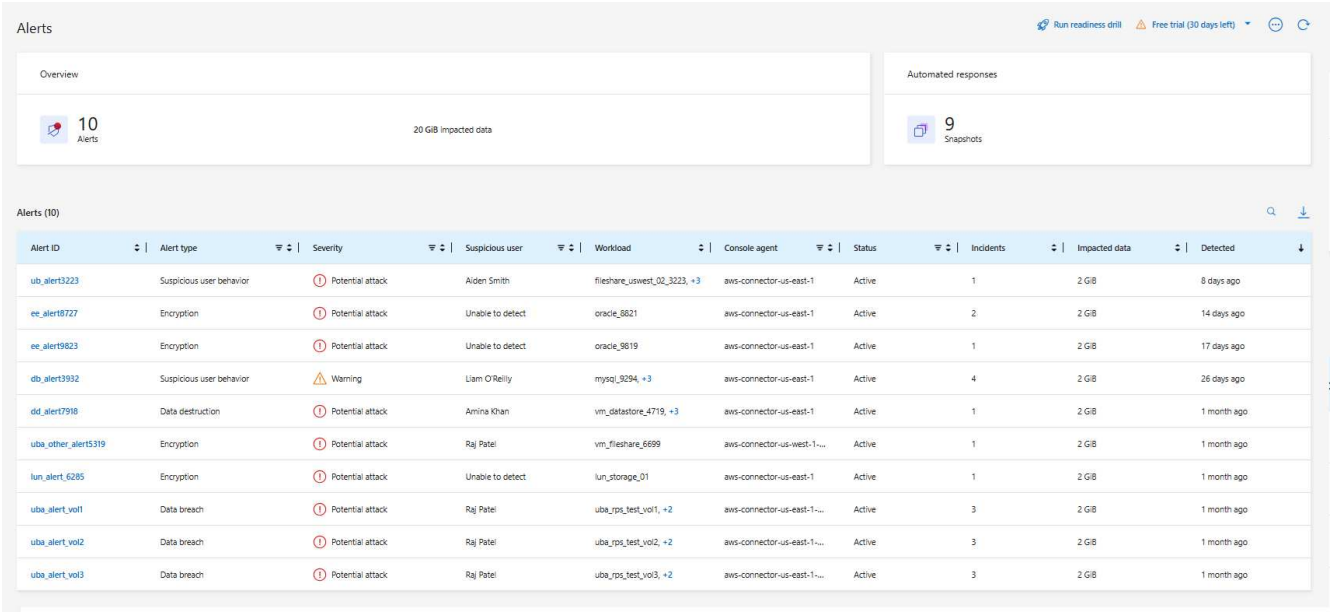
After stopping the attack, notify your storage administrator that the data is ready so they can initiate the recovery process.

Required Console role

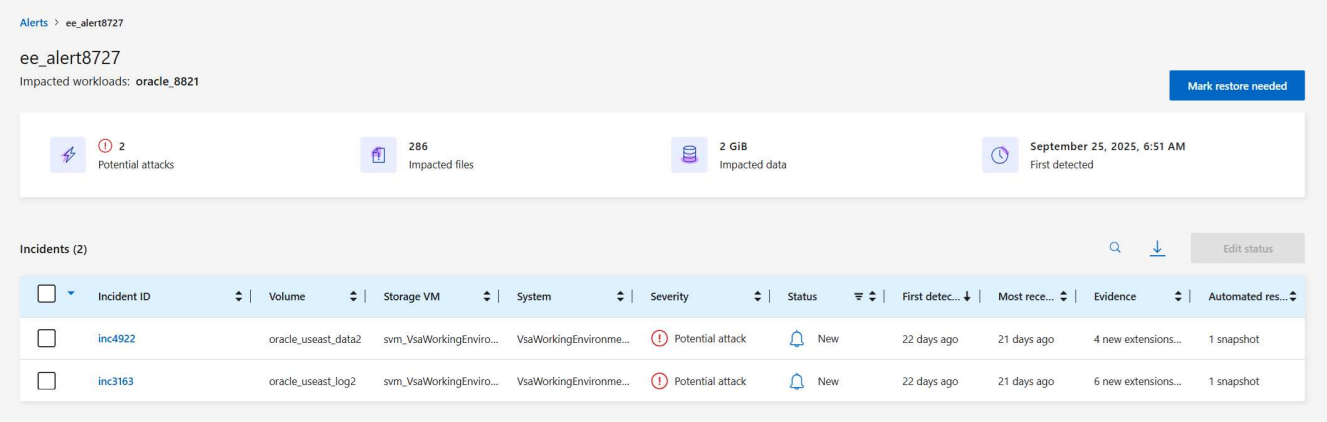
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. From the Ransomware Resilience menu, select **Alerts**.



2. In the Alerts page, select the alert.
3. Review the incidents in the alert.



4. If you determine that the incidents are ready for recovery, select **Mark restore needed**.
5. Confirm the action and select **Mark restore needed**.
6. To initiate the workload recovery, select **Recover** workload in the message or select the **Recovery** tab.

Result

After the alert is marked for restore, the alert moves from the Alerts tab to the Recovery tab.

Dismiss incidents that are not potential attacks

After you review incidents, you need to determine whether the incidents are potential attacks. If they aren't actual threats, they can be dismissed.

You can dismiss false positives or decide to recover your data immediately. If you dismiss the alert, Ransomware Resilience learns this behavior and associates it with normal operations, and doesn't initiate an alert on such a behavior again.

If you dismiss a workload, all snapshot copies taken automatically in response to a potential ransomware attack are permanently deleted.

