Protect workloads

NetApp Ransomware Resilience

NetApp
November 14, 2025

Table of Contents

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 both *detection* and *protection* policies.

- **Detection policies** detect 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.

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 and MySQL

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.

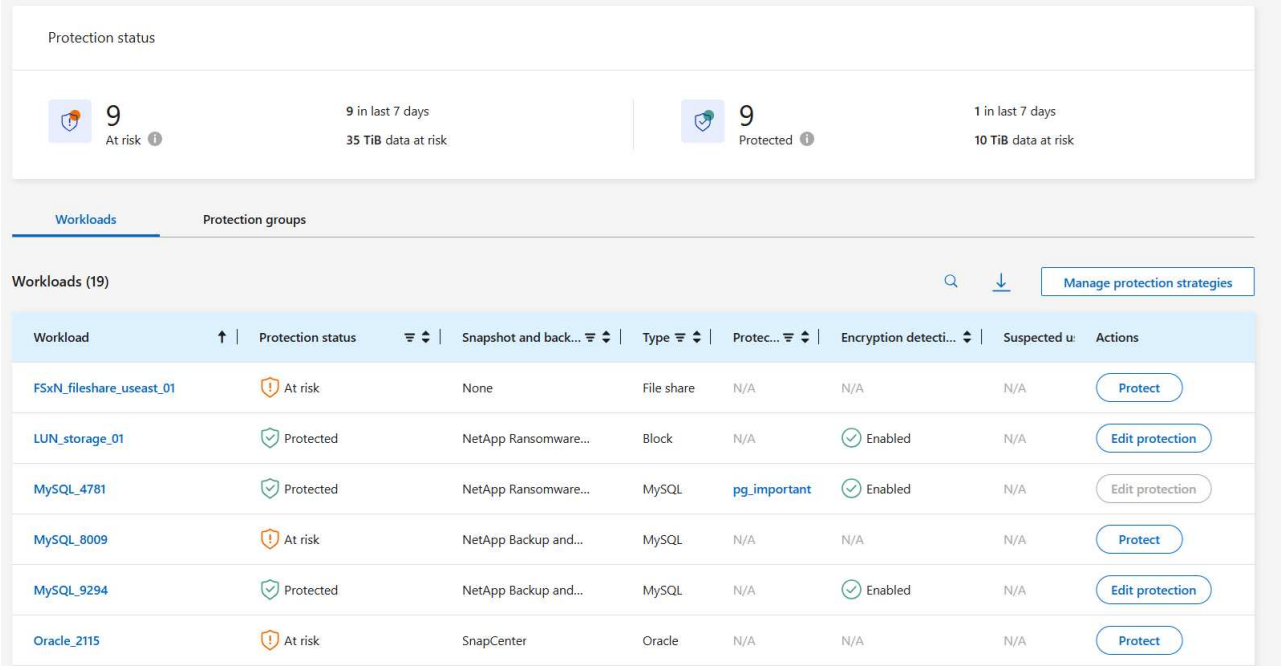
View ransomware protection on a workload

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 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.

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.

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**: Snapshot copies taken more than 1 per hour (highly aggressive protection schedule)
- **Important**: Snapshot copies taken less than 1 per hour but greater than 1 per day

- **Standard**: Snapshot copies taken more than 1 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.

Policy level	Snapshot	Frequency	Retention (Days)	# of snapshot copies	Total Max # 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

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.

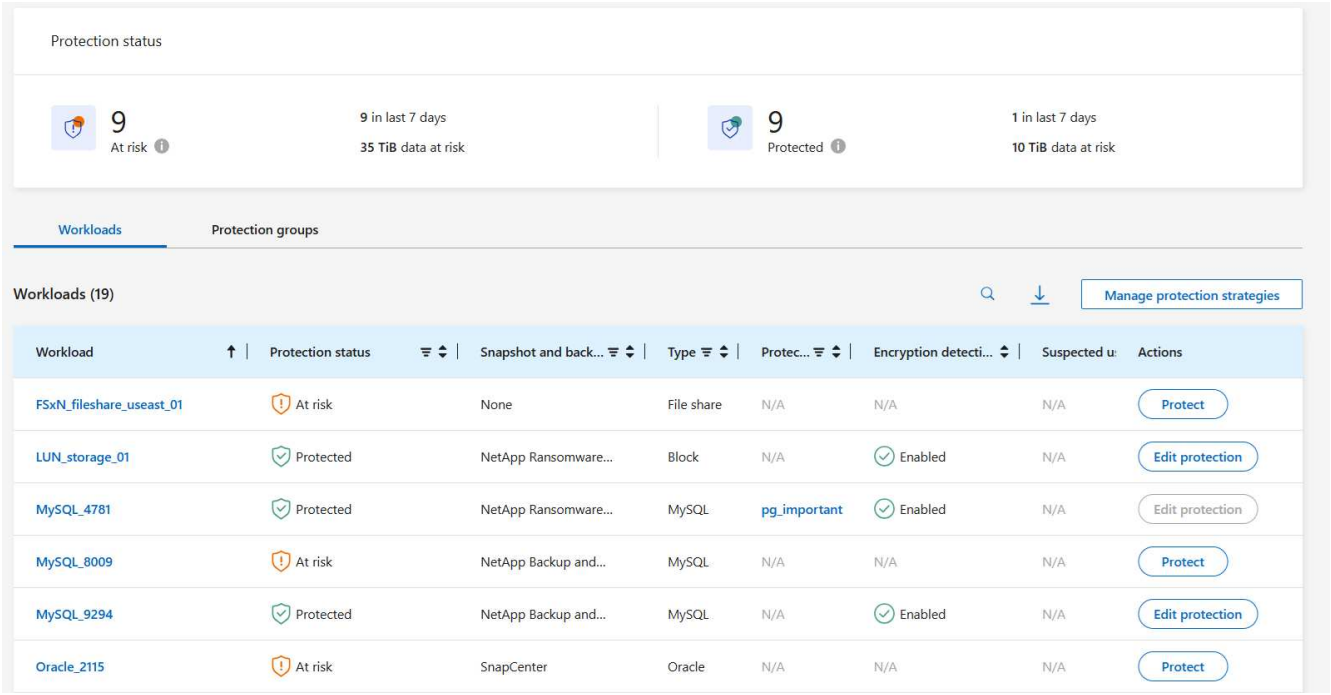
Create a ransomware protection strategy (if you have no snapshot or backup policies)

