Protect workloads

BlueXP ransomware protection

NetApp
December 20, 2024

Table of Contents

Protect workloads

Protect workloads with ransomware strategies

You can protect workloads against ransomware attacks by completing the following actions using BlueXP ransomware protection.

- Enable workload-consistent protection, which works with SnapCenter Software or SnapCenter Plug-in for VMware vSphere.
- Create or manage ransomware protection strategies, which include policies that you create for snapshots, backups, and ransomware protection (known as *detection policies*).
- Import a strategy and adjust it.
- Group file shares to make it easier for you to protect workloads rather than protect them individually.
- Delete a ransomware protection strategy.

Which services are used in protection?
The following services can be used to manage protection policies. Protection information from these services appears in BlueXP ransomware protection:

- BlueXP backup and recovery for file shares, VM file shares
- SnapCenter for VMware for VM datastores
- SnapCenter for Oracle and MySQL

Protection policies

You might find it helpful to review information about the protection policies you can change and what types of policies are in a protection strategy.

Which protection policies can you change?

You can change protection policies based on the workload protection you have:

- **Workloads not protected by NetApp applications**: These workloads are not managed by SnapCenter, SnapCenter Plug-in for VMware vSphere, or BlueXP backup and recovery. These workloads might 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.
- **Workloads with existing protection by NetApp applications**: These workloads have backup or snapshot policies managed by SnapCenter, SnapCenter for VMWare vSphere, or BlueXP backup and recovery.
  - If snapshot or backup policies are being managed by SnapCenter, SnapCenter for VMWare, or BlueXP backup and recovery, they will continue to be managed by these applications. Using BlueXP ransomware protection, you can also apply a ransomware detection policy to those workloads.
  - If a ransomware detection policy is being managed by Autonomous Ransomware Protection (ARP) and FPolicy in ONTAP, those workloads are protected and will continue to be managed by ARP and FPolicy.

Which policies are required in a ransomware protection strategy?

The following policies are required in ransomware protection strategy:

- Ransomware detection policy
- Snapshot policy

A backup policy is not required in the BlueXP ransomware protection strategy.

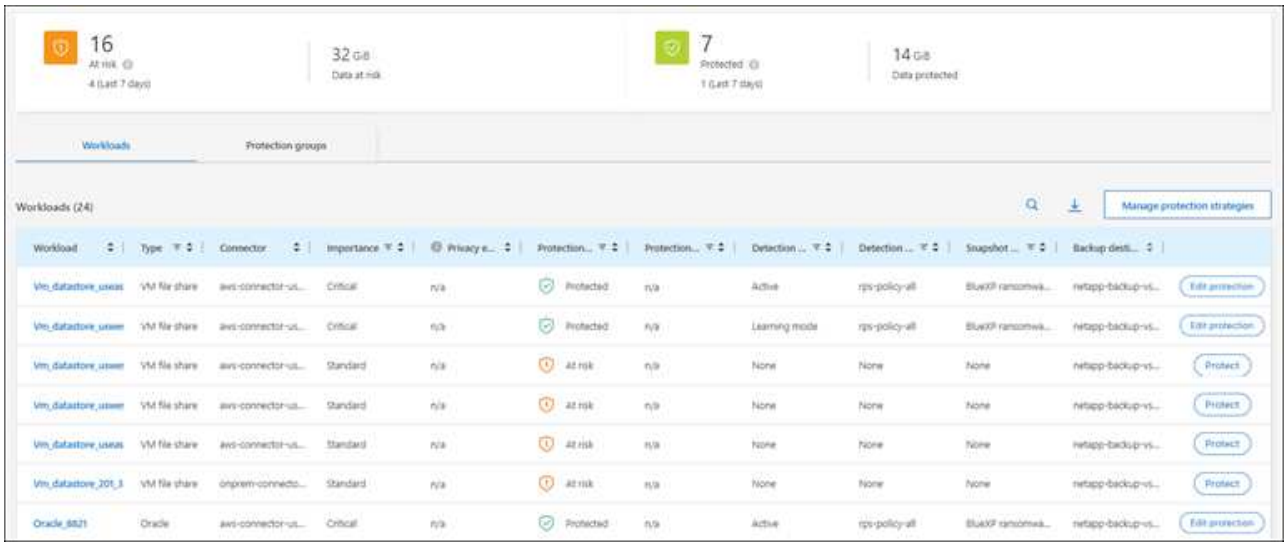
View ransomware protection on a workload

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
- VM workloads
- File share workloads

Steps

1. From the BlueXP left navigation, select **Protection** > **Ransomware protection**.
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.

> For workloads that already have a protection policy with SnapCenter or BlueXP backup and recovery service, you cannot edit the protection. For these workloads, BlueXP ransomware enables Autonomous Ransomware Protection and/or FPolicy protection if they are already activated in other services. Learn more about Autonomous Ransomware Protection, BlueXP backup and recovery, and ONTAP FPolicy.

Protection details on 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 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 the service 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 the service has encountered an error.

When protection is enabled in BlueXP ransomware protection, 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 BlueXP backup and recovery
- Name of ransomware protection policy that governs snapshots and backups
- None

Workload importance

BlueXP ransomware protection 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 BlueXP ransomware protection predefined policies, which are aligned with workload importance:

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

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 BlueXP backup and recovery.

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

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

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

Steps

1. From the BlueXP ransomware protection menu, select **Dashboard**.
2. From the Recommendations pane, locate one of the following recommendations and select **Review and fix**:
    - Register available SnapCenter Server with BlueXP
    - Register available SnapCenter Plug-in for VMware vSphere (SCV) with BlueXP
3. Follow the information to register the SnapCenter or SnapCenter Plug-in for VMware vSphere host using BlueXP backup and recovery.
4. Return to BlueXP ransomware protection.
5. From BlueXP ransomware protection, go the Dashboard and initiate the discover process again.
6. From BlueXP ransomware protection, 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

You can add a ransomware protection strategy to workloads. The way you do this depends on whether snapshot and backup policies exist already:

- **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 BlueXP ransomware protection:
    - Snapshot policy
    - Backup policy
    - Ransomware detection policy
- **Create a detection policy to workloads that already have snapshot and backup policies**, which are managed in other NetApp products or services. The detection policy will not change the policies managed in other products.