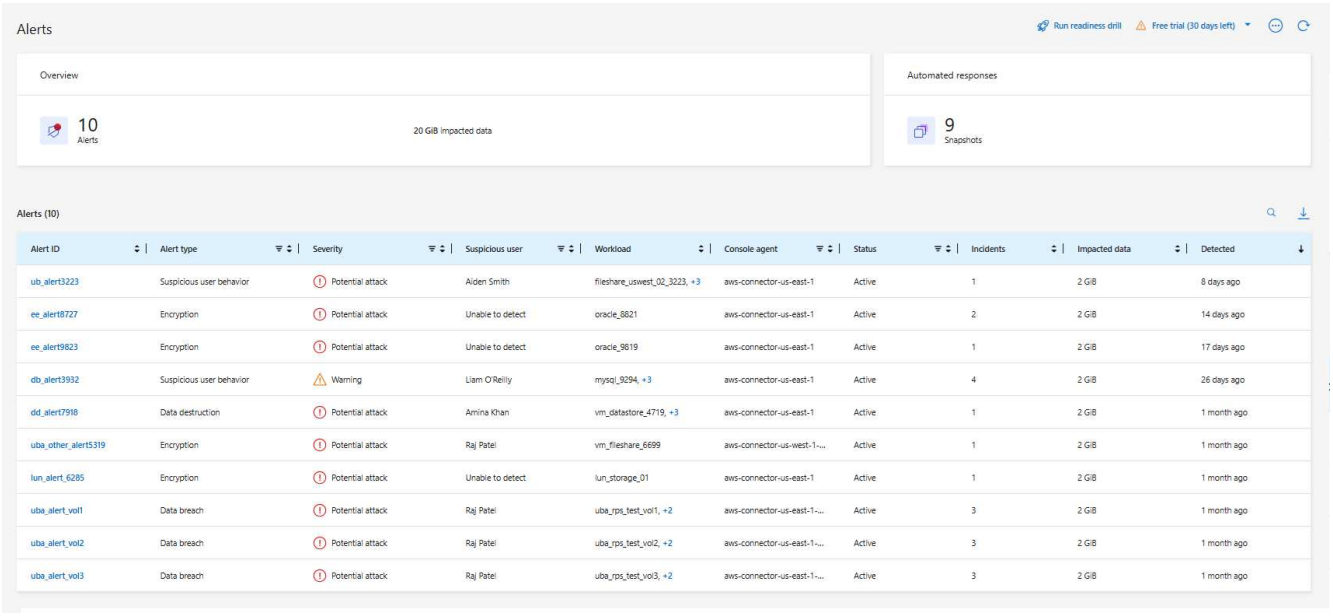
If you dismiss an alert, you can't change its status or undo this change.

Required Console role

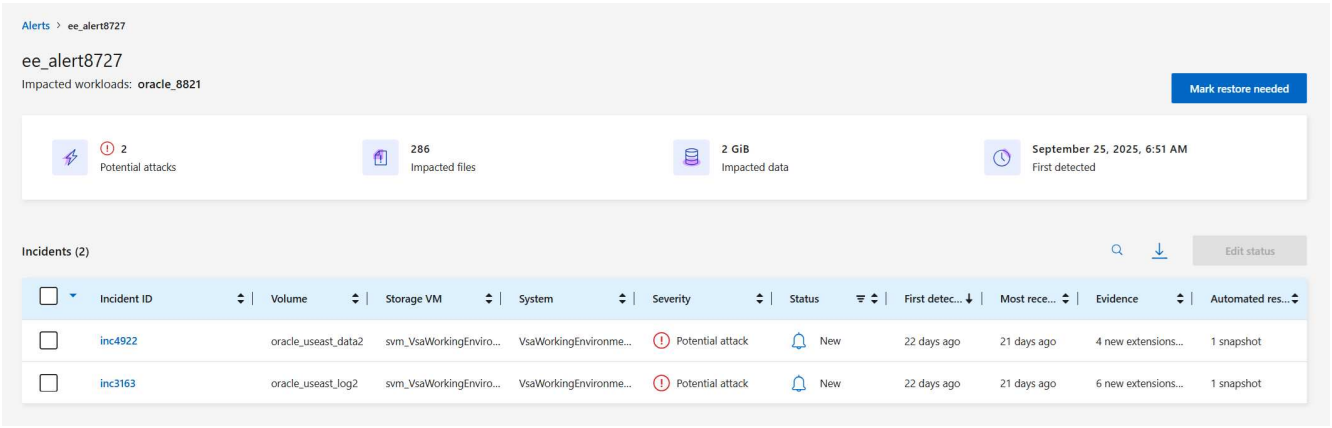
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

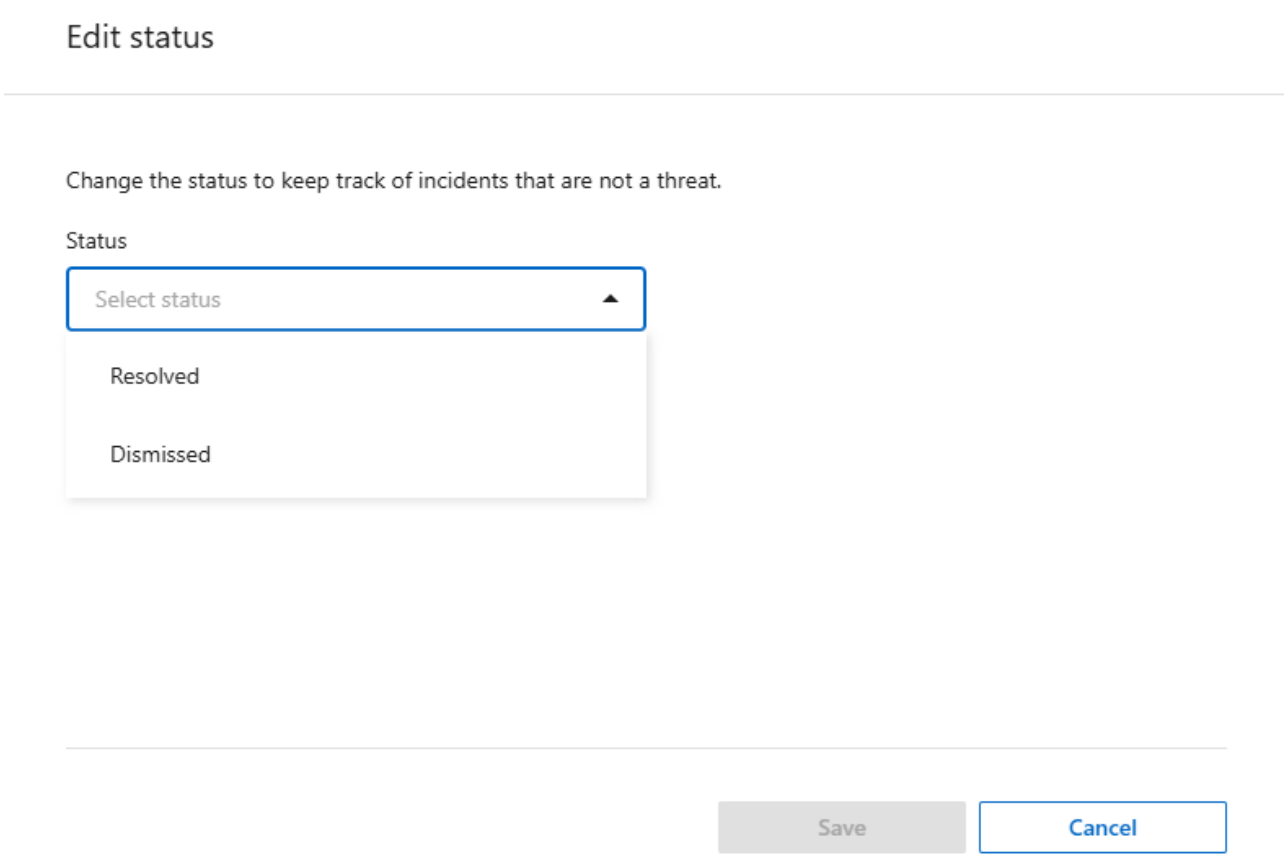
1. From the Ransomware Resilience menu, select **Alerts**.



