Get started

BlueXP ransomware protection

NetApp
March 22, 2024

Table of Contents

Get started

Learn about BlueXP ransomware protection preview

Ransomware attacks can block access to your systems and data and attackers can ask for ransom in exchange for the release of data or decryption. According to the IDC, it is not uncommon for victims of ransomware to experience multiple ransomware attacks. The attack can disrupt access to your data between one day and several weeks.

BlueXP ransomware protection is an orchestration service for ransomware protection, detection, and recovery. For the preview version, the service protects application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage as well as Cloud Volumes ONTAP in Amazon Web Services (using the NFS protocol) across BlueXP accounts and backs up data to Amazon Web Services cloud storage or NetApp StorageGRID.

> THIS DOCUMENTATION IS PROVIDED AS A TECHNOLOGY PREVIEW. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

What you can do with BlueXP ransomware protection

The BlueXP ransomware protection service provides full use of several NetApp technologies so that your storage administrator, data security administrator, or security operations engineer can accomplish the following goals:

- **Identify** all application-based, file-share, or VMware-managed workloads in NetApp on-premises NAS with NFS working environments in BlueXP, across BlueXP accounts, workspaces, and BlueXP Connectors. The service then categorizes the data priority and provides recommendations to you for ransomware protection improvements.
- **Protect** your workloads by enabling backups and Snapshot copies on your data.
- **Detect** anomalies that might be ransomware attacks.
- **Respond** to potential ransomware attacks by automatically initiating a NetApp ONTAP Snapshot copy.
- **Recover** your workloads that help accelerate workload uptime by orchestrating several NetApp technologies. You can choose to recover volumes, folders, or specific files. The service provides recommendations on the best options.

Benefits of using BlueXP ransomware protection

BlueXP ransomware protection offers the following benefits:

- Discovers workloads and datasets, analyzes the priority based on usage index, and ranks their relative importance.
- Evaluates your ransomware protection posture and displays it in an easy-to-understand dashboard.
- Provides recommendations on next steps based on discovery and protection posture analysis.
- Applies AI/ML-driven data protection recommendations with one-click access.

- Protects data in top application-based workloads, such as MySQL, Oracle, VMware datastores and file-shares.
- Detects ransomware attacks on data in real time on primary storage using AI technology.
- Initiates automated actions in response to detected potential attacks by creating Snapshot copies and initiating alerts about abnormal activity.
- Applies curated recovery to meet RPO policies. BlueXP ransomware protection orchestrates recovery from ransomware incidents by using several NetApp recovery services, including BlueXP backup and recovery (formerly Cloud Backup).

Cost

NetApp doesn’t charge you for using the preview version of BlueXP ransomware protection.

Licensing

The BlueXP ransomware protection preview itself does not require any special licensing. All preview licenses are Evaluation licenses.

For the preview version, NetApp helps to set up the evaluation and any required licenses.

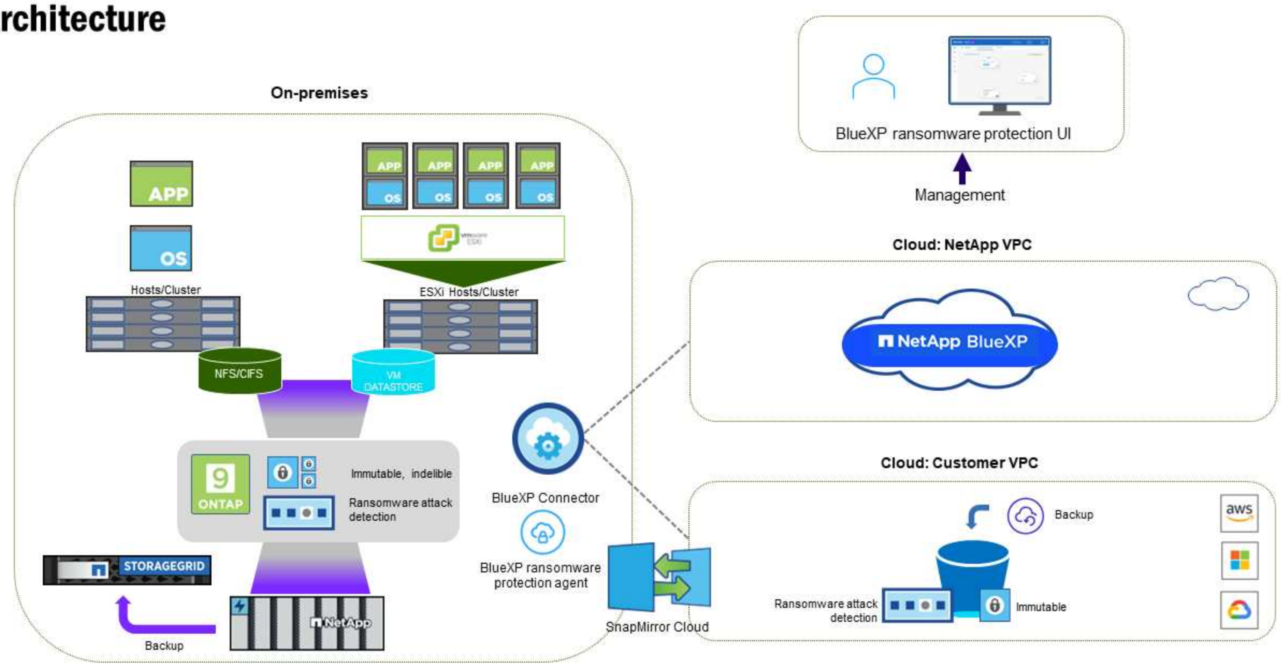
The BlueXP ransomware protection preview requires the following licenses:

- ONTAP
- NetApp Autonomous Ransomware Protection technology. Refer to Autonomous Ransomware Protection overview for details.
- BlueXP backup and recovery service

How BlueXP ransomware protection works

At a high-level, BlueXP ransomware protection works like this.

Architecture



Feature	Description
IDENTIFY	• Finds all customer on-premises NAS (NFS mounts) data connected to BlueXP. • Identifies customer data from ONTAP service APIs and associates it with workloads. Learn more about ONTAP and SnapCenter Software. • Discovers each volume's current protection level of NetApp Snapshot copies and backup policies as well as any on-box detection capabilities. The service then associates this protection posture with the workloads by using BlueXP backup and recovery, BlueXP digital advisor, and ONTAP services and NetApp technologies such as Autonomous Ransomware Protection, FPolicy, Backup policies, and Snapshot policies. Learn more about Autonomous Ransomware Protection and BlueXP backup and recovery, BlueXP Digital Advisor, and ONTAP FPolicy. • Assigns a business priority to each workload based on automatically discovered protection levels and recommends protection policies for workloads based on their business priority. • Ransomware protection also learns the policy associations and recommends your custom policies to similar workloads.
PROTECT	• Actively monitors workloads and orchestrates the use of BlueXP backup and recovery and ONTAP APIs by applying policies to each of the identified workloads.

Feature	Description
DETECT	• Detects potential attacks with an integrated machine learning (ML) model that detects potentially anomalous encryption and activity. • Provides dual-layer detection that starts with detecting potential ransomware attacks in the primary storage and responding to abnormal activities by taking additional automated Snapshot copies to create the nearest data restore points. The service provides the ability to dig deeper to identify potential attacks with greater precision without impacting the performance of the primary workloads. • Determines the specific suspect files and maps that attack to the associated workloads, using ONTAP, Autonomous Ransomware Protection and FPolicy technologies.
RESPOND	• Shows relevant data, such as file activity, user activity, and entropy, to help you complete forensic reviews about the attack. • Initiates quick Snapshot copies by using NetApp technologies and products such as ONTAP, Autonomous Ransomware Protection and FPolicy.
RECOVER	• Determines the best Snapshot or backup and recommends the best recovery point actual (RPA) by using BlueXP backup and recovery, ONTAP, Autonomous Ransomware Protection and FPolicy technologies and services. • Orchestrates the recovery of workloads including VMs, file shares, and databases with application consistency.

Supported backup targets, working environments, and data sources

Use BlueXP ransomware protection preview to see how resilient your data is to a cyber attack on the following types of backup targets, working environments, and data sources:

Backup targets supported

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Supported working environments

- On-premises ONTAP NAS (using NFS protocol)
- ONTAP Select
- Cloud Volumes ONTAP in AWS (using NFS protocol)

Data sources

For the preview version, the service protects the following application-based workloads:

- NetApp file shares
- VMware datastores
- Databases (For the preview version, Oracle and MySQL)

Terms that might help you with ransomware protection

You might benefit by understanding some terminology related to ransomware protection.