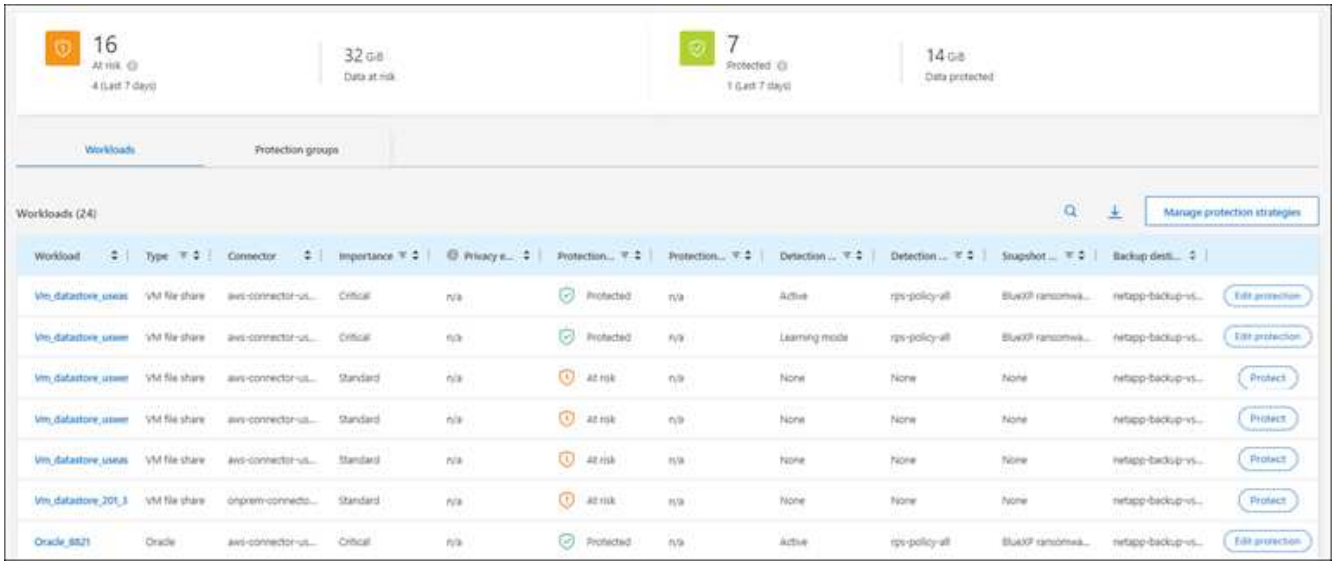
Create a ransomware protection strategy (if you have no snapshot or backup policies)

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 BlueXP ransomware protection:

- Snapshot policy
- Backup policy
- Ransomware detection policy

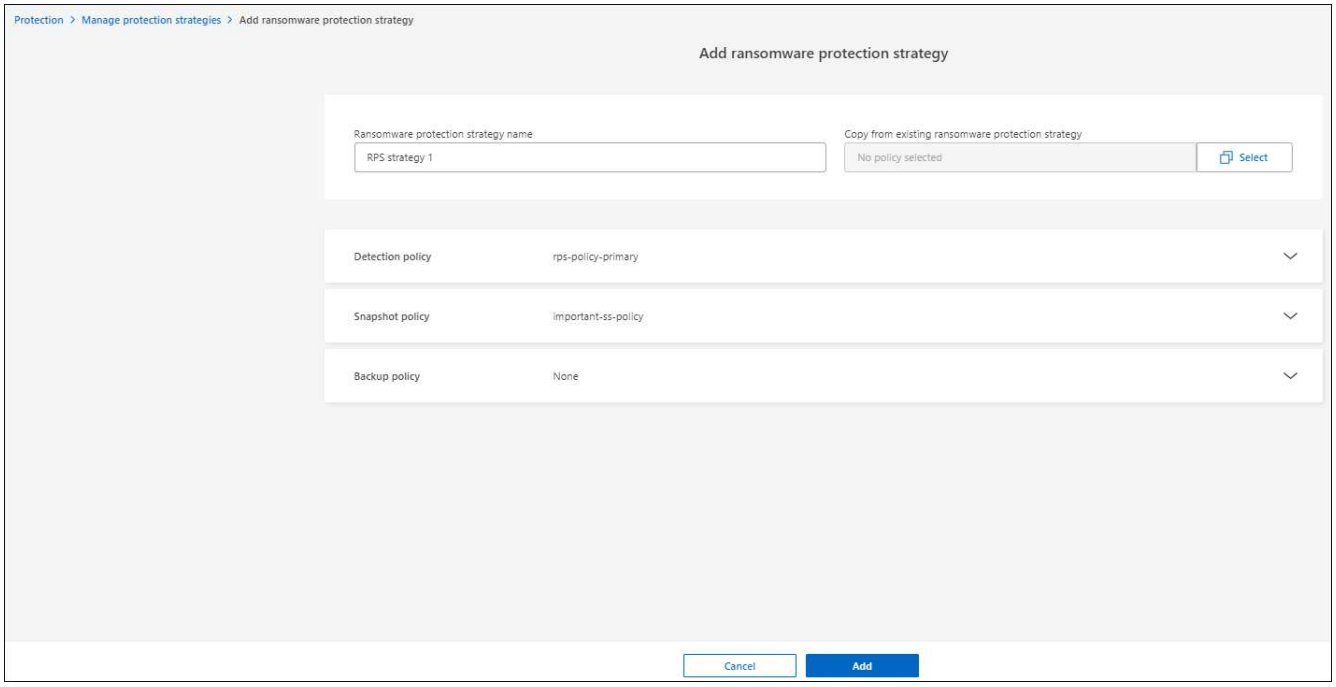
Steps to create a ransomware protection strategy

1. From the BlueXP ransomware protection menu, select **Protection**.



2. From the Protection page, select **Manage protection strategies**.

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, the service 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 the service detect potential ransomware attacks.
     - **Block file extensions**: Enable this to have the service block known suspicious file extensions. The service 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 ame**: 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 that already have snapshot and backup policies

With BlueXP ransomware protection, you can assign a ransomware detection policy to workloads that already have snapshot and backup policies, which are managed in other NetApp products or services. The detection policy will not change the policies managed in other products.