2. In the Alerts page, select the alert.



3. Select one or more incidents. Alternately, select all incidents by selecting the Incident ID box at the top left of the table.
4. If you determine that the incident is not a threat, dismiss it as a false positive:
   - Select the incident.
   - Select the **Edit status** button above the table.



5. From the Edit status box, choose the **Dismissed** status.

   Additional information about the workload and the snapshot copies are deleted appears.

6. Select **Save**.

   The status on the incident or incidents changes to "Dismissed."

View a list of impacted files

Before you restore an application workload at the file level, you can view a list of impacted files. You can access the Alerts page to download a list of impacted files. Then use the Recovery page to upload the list and choose which files to restore.

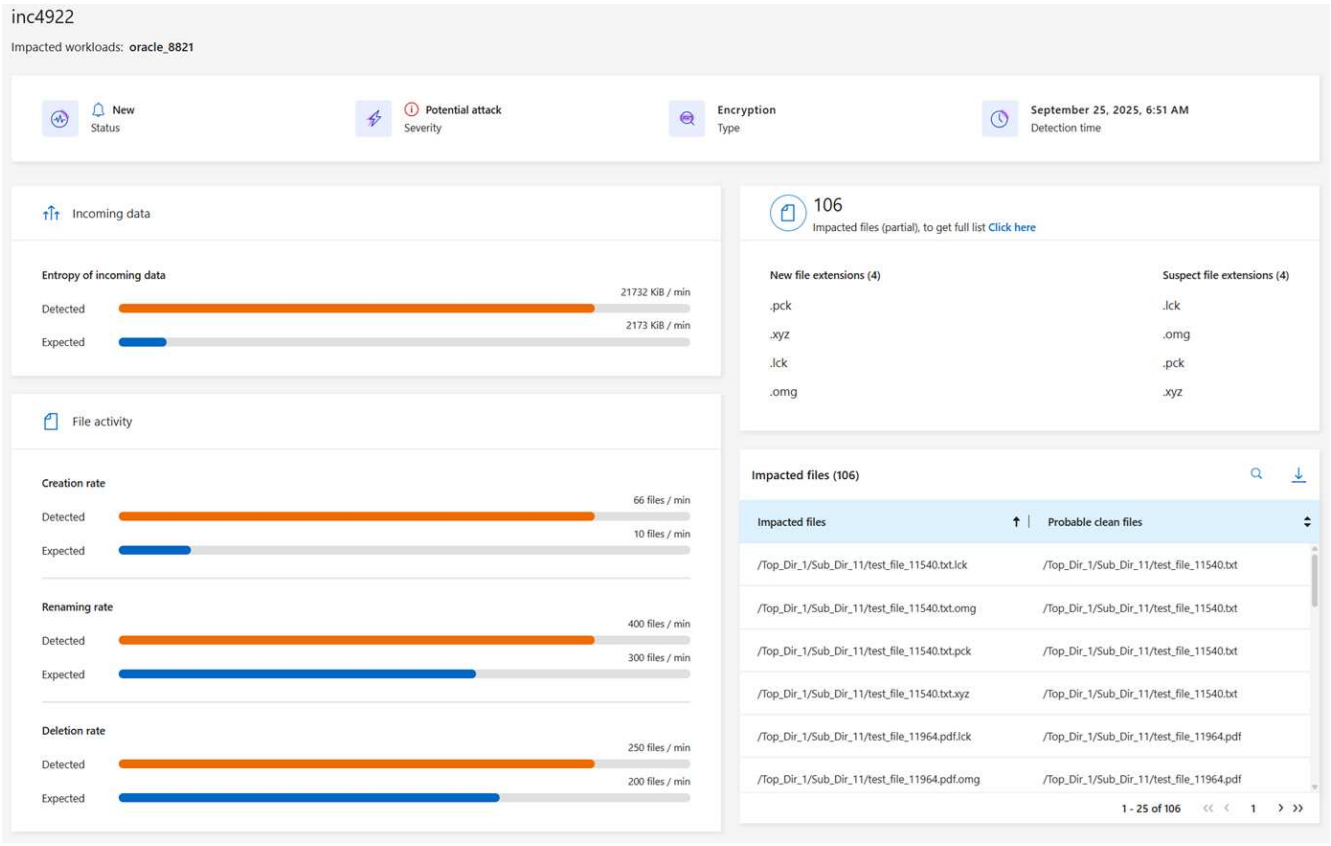
Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps
Use the Alerts page to retrieve the list of impacted files.

If a volume has multiple alerts, you might need to download the CSV list of impacted files for each alert.

1. From the Ransomware Resilience menu, select **Alerts**.

2. On the Alerts page, sort the results by workload to show the alerts for the application workload that you want to restore.
3. From the list of alerts for that workload, select an alert.
4. For that alert, select a single incident.



5. For that incident, select the download icon to download the list of impacted files in CSV format.

Recover from a ransomware attack (after incidents are neutralized) with NetApp Ransomware Resilience

After workloads have been marked "Restore needed", NetApp Ransomware Resilience recommends a recovery point actual (RPA) and orchestrates the workflow for a crash-resistant recovery.

- If the application or VM is managed by SnapCenter, Ransomware Resilience restores the application or VM back to its previous state and last transaction using the application-consistent or VM-consistent process. The application or VM-consistent restore adds any data that did not make it into storage, for example, data in cache or in an I/O operation, to the data in the volume.
- If the application or VM is *not* managed by SnapCenter and is managed by NetApp Backup and Recovery or Ransomware Resilience, Ransomware Resilience performs a crash-consistent restore, where all the data that was in the volume at the same point of time is restored, for example, if the system crashed.

  You can restore the workload by selecting all volumes, specific volumes, or specific files.

Workload recovery can impact running workloads. You should coordinate recovery processes with the appropriate stakeholders.