- **Protection**: Protection in BlueXP ransomware protection means ensuring that Snapshots and immutable backups occur on a regular basis to a different security domain using protection policies.
- **Workload**: A workload in BlueXP ransomware protection preview can include MySQL or Oracle databases, VMware datastores, or file shares.

BlueXP ransomware protection prerequisites

Get started with BlueXP ransomware protection by verifying the readiness of your operational environment, login, network access, and web browser.

To use BlueXP ransomware protection preview version, you'll need these prerequisites:

- An account in NetApp StorageGRID or AWS S3 for backup targets and the access permissions set

  Refer to the AWS permissions list for details.

- ONTAP 9.11.1 and later
  - Cluster admin ONTAP permissions
  - A license for NetApp Autonomous Ransomware Protection, used by BlueXP ransomware protection, enabled on the on-premises ONTAP instance, depending on the version of ONTAP you are using. Refer to Autonomous Ransomware Protection overview.

    For more licensing details, refer to Learn about BlueXP ransomware protection.

- In BlueXP:
  - A BlueXP Connector per each Virtual Private Cloud (VPC) or on an on-premises region must be set up in BlueXP. Refer to BlueXP documentation to configure the Connector.

    > If you have multiple BlueXP Connectors, the service will scan data across all Connectors beyond the one that currently shows in the BlueXP UI.

  - The BlueXP backup and recovery service with backup enabled on the working environment
  - A BlueXP working environment with NetApp NAS on-premises storage
  - A BlueXP account with at least one active Connector connecting to on-premises ONTAP clusters. All source and working environments must be on the same BlueXP account.
  - A BlueXP user account with Account Admin privileges for discovering resources
  - Standard BlueXP requirements

Quick start for BlueXP ransomware protection

Here's an overview of the steps needed to get started with BlueXP ransomware protection. The links within each step take you to a page that provides more details.

1 **Review prerequisites**

Ensure your environment meets these requirements.

2 **Set up the ransomware protection service**

- Prepare NetApp StorageGRID or Amazon Web Services as a backup destination.
- Configure a Connector in BlueXP.
- Configure backup destinations.
- Discover workloads in BlueXP.

3 **What's next?**

After you set up the service, here's what you might do next.

- View workload protection health on the Dashboard.
- Protect workloads.
- Respond to detection of potential ransomware attacks.
- Recover from an attack (after incidents are neutralized).

Set up BlueXP ransomware protection

To use BlueXP ransomware protection, perform a few steps to set it up.

Before you begin, review prerequisites to ensure that your environment is ready.

Prepare the backup destination

Prepare one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services

After you configure options in the backup destination itself, you will later configure it as a backup destination in the BlueXP ransomware protection service.

Prepare StorageGRID to become a backup destination

If you want to use StorageGRID as your backup destination, refer to StorageGRID documentation for details about StorageGRID.

Prepare AWS to become a backup destination

- Set up an account in AWS.
- Configure AWS permissions in AWS.

For details about managing your AWS storage in BlueXP, refer to Manage your Amazon S3 buckets.

Set up BlueXP

The next step is to set up BlueXP and the BlueXP ransomware protection service.

Review standard BlueXP requirements.

Create a Connector in BlueXP

You should reach out to your NetApp Sales Rep to try out this service. Then, when you use the BlueXP Connector, it will include the appropriate capabilities for the ransomware protection service.

To create a Connector in BlueXP before using the service, refer to the BlueXP documentation that describes how to create a BlueXP Connector.

> ⓘ If you have multiple BlueXP Connectors, the service will scan data across all Connectors beyond the one that currently shows in the BlueXP UI. This service discovers all workspaces and all Connectors associated with this account.

Access BlueXP ransomware protection

You use NetApp BlueXP to log in to the BlueXP ransomware protection service. From the BlueXP left navigation, select **Protection** > **Ransomware protection**.

For details, refer to Access BlueXP ransomware protection.

Configure backup destinations in BlueXP ransomware protection

Use the BlueXP ransomware protection backup destinations option to configure backup destinations. For details, refer to Configure settings options.

Access BlueXP ransomware protection

You use NetApp BlueXP to log in to the BlueXP ransomware protection service.

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. Learn more about logging in.