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:

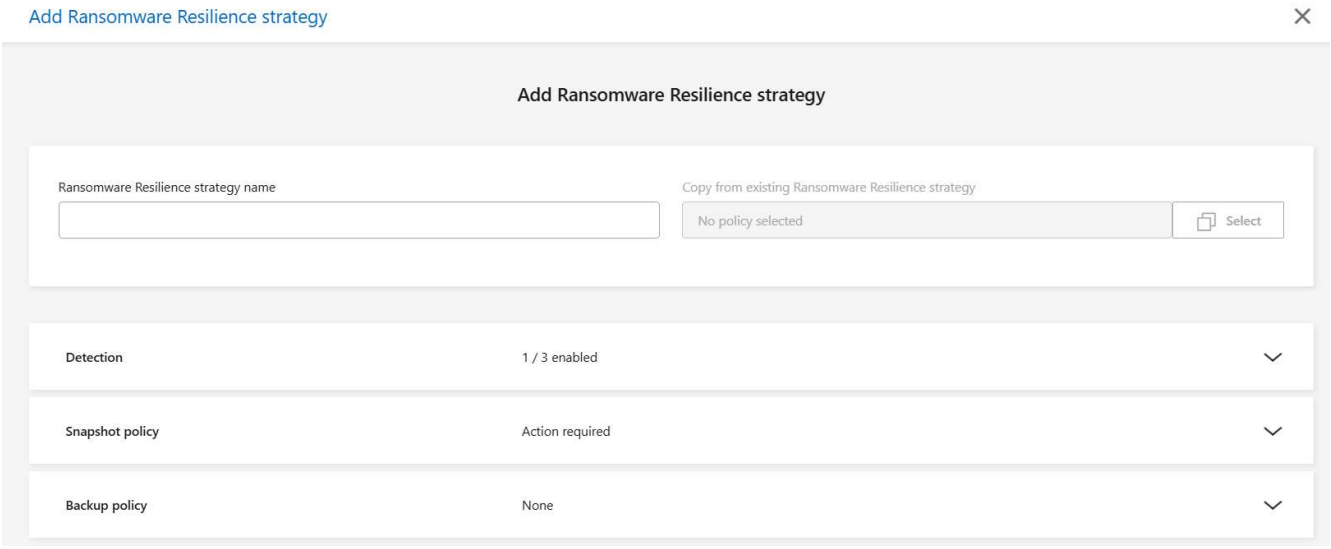
- Snapshot policy
- Backup policy
- Ransomware detection policy

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 detection to have Ransomware Resilience 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 this to have Ransomware Resilience 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.