A workload can have one of the following restore statuses:

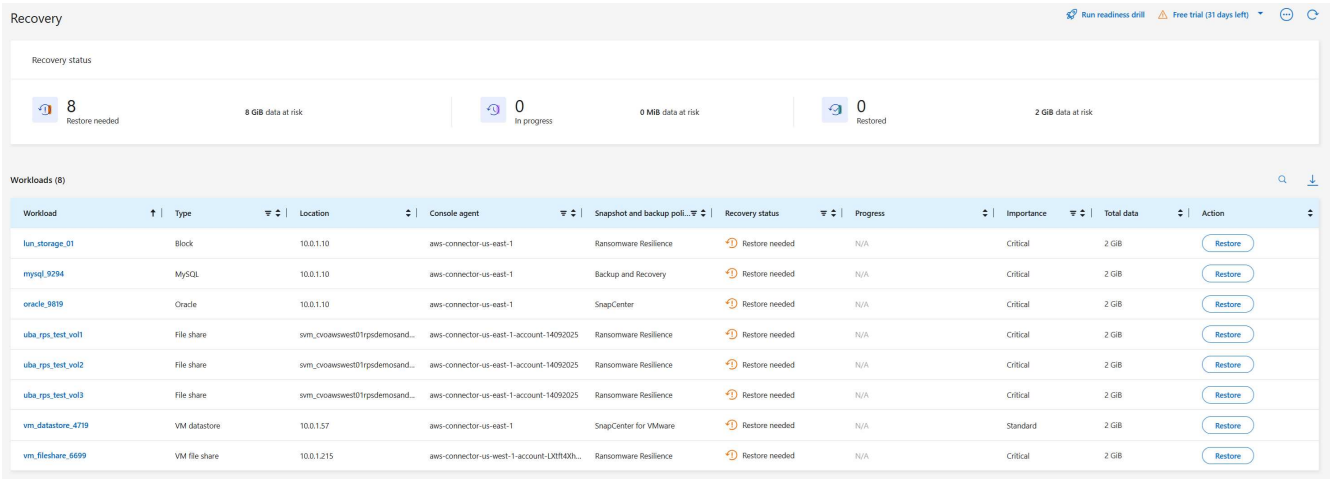
- **Restore needed**: The workload needs to be restored.
- **In progress**: The restore operation is currently underway.
- **Restored**: The workload has been restored.
- **Failed**: The workload restore process could not be completed.

View workloads that are ready to be restored

Review the workloads that are in the "Restore needed" recovery status.

Steps

1. Do one of the following:
   - From the Dashboard, review the "Restore needed" totals in the Alerts pane and select **View all**.
   - From the menu, select **Recovery**.
2. Review the workload information in the **Recovery** page.



Restore a workload managed by SnapCenter

Using Ransomware Resilience, the storage administrator can determine how best to restore workloads either from the recommended restore point or the preferred restore point.

The application state will change if required for the restore. The application will be restored to its previous state from control files, if they are included in the backup. After the restore finishes, the application opens in READ-WRITE mode.

Required Console role

To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. From Ransomware Resilience, select **Recovery**.

2. Review the workload information in the **Recovery** page.
3. Select a workload that is in the "Restore needed" state.
4. To restore, select **Restore**.
5. **Restore scope**: Application-consistent (or for SnapCenter for VMs, the restore scope is "By VM")
6. **Source**: Select the down arrow next to Source to see details. Select the restore point that you want to use to restore the data.

   Ransomware Resilience identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

7. **Destination**: Select the down arrow next to Destination to see details.
   a. Select the original or alternate location.
   b. Select the system.
   c. Select the Storage VM.
8. If the original destination does not have enough space to restore the workload, a "Temporary storage" row appears. You can select the temporary storage to restore the workload data. The restored data will be copied from the temporary storage to the original location. Click on the **Down arrow** in the Temporary storage row and set the destination cluster, storage VM, and local tier.
9. Select **Save**.
10. Select **Next**.
11. Review your selections.
12. Select **Restore**.
13. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a workload not managed by SnapCenter

Using Ransomware Resilience, the storage administrator can determine how best to restore workloads either from the recommended restore point or the preferred restore point.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

The security storage admin can recover data at different levels:

- Recovery all volumes
- Recover an application at the volume level or file and folder level.
- Recover a file share at the volume level, directory, or file/folder level.
- Recover from a datastore at a VM level.

The process differs depending on the workload type.

Steps

1. From the Ransomware Resilience menu, select **Recovery**.

2. Review the workload information in the **Recovery** page.
3. Select a workload that is in the "Restore needed" state.
4. To restore, select **Restore**.
5. **Restore scope**: Select the type of restore you want to complete:
   - All volumes
   - By volume
   - By file: You can specify a folder or single files to restore.

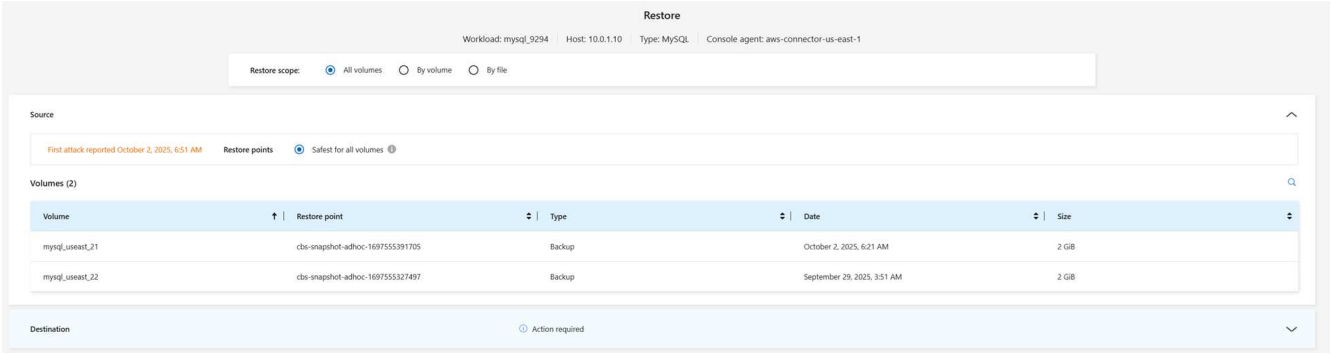
   For SAN workloads, you can only restore by workload.

   You can select up to 100 files or a single folder.

6. Continue with one of the following procedures depending on whether you chose application, volume, or file.

Restore all volumes

1. From the Ransomware Resilience menu, select **Recovery**.
2. Select a workload that is in the "Restore needed" state.
3. To restore, select **Restore**.
4. On the Restore page, in the Restore scope, select **All volumes**.