Steps

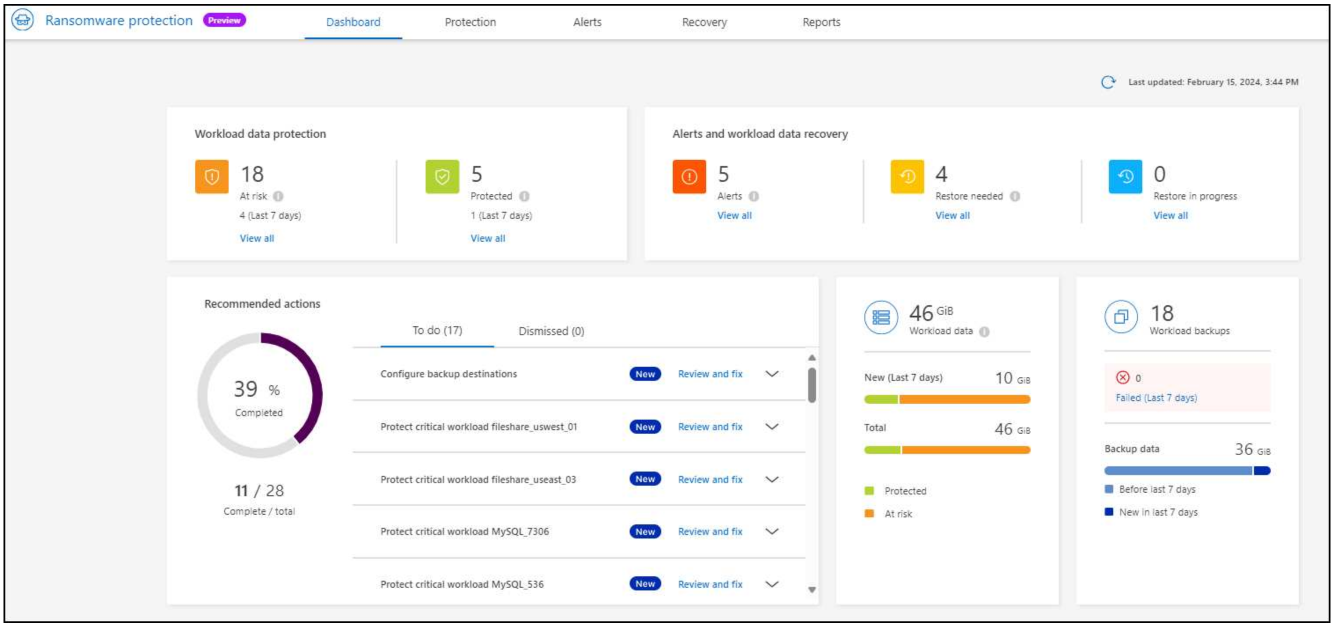
1. Open a web browser and go to the BlueXP console.

   The NetApp BlueXP login page appears.

2. Log in to BlueXP.
3. From the BlueXP left navigation, select **Protection** > **Ransomware protection**.

   If this is your first time logging in to this service, the landing page appears.

   Otherwise, the BlueXP ransomware protection Dashboard appears.



Last updated: February 15, 2024, 3:44 PM

Workload data protection

18 At risk — 4 (Last 7 days) — View all

5 Protected — 1 (Last 7 days) — View all

Alerts and workload data recovery

5 Alerts — View all

4 Restore needed — View all

0 Restore in progress — View all

Recommended actions

39 % Completed

11 / 28 Complete / total

To do (17) | Dismissed (0)

Configure backup destinations	New	Review and fix
Protect critical workload fileshare_uswest_01	New	Review and fix
Protect critical workload fileshare_useast_03	New	Review and fix
Protect critical workload MySQL_7306	New	Review and fix
Protect critical workload MySQL_536	New	Review and fix

46 GiB Workload data

New (Last 7 days) 10 GiB

Total 46 GiB

🟩 Protected

🟧 At risk

18 Workload backups

0 Failed (Last 7 days)

Backup data 36 GiB

■ Before last 7 days

■ New in last 7 days

4. Start using the service.
   - If you don’t have a BlueXP Connector or it’s not the one for this preview, you might need to contact NetApp Support or follow messages to sign up for this preview.
   - If you are new to BlueXP and haven’t used any Connector, when you select "**Ransomware protection**", a message appears about signing up. Go ahead and submit the form. NetApp will contact you about your evaluation request.
   - If you are a BlueXP user with an an existing Connector, when you select "**Ransomware protection**", a message appears about signing up.
   - If you are already participating in the preview, when you select "**Ransomware protection**", you can proceed with the service. If you haven’t done so already, you should select the **Discover workloads** option.