- **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

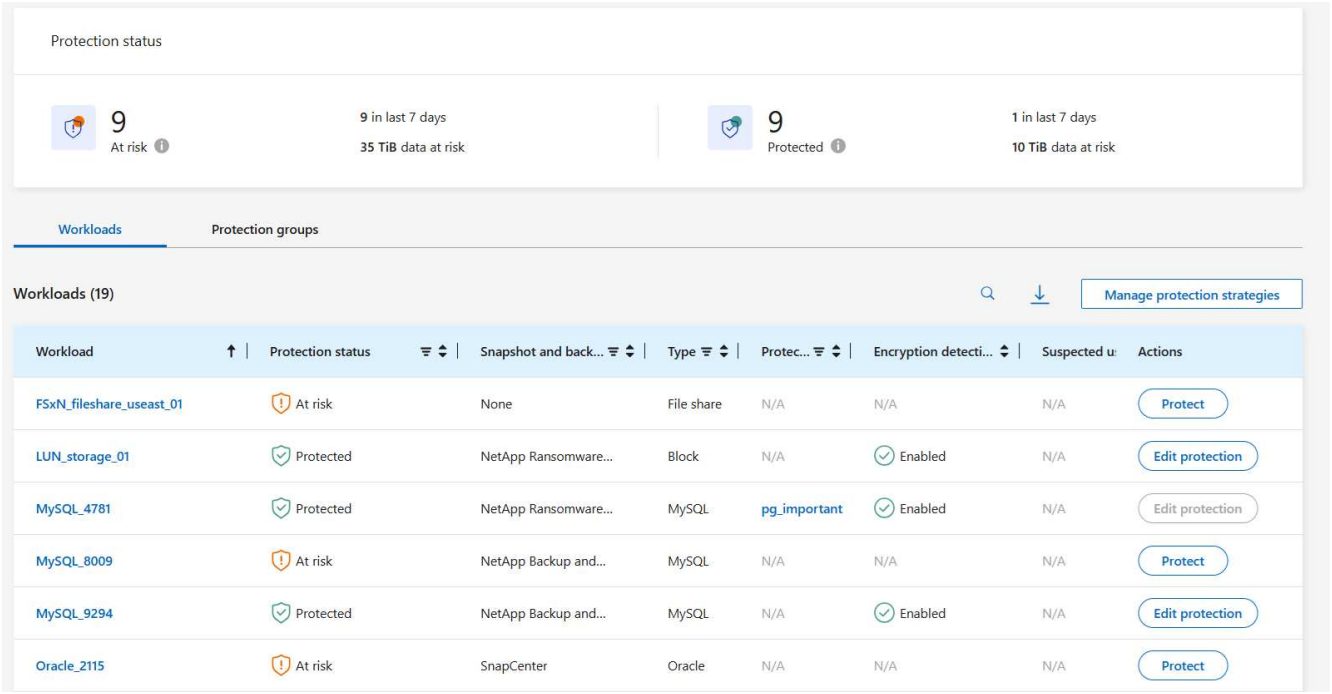
Ransomware Resilience enables you to assign either a detection policy or a protection policy to workloads with existing snapshot and backup protection managed in other NetApp products or services. Other services, such as Backup and Recovery and SnapCenter, use policies that govern snapshots, replication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

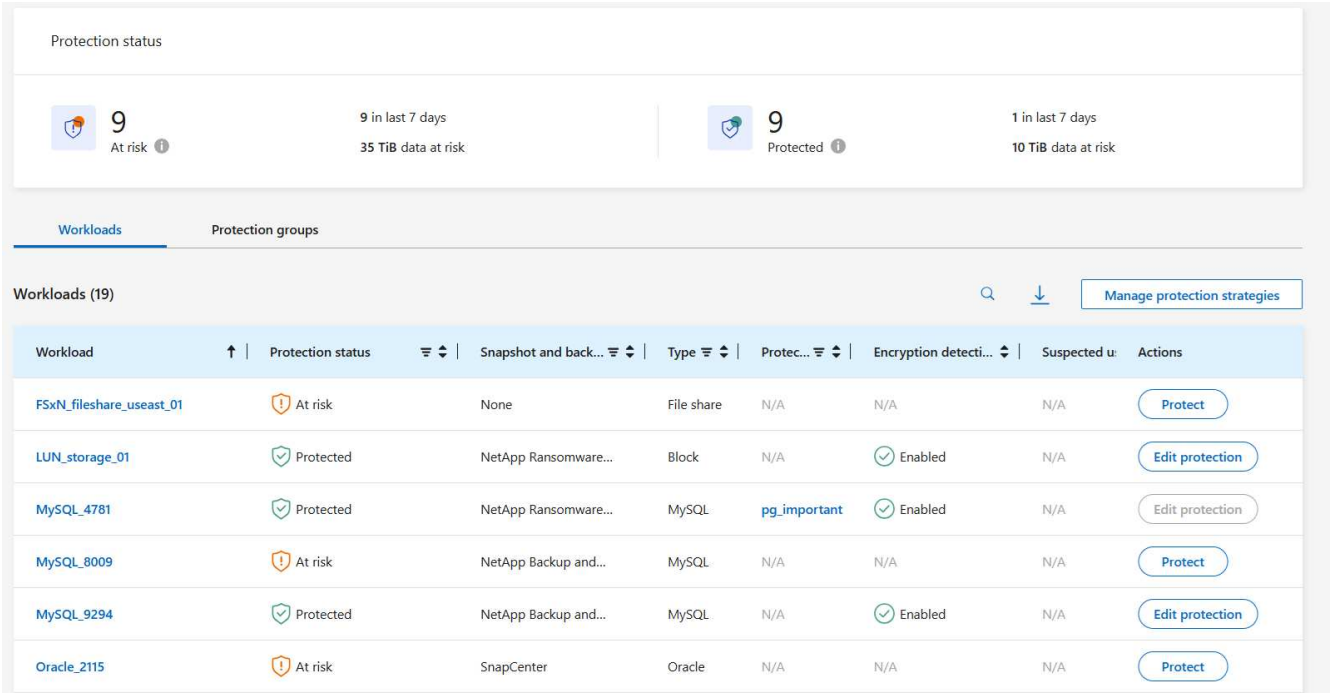
9. Select **Next**.
10. Review your choices. Select **Create** to activate detection.
11. On the Protection page, review the **Detection status** to confirm detection is Active.