5. **Source**: Select the down arrow next to Source to see details.
   a. Select the restore point that you want to use to restore the data.

   Ransomware Resilience identifies the best restore point as the latest backup just before the incident and shows a "Safest for all volumes" indication. This means that all volumes will be restored to a copy prior to the first attack on the first volume detected.

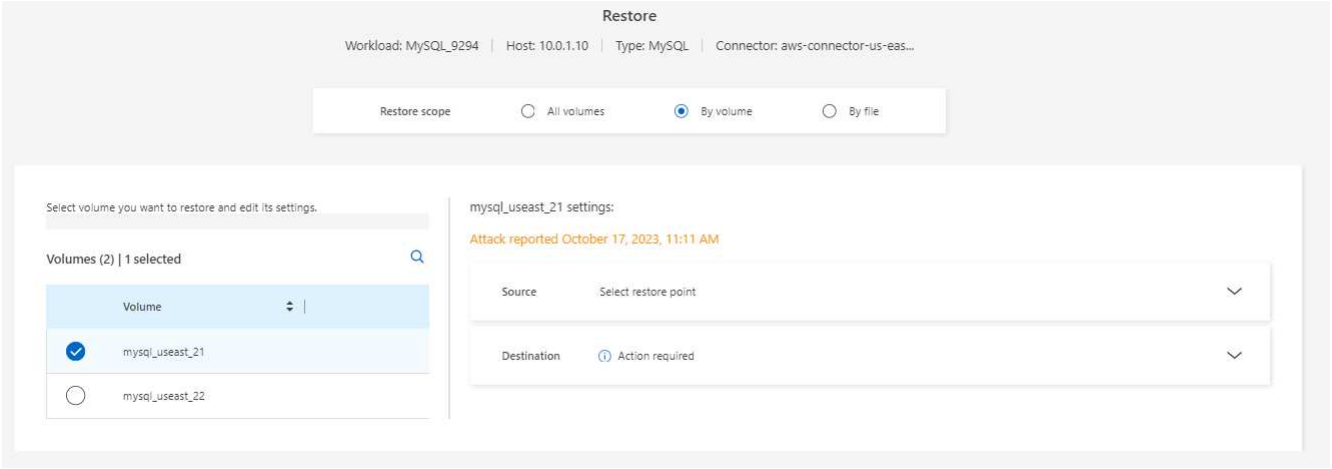
6. **Destination**: Select the down arrow next to Destination to see details.
   a. Select the system.
   b. Select the Storage VM.
   c. Select the aggregate.
   d. Change the volume prefix that will be prepended to all new volumes.

The new volume name appears as prefix + original volume name + backup name + backup date.

7. Select **Save**.
8. Select **Next**.
9. Review your selections.
10. Select **Restore**.
11. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the volume level

1. From the Ransomware Resilience menu, select **Recovery**.
2. Select an application workload that is in the "Restore needed" state.
3. To restore, select **Restore**.
4. On the Restore page, in the Restore scope, select **By volume**.



5. On the list of volumes, select the volume you want to restore.
6. **Source**: Select the down arrow next to Source to see details.
   a. Select the restore point that you want to use to restore the data.

Ransomware Resilience identifies the best restore point as the latest backup just before the incident and shows a "Recommended" indication.

7. **Destination**: Select the down arrow next to Destination to see details.
   a. Select the system.
   b. Select the Storage VM.
   c. Select the aggregate.
   d. Review the new volume name.

The new volume name appears as the original volume name + backup name + backup date.

8. Select **Save**.
9. Select **Next**.
10. Review your selections.
11. Select **Restore**.
12. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the file level

Before you restore an application workload at the file level, you can view a list of impacted files. You can access the Alerts page to download a list of impacted files. Then use the Recovery page to upload the list and choose which files to restore.

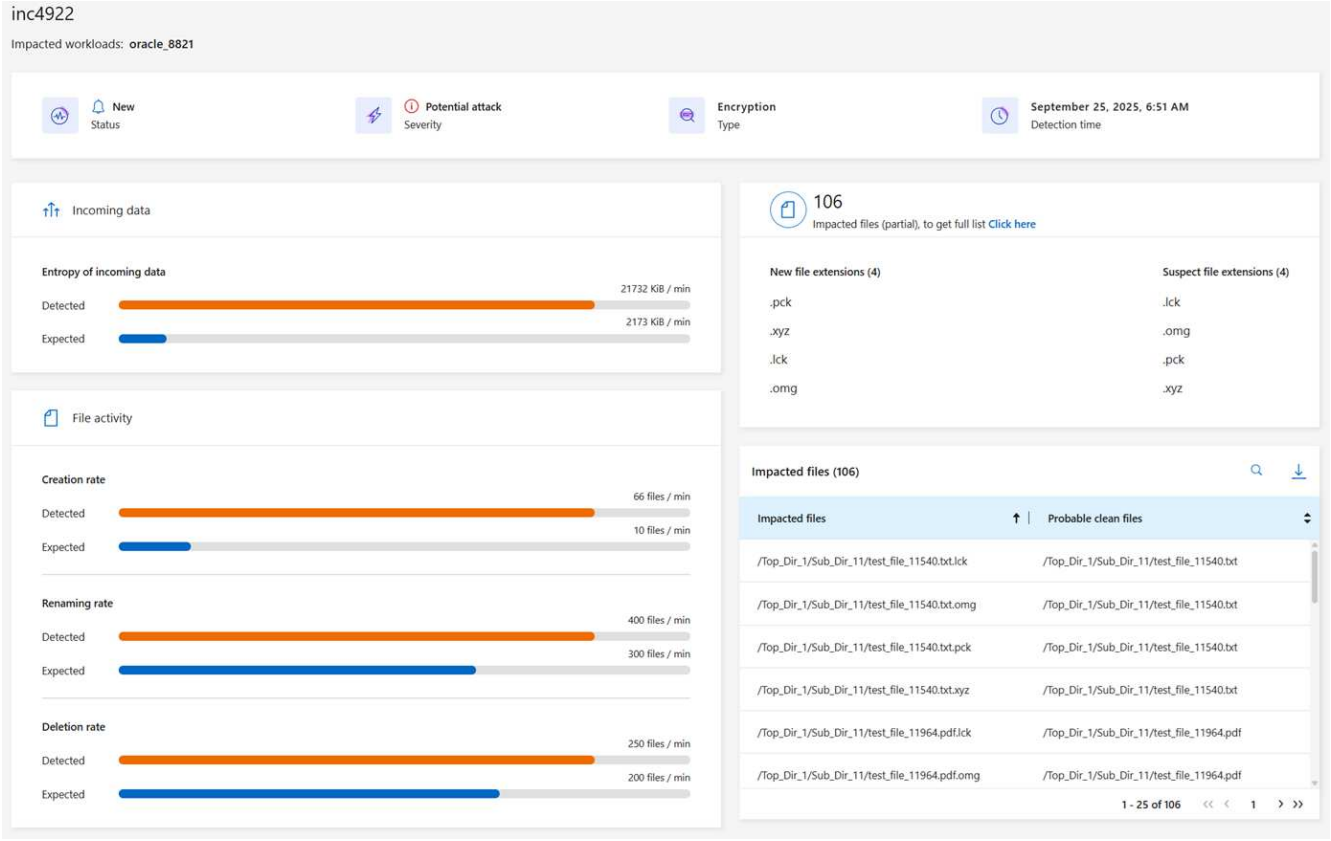
You can restore an application workload at the file level to the same or different system.