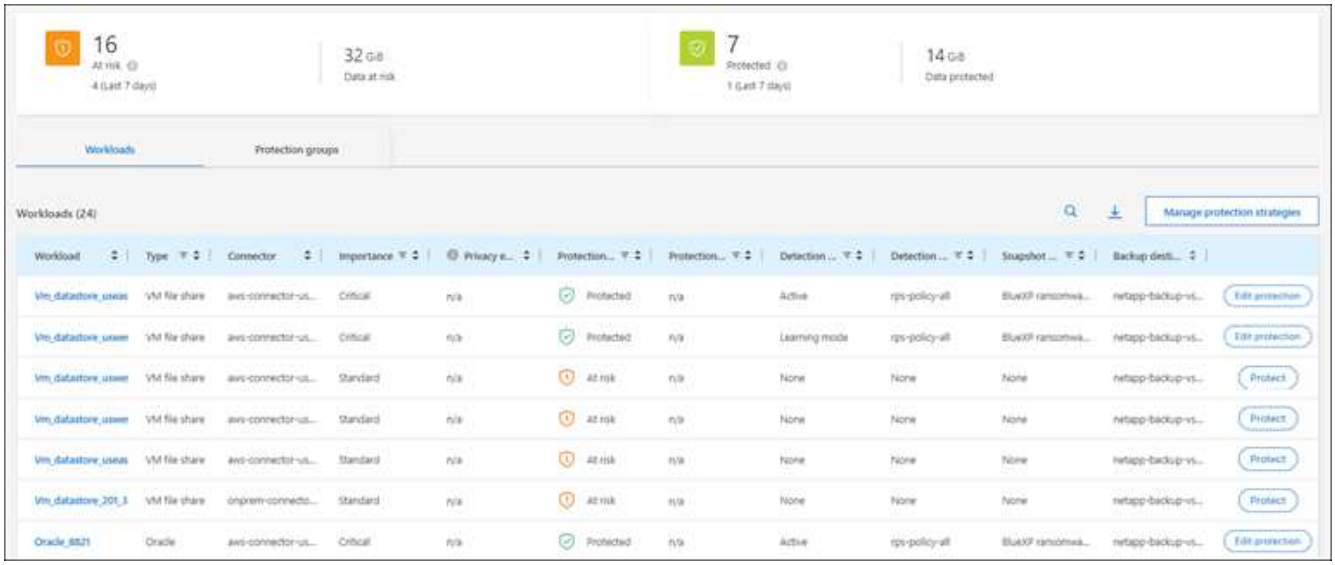
Other services, such as BlueXP backup and recovery and SnapCenter, use the following types of policies to govern workloads:

- Policies governing snapshots
- Policies governing replication to secondary storage

- Policies governing backups to object storage

Steps

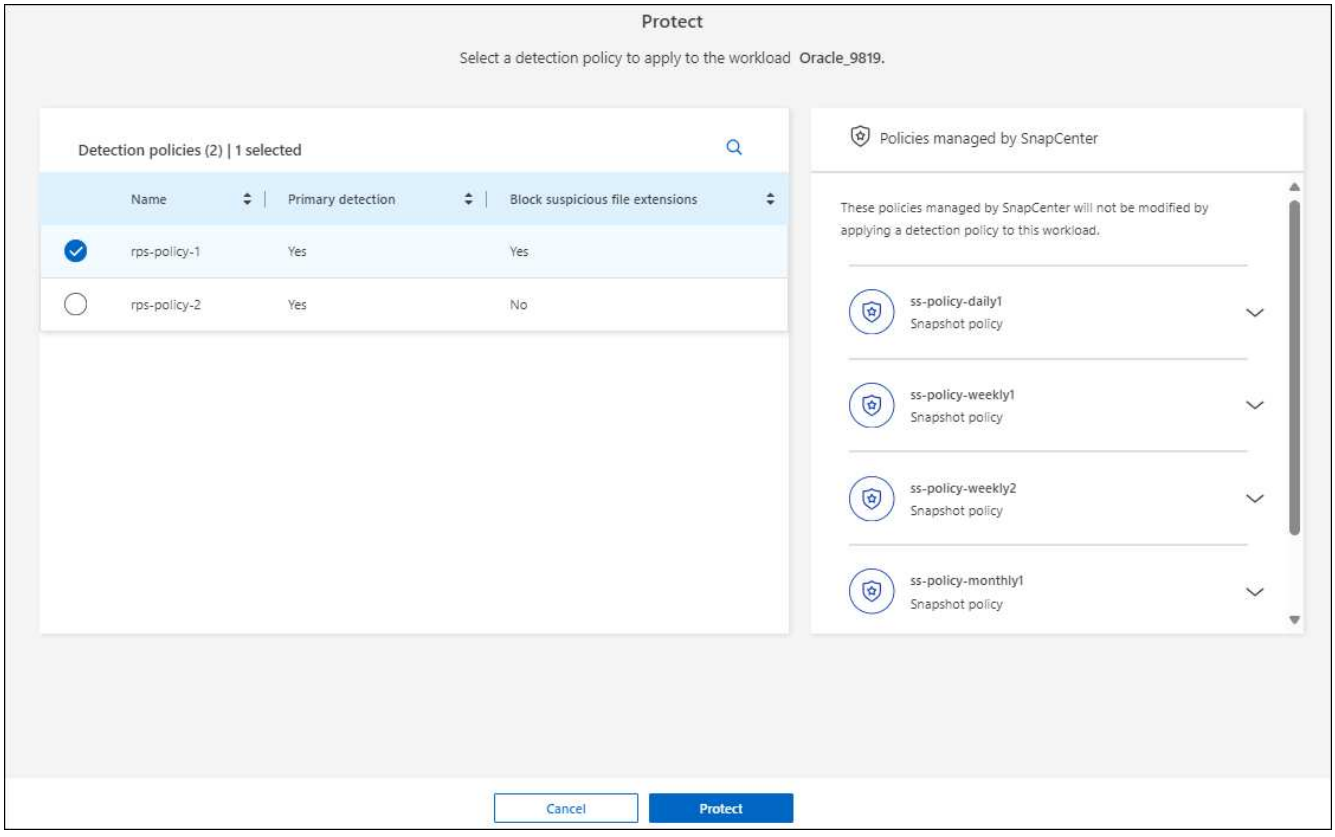
1. From the BlueXP ransomware protection menu, select **Protection**.