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. 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.
6. Review the new protection strategy then select **Protect** to apply it.
7. 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.

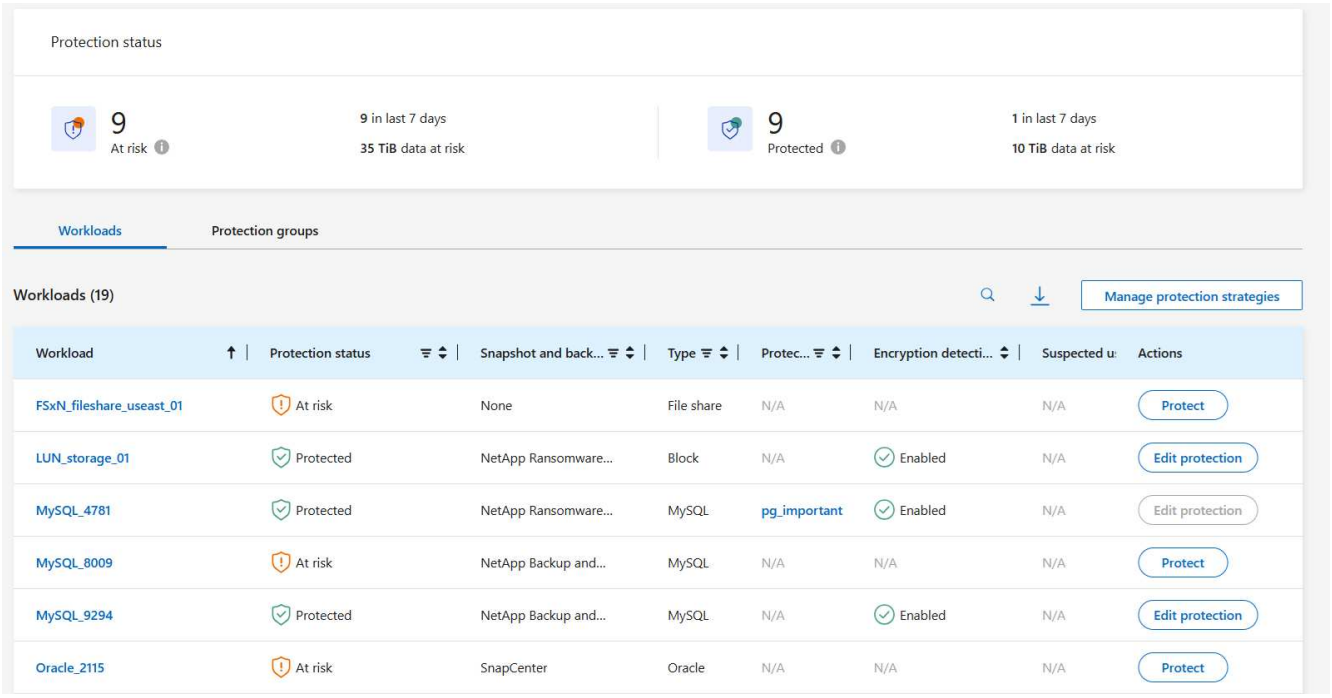
Create a protection group

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.

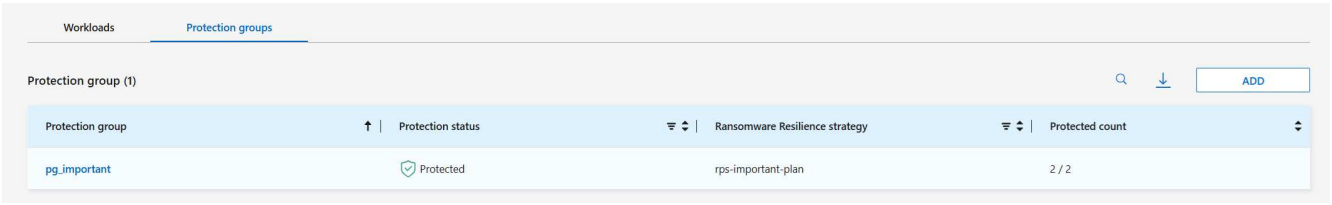
You can create groups regardless of their protection status (that is, groups not protected and groups that are protected). When you add a protection policy to a protection group, the new protection policy replaces any existing policy, including policies managed by SnapCenter and NetApp Backup and Recovery.