Steps to get the list of impacted files

Use the Alerts page to retrieve the list of impacted files.

If a volume has multiple alerts, you will need to download the CSV list of impacted files for each alert.

1. From the Ransomware Resilience menu, select **Alerts**.
2. On the Alerts page, sort the results by workload to show the alerts for the application workload that you want to restore.
3. From the list of alerts for that workload, select an alert.
4. For that alert, select a single incident.



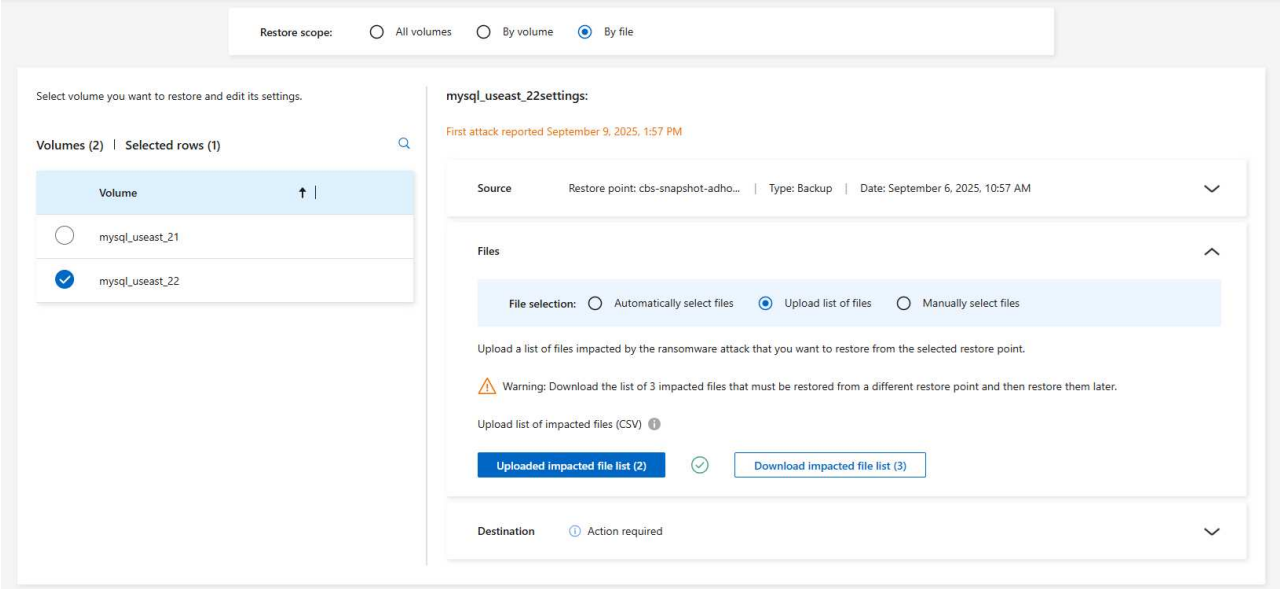
5. To see the full list of files, select **Click here** at the top of the Impacted files pane.
6. For that incident, select the download icon and download the list of impacted files in CSV format.

Steps to restore those files

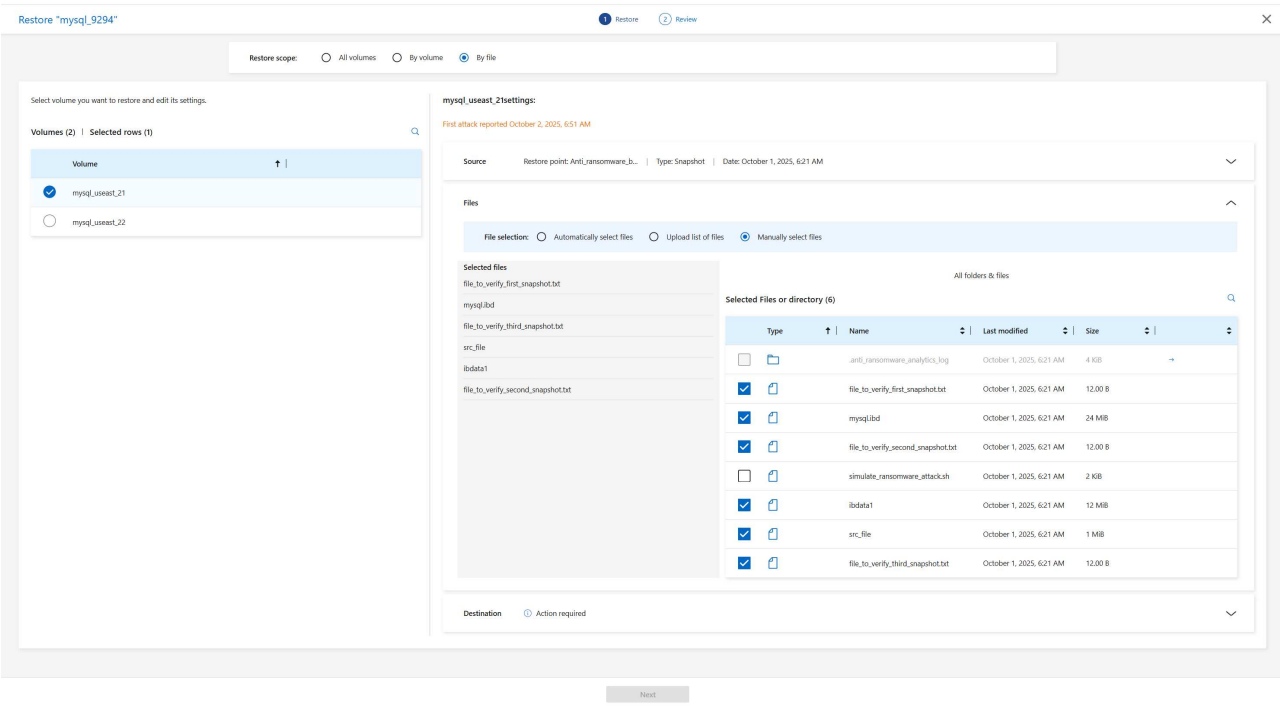
1. From the Ransomware Resilience menu, select **Recovery**.
2. Select an application workload that is in the "Restore needed" state.
3. To restore, select **Restore**.
4. On the Restore page, in the Restore scope, select **By file**.
5. On the list of volumes, select the volume that contains the files that you want to restore.
6. **Restore point**: Select the down arrow next to **Restore point** to see details. Select the restore point that you want to use to restore the data.