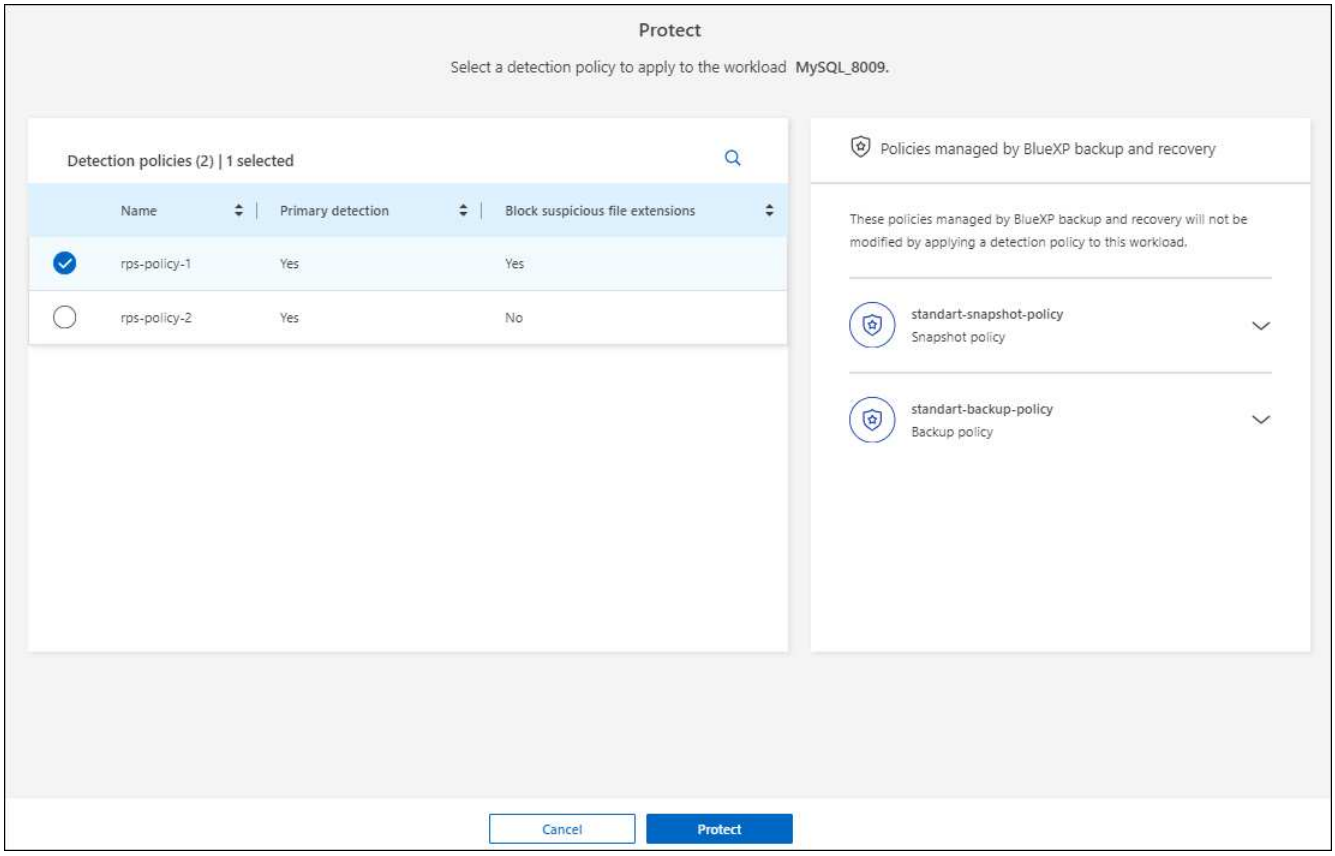
2. From the Protection page, select a workload, and select **Protect**.

   The Protect page shows the policies managed by SnapCenter Software, SnapCenter for VMware vSphere, and BlueXP backup and recovery.

   The following example shows policies managed by SnapCenter:



The following example shows policies managed by BlueXP backup and recovery:



3. To see details of the policies managed elsewhere, click the **Down arrow**.
4. To apply a detection policy in addition to the snapshot and backup policies managed elsewhere, select the Detection policy.
5. Select **Protect**.
6. On the Protection page, review the Detection policy column to see the Detection policy assigned. Also, the snapshot and backup policies column shows the name of the product or service managing the policies.

Assign a different policy

You can assign a different protection policy replacing the current one.