Steps

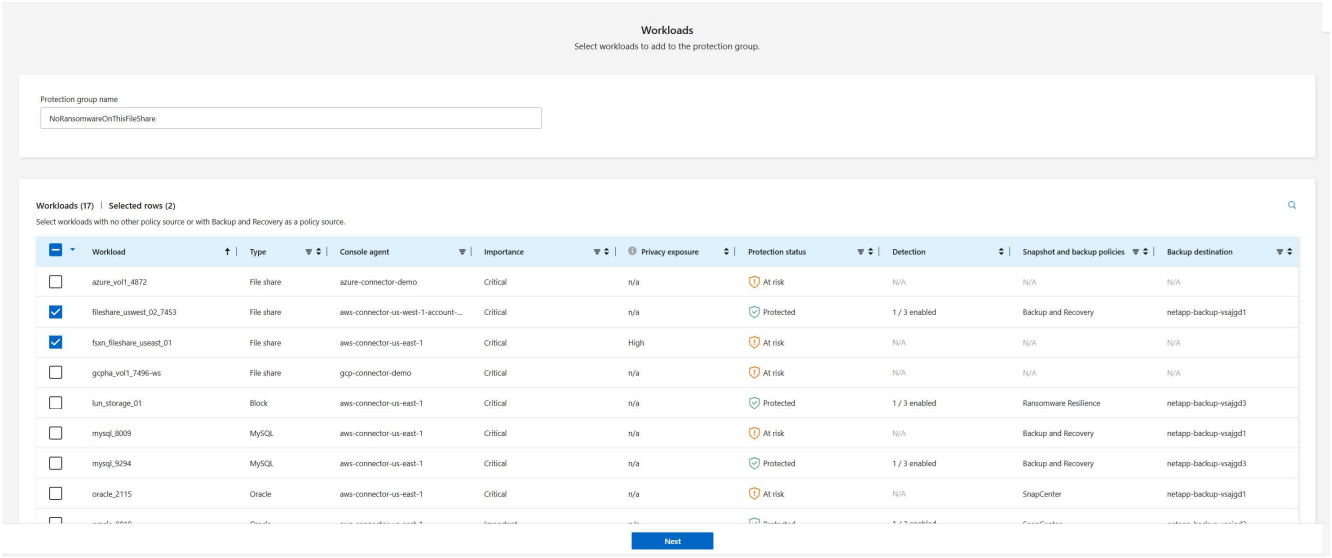
1. From the Ransomware Resilience menu, select **Protection**.



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



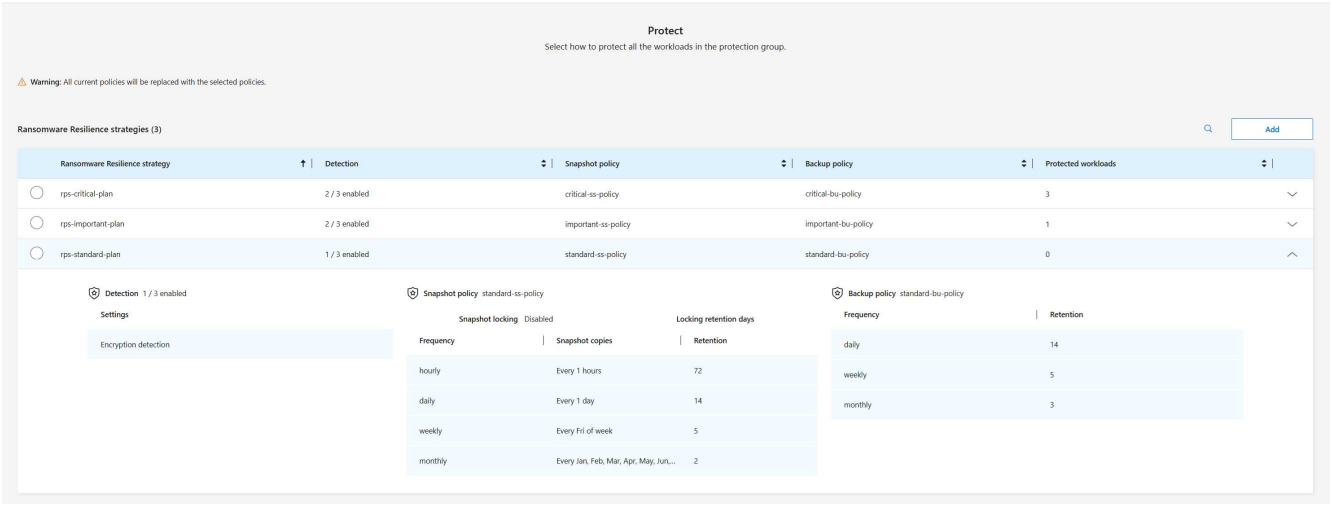
3. Select **Add**.