> The Reason column in the Restore points pane shows the reason for the snapshot or backup as either "Scheduled" or "Automated response to ransomware incident."

7. **Files**:
   - **Automatically select files**: Let Ransomware Resilience select the files to be restored.
   - **Upload list of files**: Upload a CSV file that contains the list of impacted files that you got from the Alerts page or that you have. You can restore up to 10,000 files at a time.



- **Manually select files**: Select up to 10,000 files or a single folder to restore.



If any files cannot be restored using the selected restore point, a message appears indicating the number of files that cannot be restored and lets you download the list of those files by selecting **Download list of impacted files**.

8. **Destination**: Select the down arrow next to Destination to see details.
   a. Choose where to restore the data: original source location or an alternate location that you can specify.

While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

   b. Select the system.

c. Select the Storage VM.

d. Optionally, enter the path.

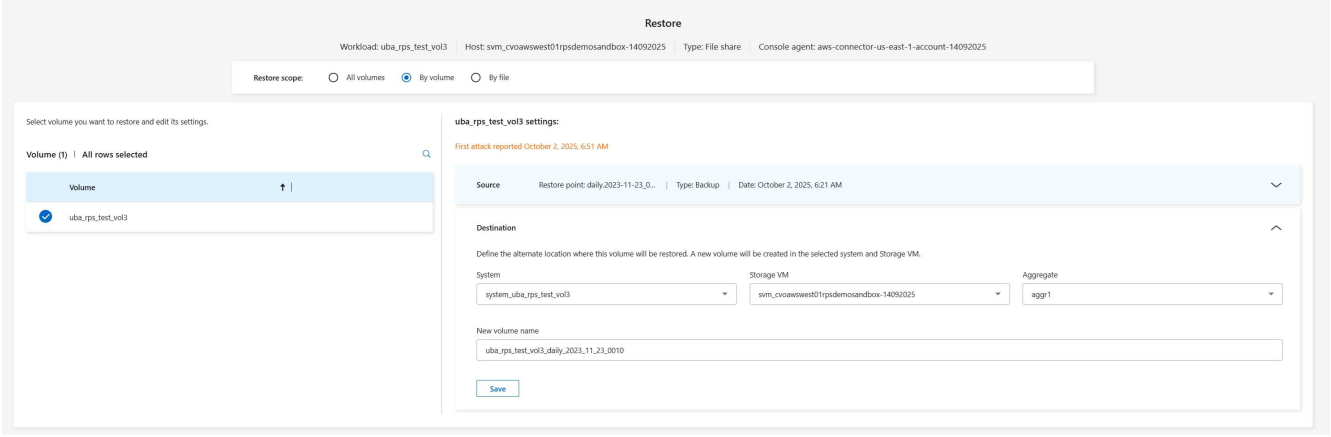
> If you don't specify a path for the restore, the files will be restored to a new volume at the top-level directory.

e. Select whether you want the names of the restored files or directory to be the same names as the current location or different names.

9. Select **Next**.
10. Review your selections.
11. Select **Restore**.
12. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a file share or datastore

1. After selecting a file share or datastore to restore, on the Restore page, in the Restore scope, select **By volume**.



2. On the list of volumes, select the volume you want to restore.
3. **Source**: Select the down arrow next to Source to see details.
   a. Select the restore point that you want to use to restore the data.

> Ransomware Resilience identifies the best restore point as the latest backup just before the incident and shows a "Recommended" indication.

4. **Destination**: Select the down arrow next to Destination to see details.
   a. Choose where to restore the data: original source location or an alternate location that you can specify.

> While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

   b. Select the system.
   c. Select the Storage VM.

d. Optionally, enter the path.

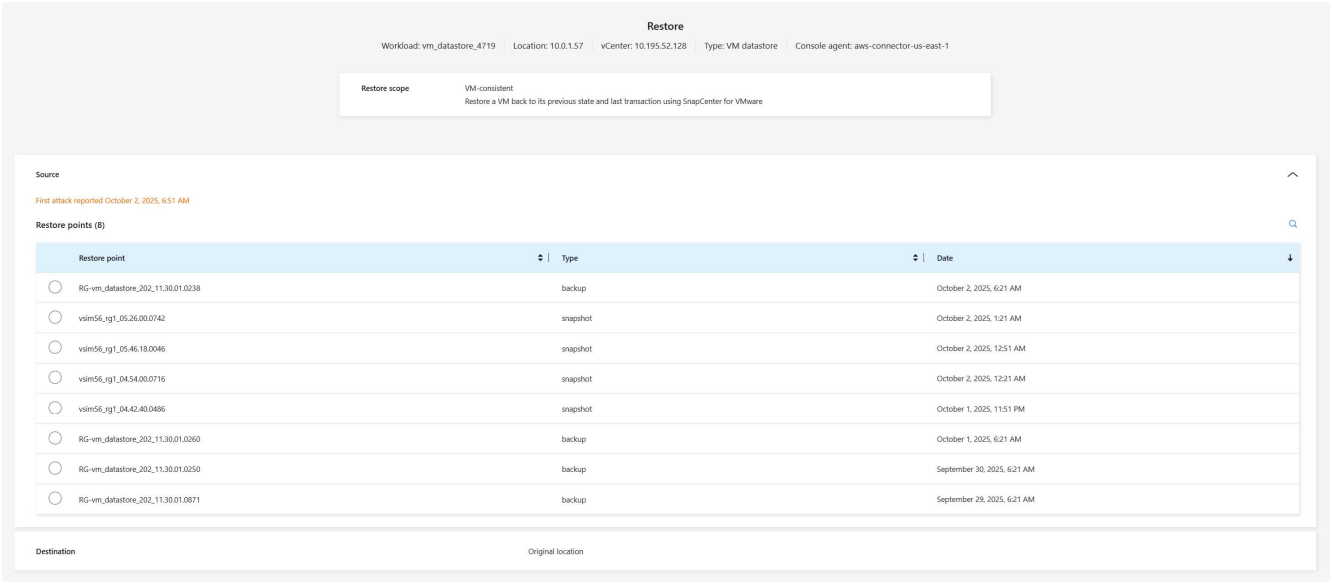
> If you don't specify a path for the restore, the files will be restored to a new volume at the top-level directory.