Discover workloads in BlueXP ransomware protection

To use BlueXP ransomware protection, the service needs to first discover data. During discovery, BlueXP ransomware protection analyzes all volumes and files in working environments across all BlueXP Connectors and workspaces within an account.

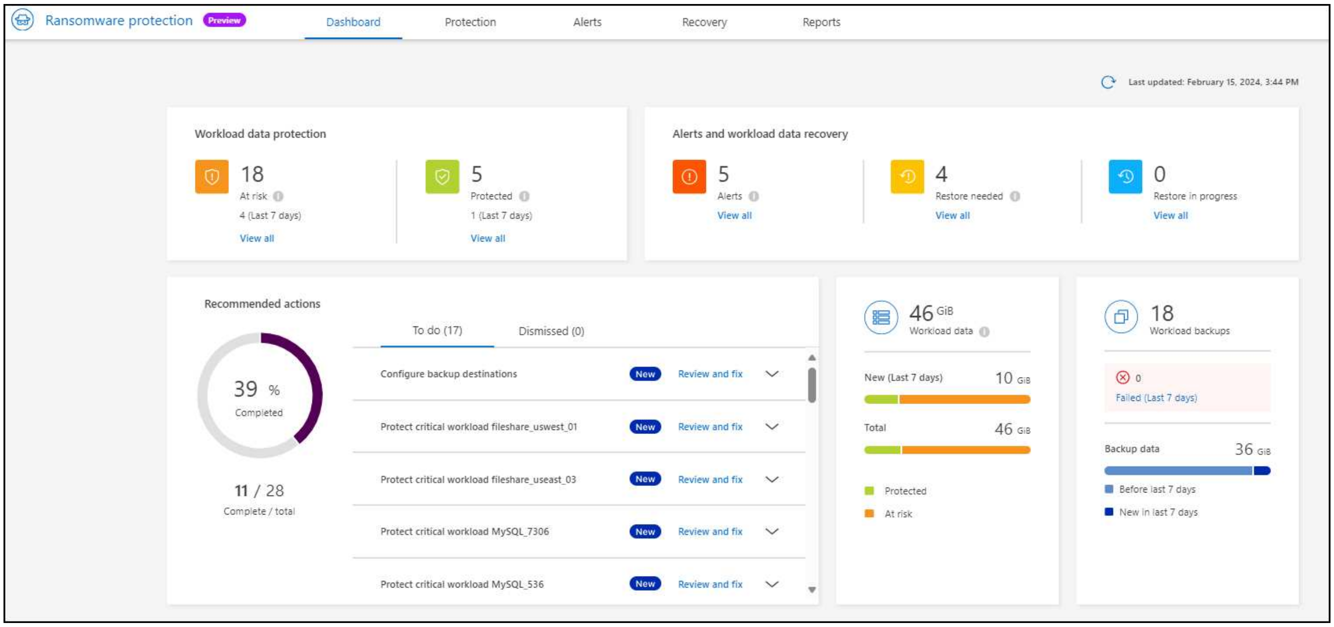
> For the preview version, BlueXP ransomware protection assesses MySQL applications, Oracle applications, VMware datastores, and file shares.

The service assesses the existing protection level including the current backup protection, Snapshot copies, and NetApp Autonomous Ransomware Protection options. Based on the assessment, the service then recommends how to improve your ransomware protection.

Steps

1. From the BlueXP left navigation, select **Protection** > **Ransomware protection**.
2. Select **Discover workloads** from the initial landing page.

   The service discovers workload data and shows the health of data protection in the Dashboard.



Configure BlueXP ransomware protection settings

You can configure a backup destination by reviewing recommendations on the Dashboard.

Add a backup destination

BlueXP ransomware protection can identify workloads that do not have any backups yet and also workloads that do not have any backup destinations assigned yet.

To protect those workloads, you should add a backup destination. You can choose one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services (AWS)