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**.
   a. If you need to configure a backup policy, choose one then select **Next**.
   b. If your detection policy includes user behavior detection, select the data collector you want to use then **Next**.
8. Review the selections for the protection group.
9. To finalize creation of the protection group, select **Add**.

Edit group protection

You can change the detection policy on an existing group.

Steps

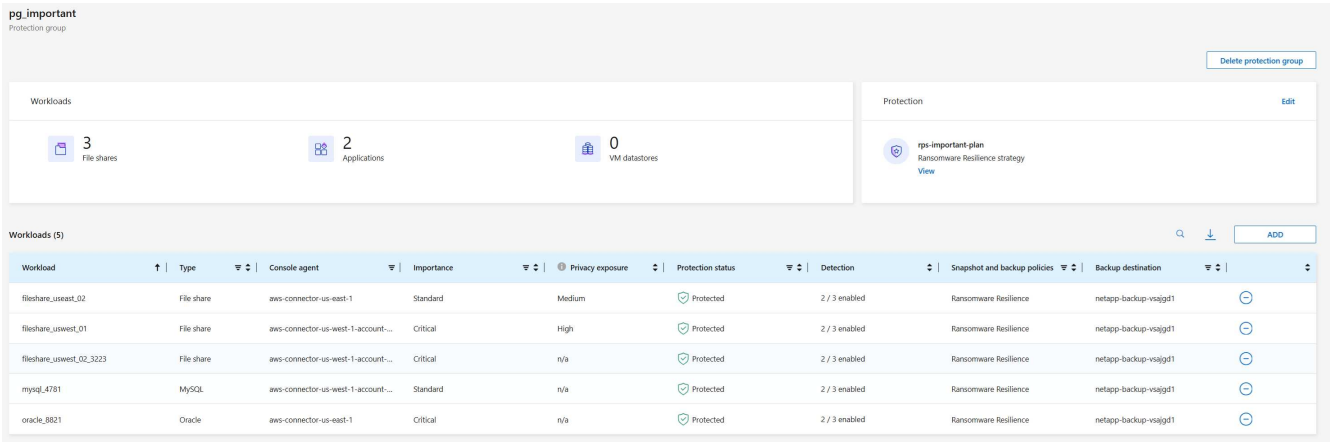
1. From the Ransomware Resilience menu, select **Protection**.
2. From the Protection page, select the **Protection groups** tab then select the group whose policy you want to modify.
3. From protection group's overview page, select **Edit protection**.
4. Select an existing protection policy to apply 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.



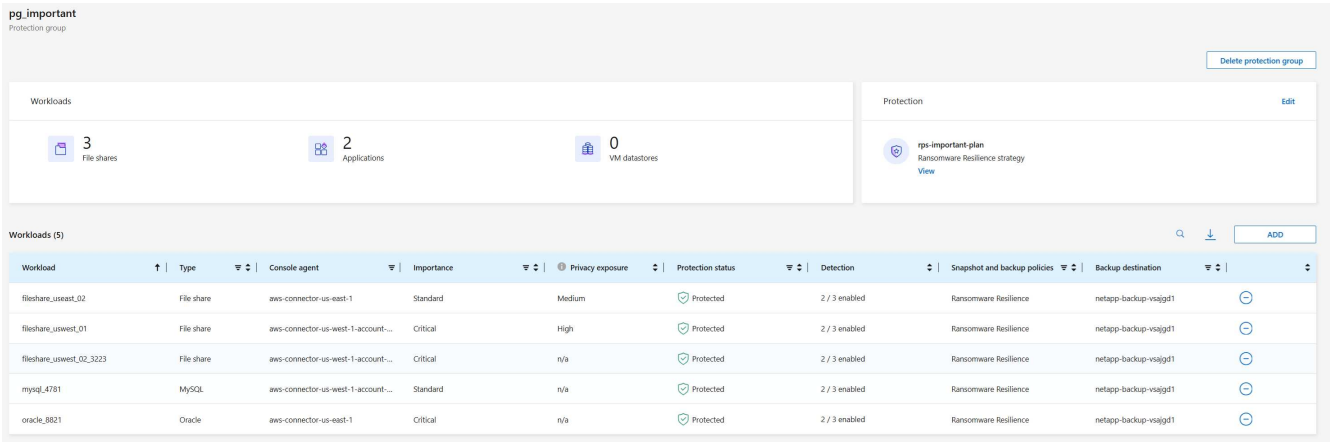
4. From the selected protection group page, select the workload you want to remove from the group and select the **Actions** ••• option.
5. From the Actions menu, select **Remove workload**.
6. Confirm that you want to remove the workload and select **Remove**.