Steps

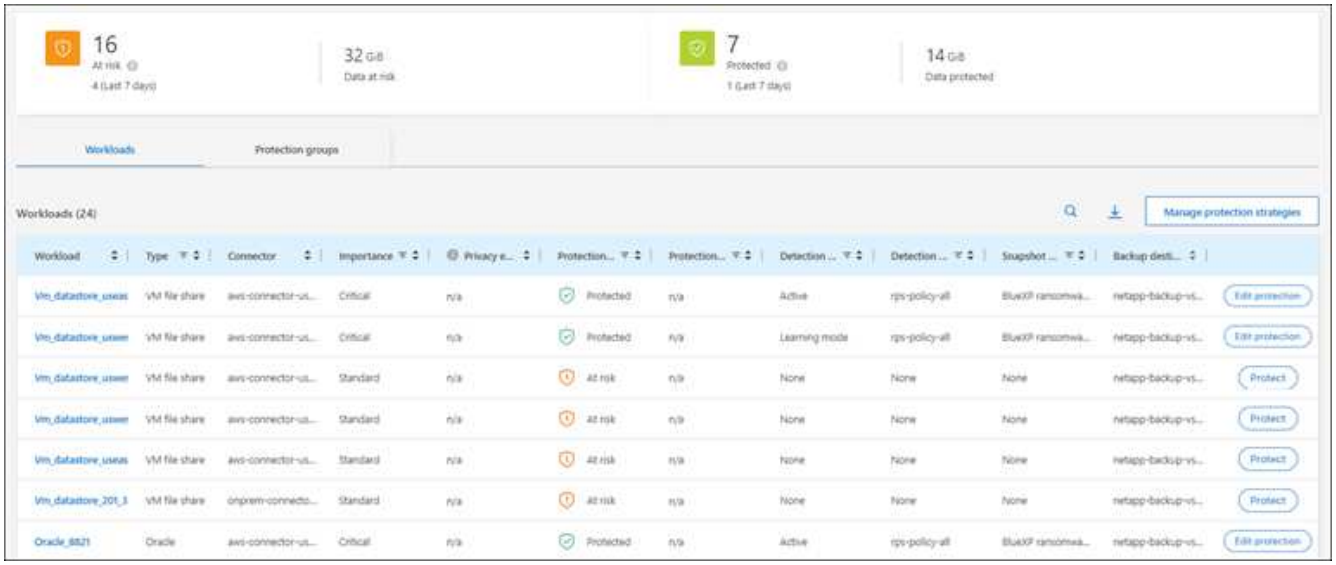
1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protection page, on the workload row, select **Edit protection**.
3. In the Policies page, click the down arrow for the policy you want to assign to review the details.
4. Select the policy you want to assign.
5. Select **Protect** to finish the change.