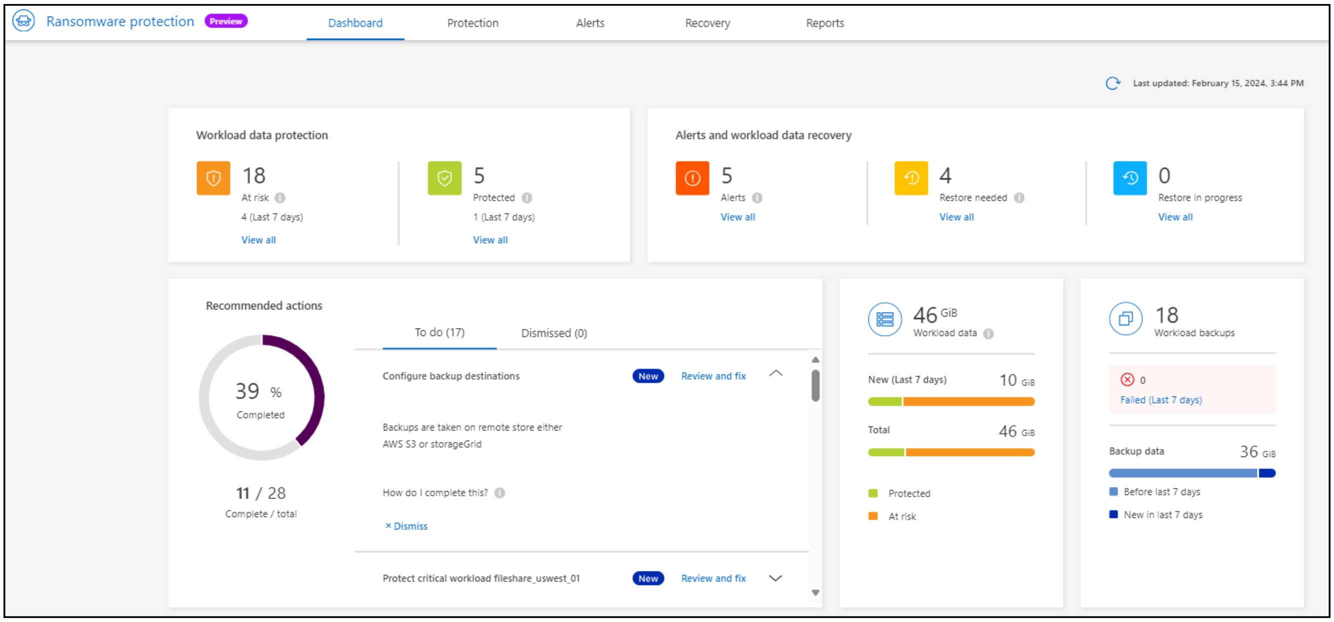
You can add a backup destination based on a recommended action from the Dashboard.

Access Backup Destination options from the Dashboard's recommended actions

The Dashboard provides many recommendations. One recommendation might be to configure a backup destination.

Steps

1. From the BlueXP left navigation, select **Protection** > **Ransomware protection**.
2. Review the Dashboard's Recommended actions pane.