5. Select **Save**.
6. Review your selections.
7. Select **Restore**.
8. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a VM file share at the VM level

On the Recovery page after you selected a VM to restore, continue with these steps.

1. **Source**: Select the down arrow next to Source to see details.



2. Select the restore point that you want to use to restore the data.
3. **Destination**: To original location.
4. Select **Next**.
5. Review your selections.
6. Select **Restore**.
7. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Download reports in NetApp Ransomware Resilience

You can export protection data and download the CSV or JSON files that show details of attack readiness drills, protection, alerts, and recovery.

Before you download the files, refresh the dashboard to capture the most recent data in your reports.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

What data can you download?
You can download files from any of the main menu options:

- **Summary**: Includes lists of supported and unsupported workloads, recommended actions to improve your cyber resiliency posture, and information captured in the Ransomware Resilience dashboard.
- **Protection**: Includes the status and details of all workloads, including the total number protected and at risk.
- **Alerts**: Includes the status and details of all alerts, including the total number of alerts and automated snapshots.
- **Recovery**: Includes the status and details of all workloads that need to be restored, including the total number of workloads marked "Restore needed", "In progress," "Restore failed" and "Successfully restored."
- **Reports**: You can export data from any of the pages and download the files.

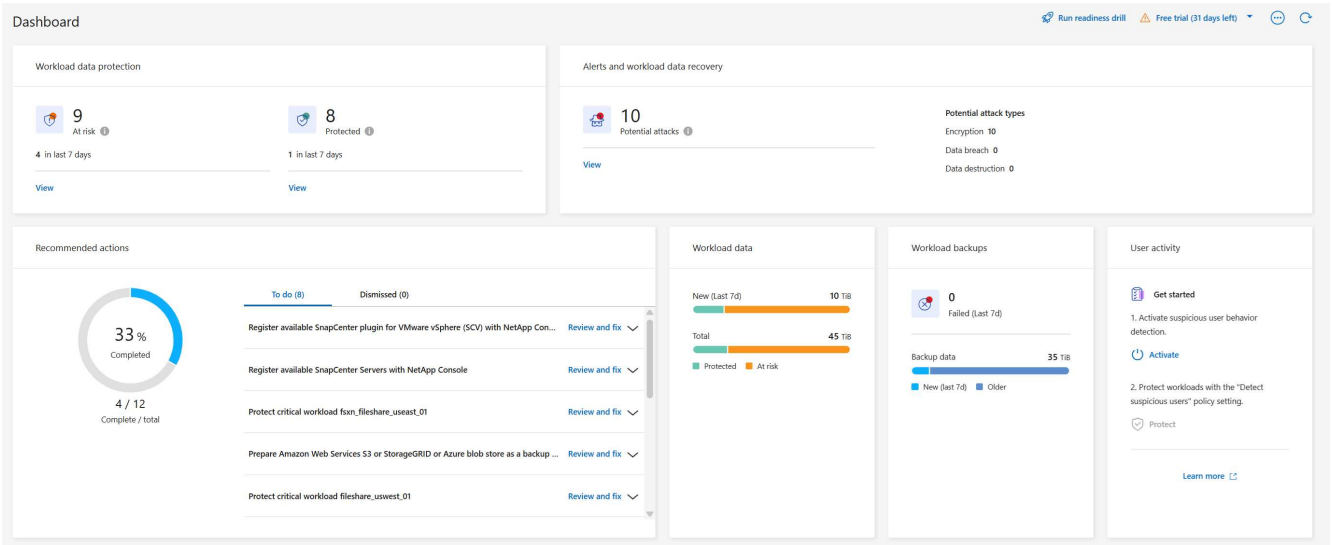
  You can download readiness drill reports only from the **Reports** page.

If you download CSV or JSON files from the Protection, Alerts, or Recovery page, the data shows only the data on that page.

The CSV or JSON files include data for all workloads on all Console systems.

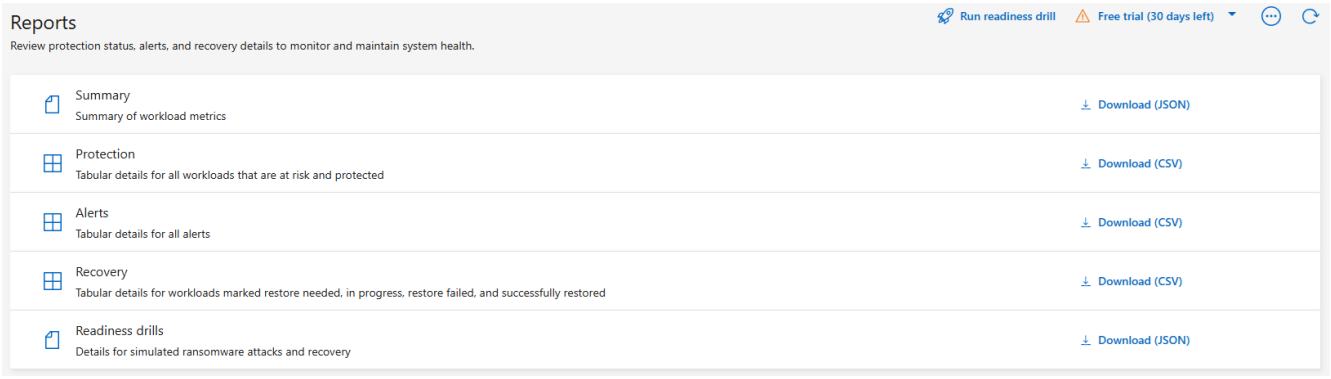
Steps

1. From the Console left navigation, select **Protection** > **Ransomware Resilience**.



2. From the Dashboard or other page, select the **Refresh** option in the upper right to refresh the data that will appear in the reports.

3. Do one of the following:
   - From the page, select the **Download** option.
   - From the NetApp Ransomware Resilience menu, select **Reports**.
4. If you selected the **Reports** option, select one of the preconfigured file names and select **Download**.



Copyright information

Trademark information