Group file shares for easier protection

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

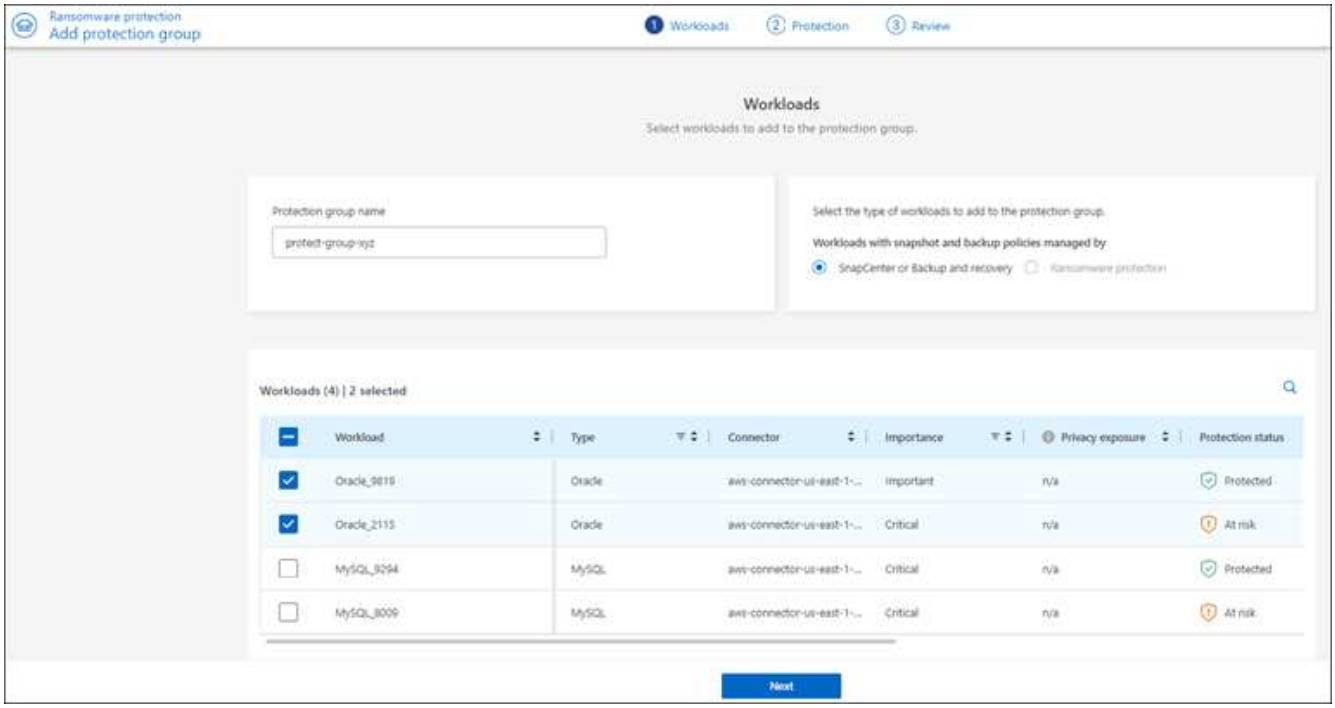
Steps

1. From the BlueXP ransomware protection menu, select **Protection**.



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

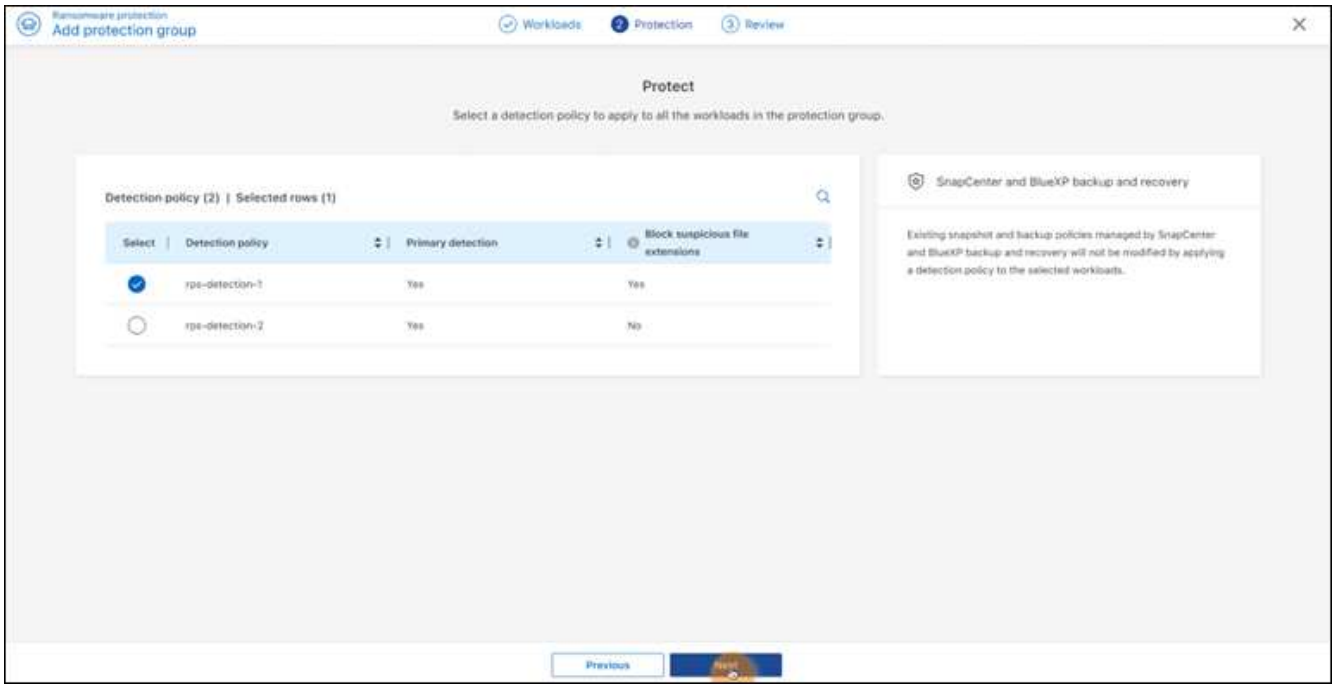
3. Select **Add**.



4. Enter a name for the protection group.
5. Complete one of the following steps:
   a. If you already have protection policies in place, select whether you want to group workloads based on whether they are managed by one of these:
      - BlueXP ransomware protection
      - SnapCenter or BlueXP backup and recovery
   b. If you don't have protection policies already in place, the page displays the preconfigured ransomware protection strategies.
      i. Choose one to protect your group and select **Next**.
      ii. If the workload you chose has volumes on multiple working environments, select the backup destination for the multiple working environments so that they can be backed up to the cloud.
6. Select the workloads to add to the group.

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

7. Select **Next**.



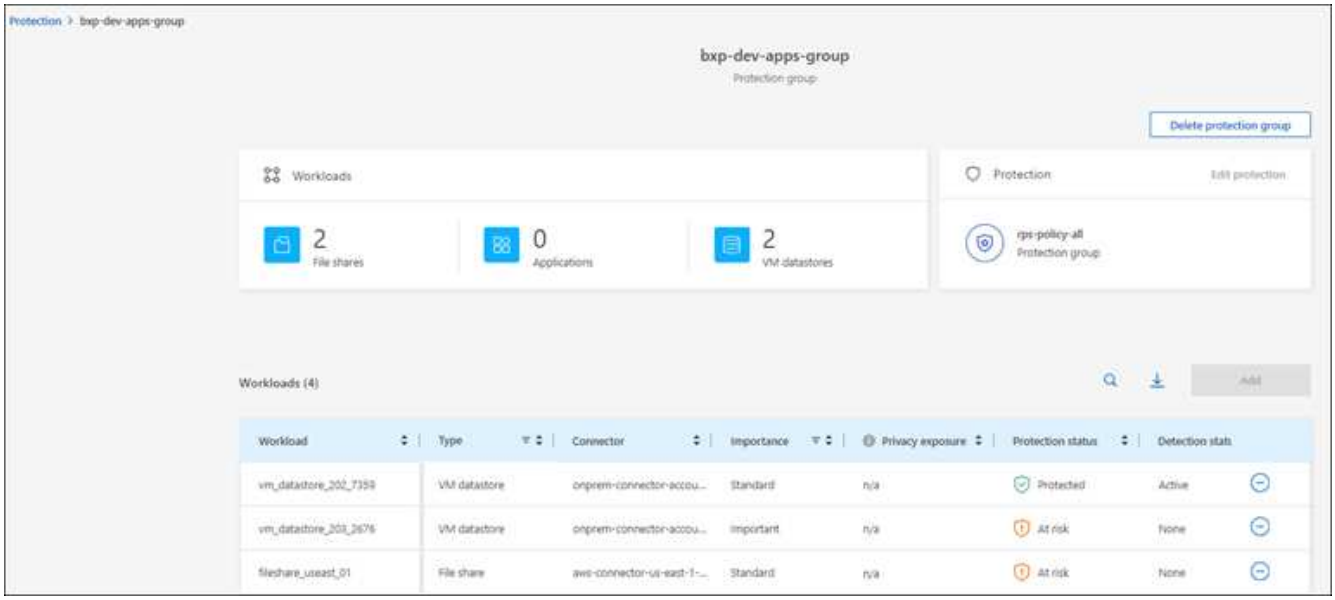
8. Select the policy that will govern the protection for this group.
9. Select **Next**.
10. Review the selections for the protection group.
11. Select **Add**.