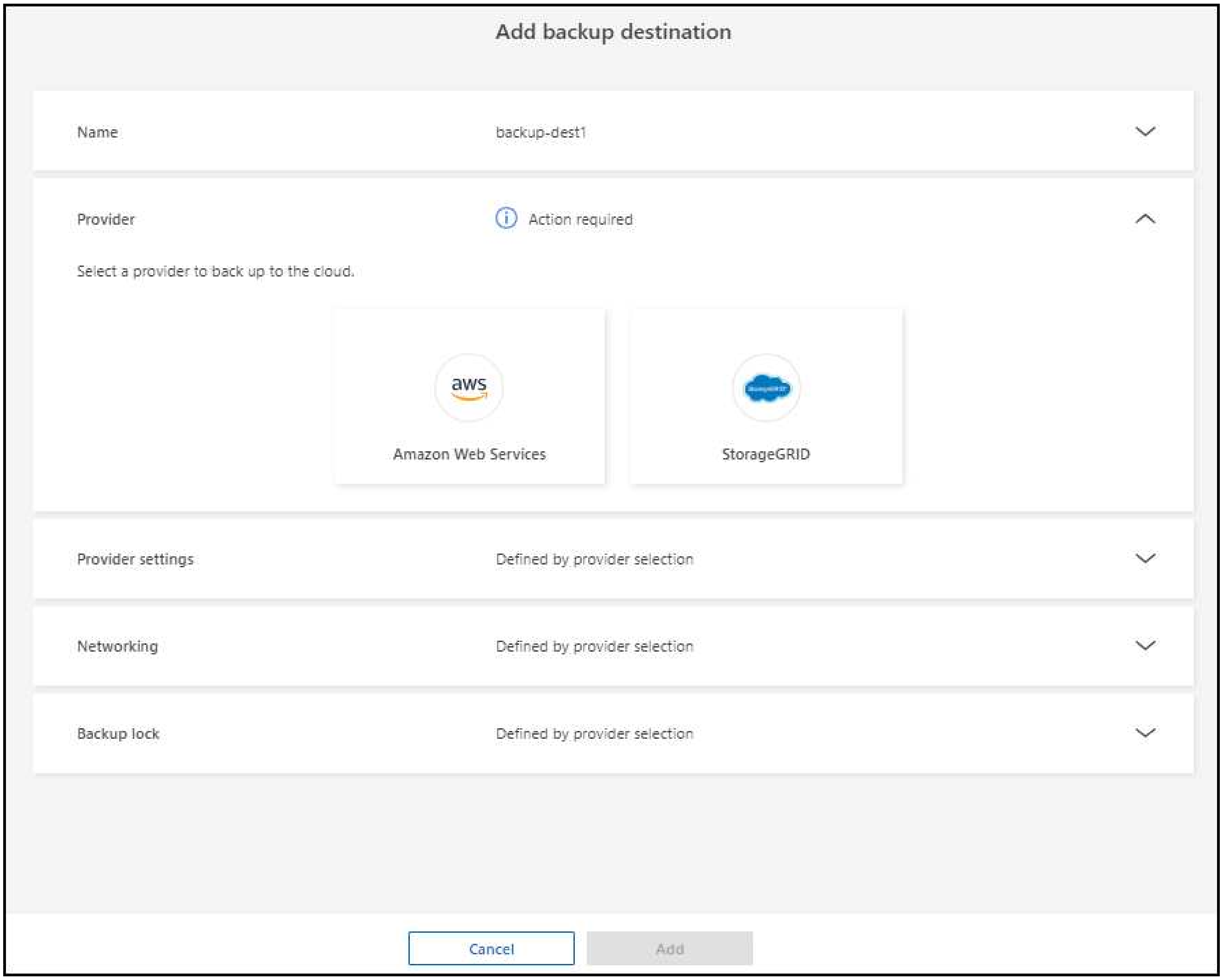
Backups are taken on remote store either AWS S3 or storageGrid

3. From the Dashboard, select **Review and fix** for the recommendation of "Configure backup destinations."
4. Continue with instructions depending on the backup provider.

Add StorageGRID as a backup destination

To set up NetApp StorageGRID as a backup destination, enter the following information.

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



Add backup destination

Name: backup-dest1

Provider: Action required

Select a provider to back up to the cloud.

Provider settings: Defined by provider selection

Networking: Defined by provider selection

Backup lock: Defined by provider selection

3. Select **StorageGRID**.
4. Select the Down arrow next to each setting and enter or select values:
   - **Provider settings**:
     - Create a new bucket or bring your own bucket that will store the backups.
     - StorageGRID gateway node fully qualified domain name, port, StorageGRID access key and secret key credentials.
   - **Networking**: Choose the IPspace.
     - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
   - **Backup lock**: Choose whether you want the service to protect backups from being modified or deleted. This option uses the NetApp DataLock technology. Each backup will be locked during the retention period, or for a minimum of 30 days, plus a buffer period of up to 14 days.

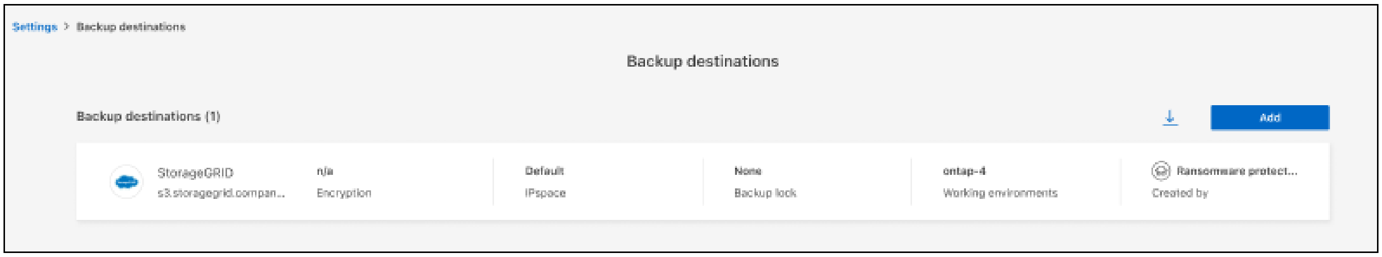
     > If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