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

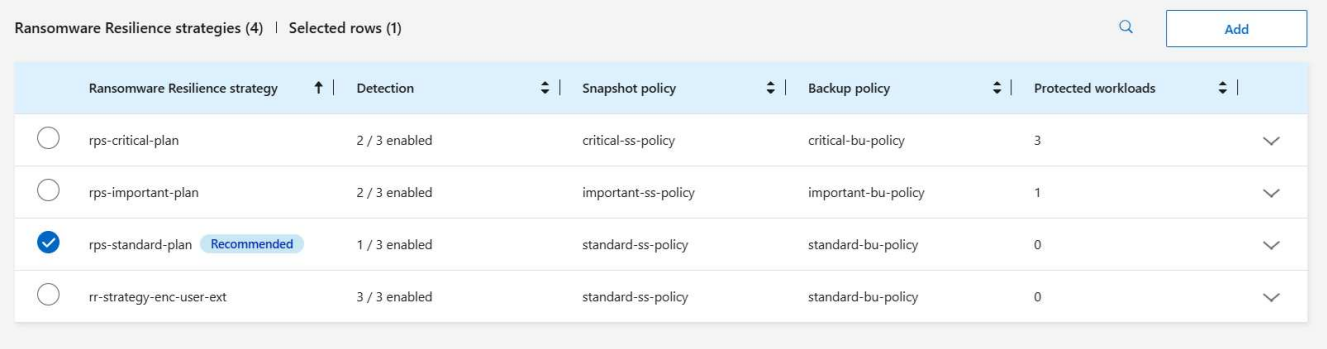
Before you delete a ransomware protection strategy, you might want to view which workloads are protected by that strategy.

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:

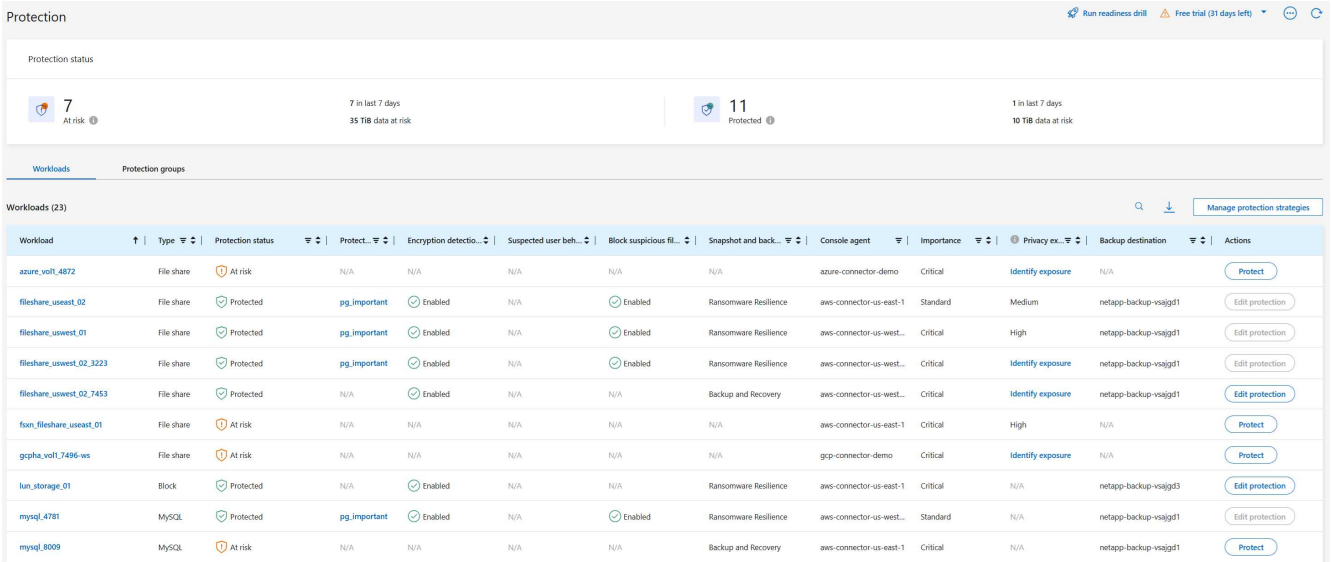
- Learn about Data Classification
- Categories of private data
- Investigate the data stored in your organization