Remove workloads from a group

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

Steps

1. From the BlueXP ransomware protection 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.



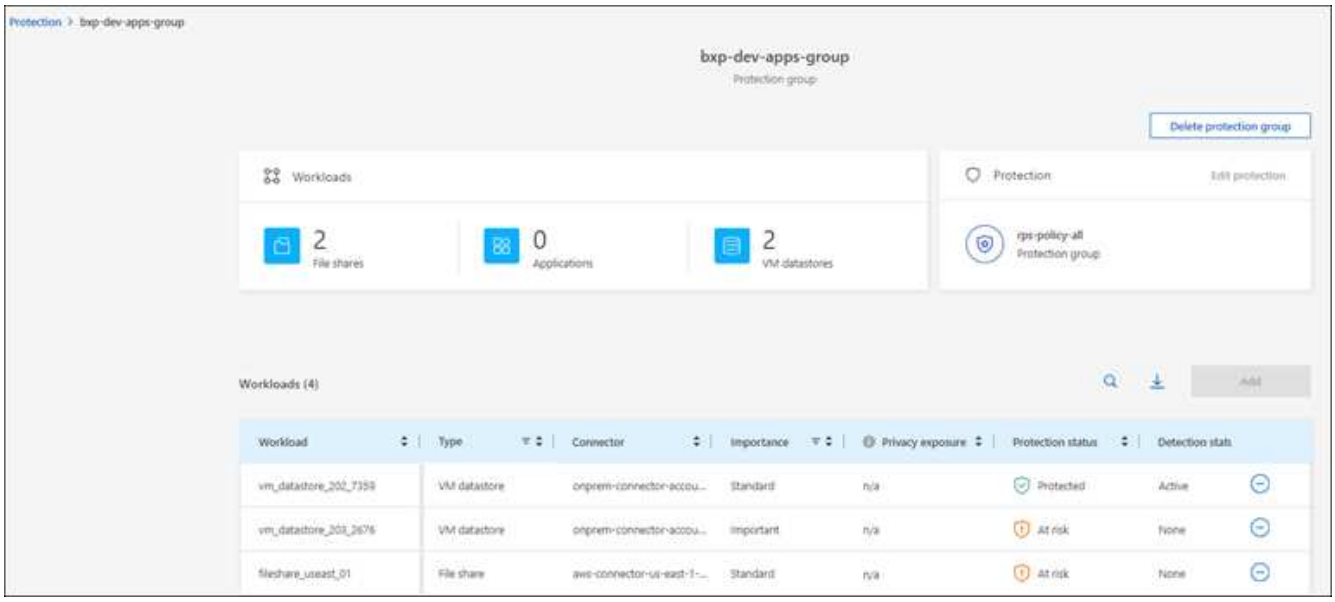
4. From the selected protection group page, select the workload you want to remove from the group and select the **Actions** ••• option.
5. From the Actions menu, select **Remove workload**.
6. Confirm that you want to remove the workload and select **Remove**.

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 BlueXP ransomware protection 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 when viewing the list of strategies

1. From the BlueXP ransomware protection 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, click 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 BlueXP ransomware protection 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 BlueXP classification

Within the BlueXP ransomware protection service, you can use BlueXP classification, a core component of the BlueXP family, to scan and classify your data on a file share workload. Classifying data helps you identify whether your data includes personally identifiable information (PII), which can increase security risks.

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

Enable BlueXP classification

Before you use BlueXP classification within the BlueXP ransomware protection service, you need to enable BlueXP classification to scan your data.

By using the BlueXP classification UI as an alternate method, an administrator can enable BlueXP classification in BlueXP ransomware protection.

It might be helpful to review these BlueXP classification resources before you begin to use the service:

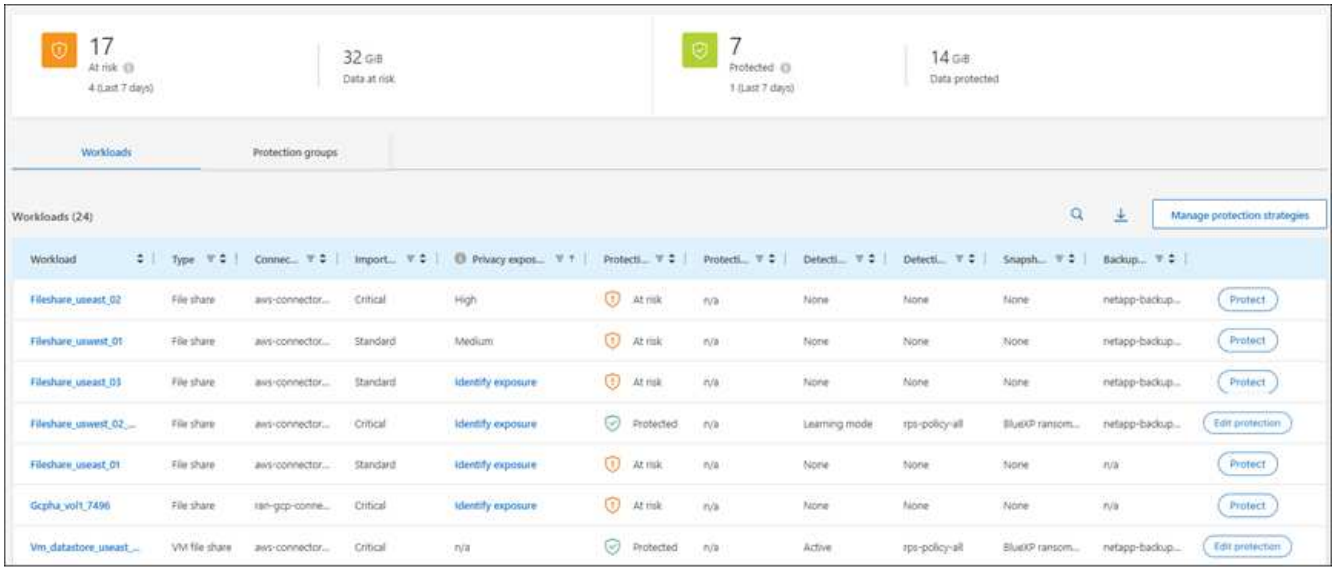
- Learn about BlueXP classification
- Categories of private data
- Investigate the data stored in your organization

Before you begin

Scanning for PII data in BlueXP ransomware protection is available to customers who deployed BlueXP classification. BlueXP classification is available as part of the BlueXP platform at no extra charge and can be deployed on-premises or in the customer cloud.

Steps

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



3. To enable BlueXP classification to scan your data for personally identifiable data, in the **Privacy exposure** column, select **Identify exposure**.