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

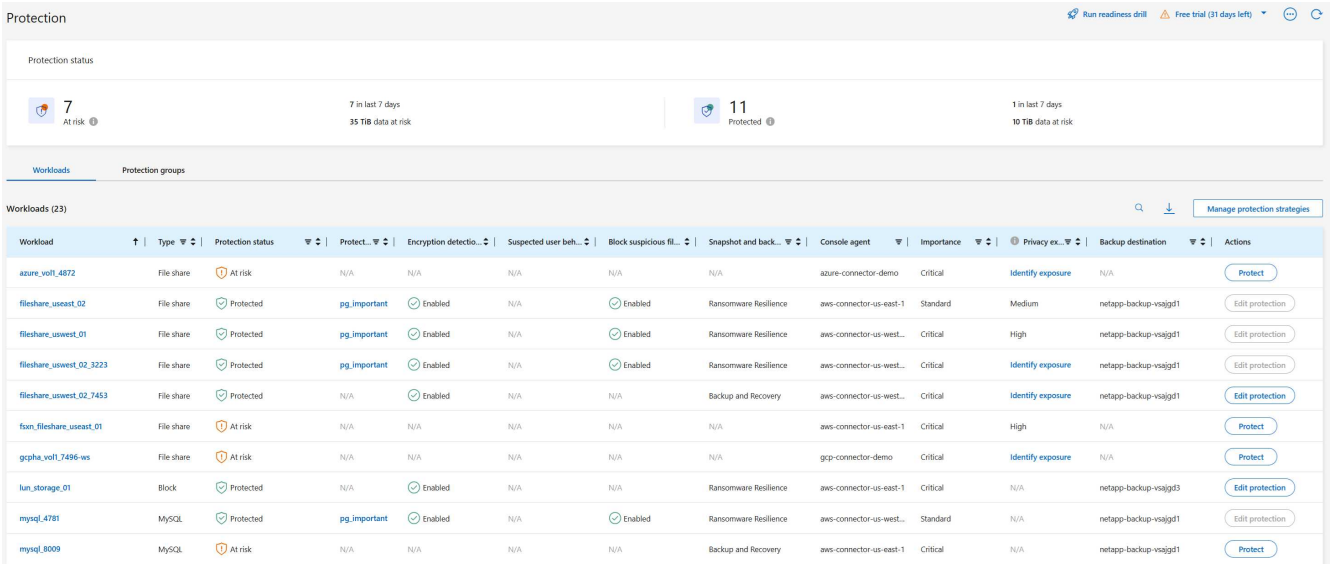
After Data Classification scans for PII, assess the risk.

PII data is classified into one of three designations:

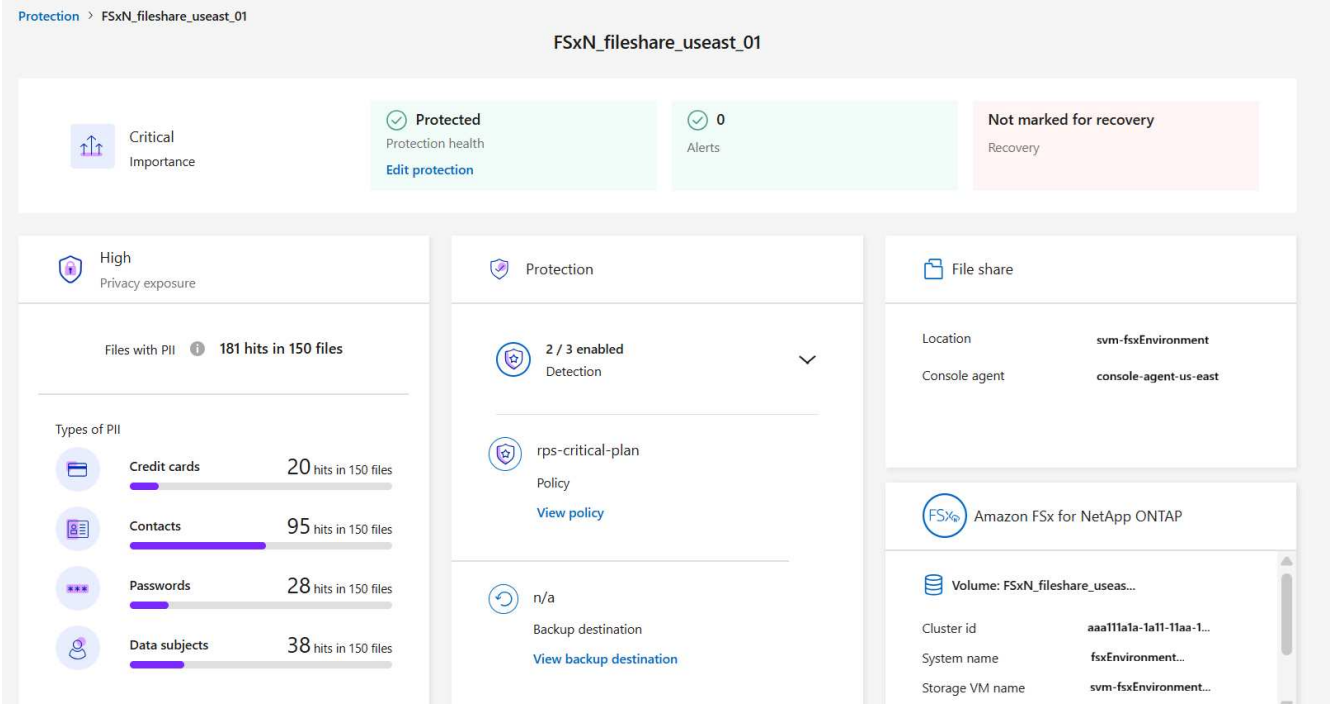
- **High**: Greater than 70% of files contain PII
- **Medium**: Greater than 30% and less than 70% of files contain PII
- **Low**: Greater than 0% and less than 30% of files contain PII

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

Copyright information

Trademark information