Result

Scanning might take several minutes depending on the amount of data. The Protection page shows that BlueXP classification is identifying files and gives you an indication of the number of files it is scanning.

When scanning is complete, the Privacy exposure column displays the exposure level as Low, Medium, or High.

Review the privacy exposure

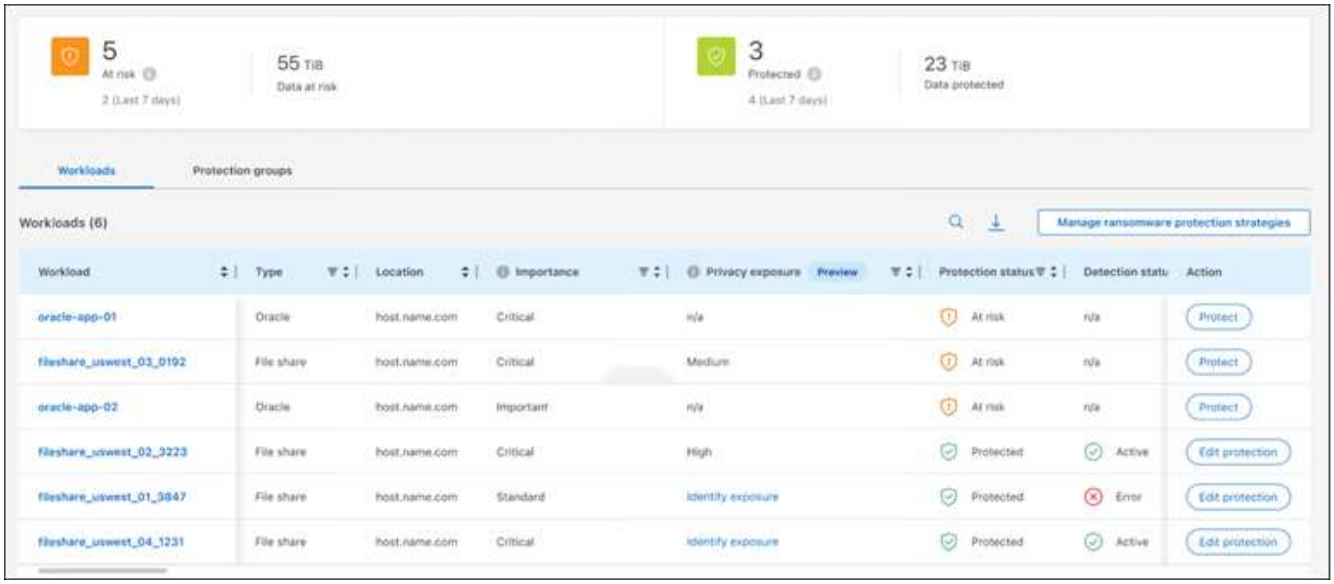
After BlueXP classification scans for personally identifiable information (PII), you can look at the PII data risk.

PII data can have one of the following privacy exposure risk statuses.

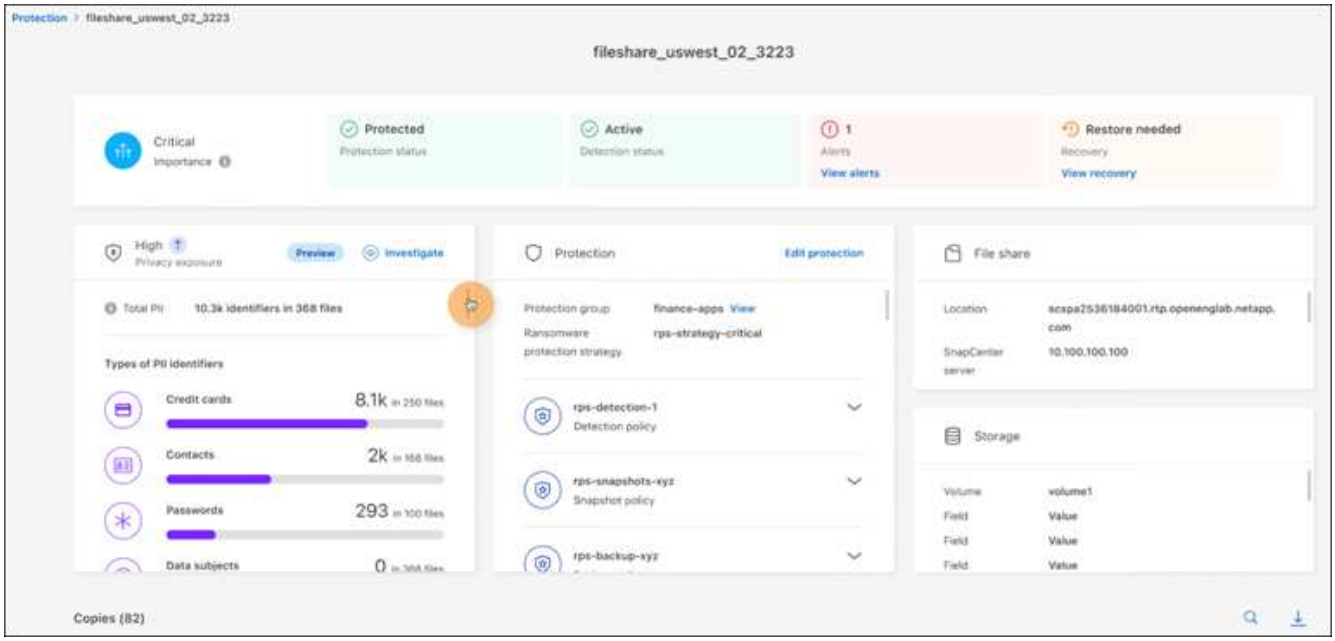
- **High**: Greater than 70% of files have PII
- **Medium**: Greater than 30% and less than 70% of files have PII
- **Low**: Greater than 0 and less than 30% of files have PII

Steps

1. From the BlueXP ransomware protection 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, review the information 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 BlueXP classification, refer to the following BlueXP classification topics:

- Learn about BlueXP classification
- Categories of private data
- Investigate the data stored in your organization

Copyright information

Trademark information