     - **Compliance mode**: Users cannot overwrite or delete protected backup files during the retention period.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Settings > Backup destinations

Backup destinations

Backup destinations (1)

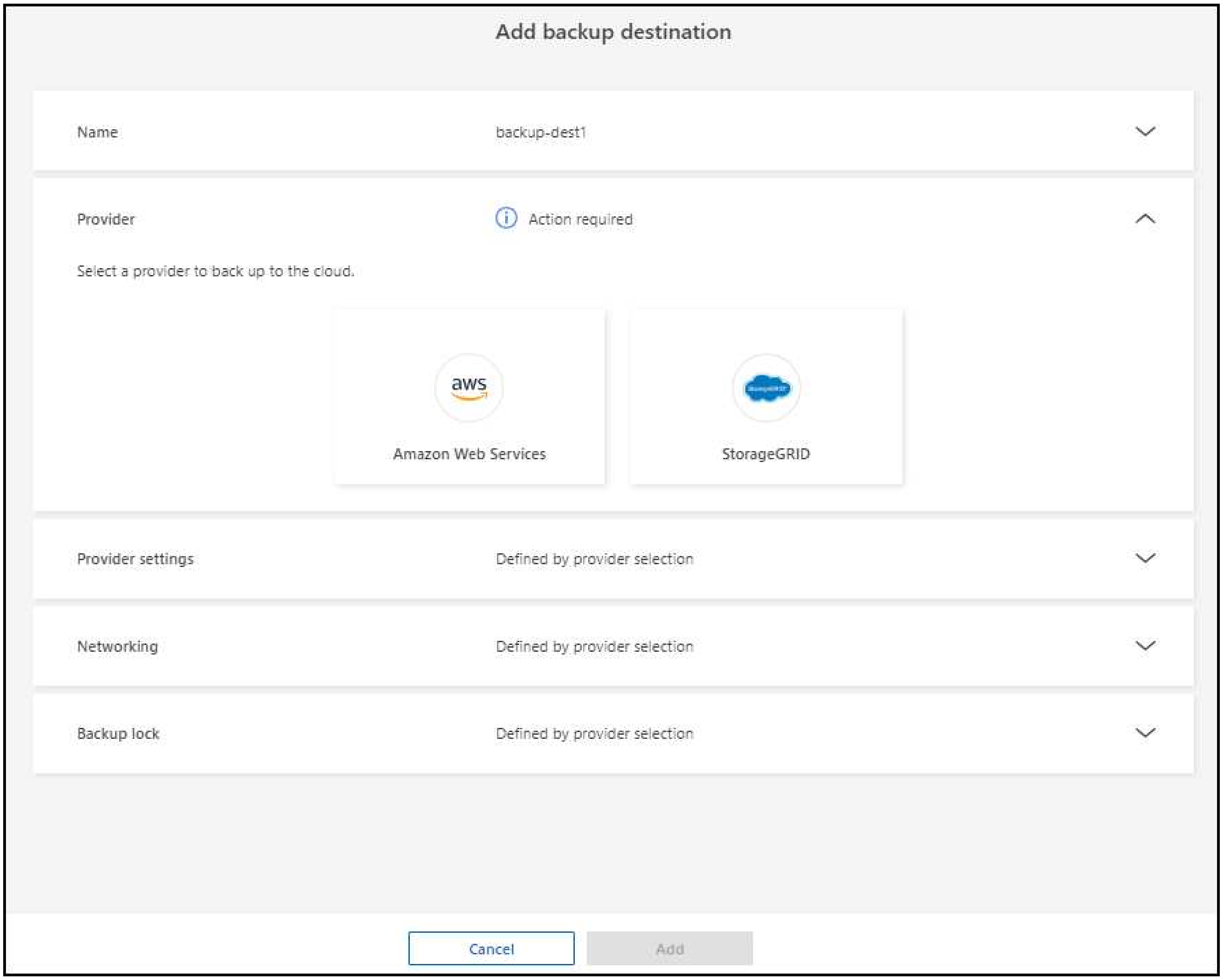
StorageGRID s3.storagegrid.compan...	n/a Encryption	Default IPspace	None Backup lock	ontap-4 Working environments	Ransomware protect... Created by

Add Amazon Web Services as a backup destination

To set up AWS as a backup destination, enter the following information.

For details about managing your AWS storage in BlueXP, refer to Manage your Amazon S3 buckets.

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



Add backup destination

Name	backup-dest1
Provider	Action required

Select a provider to back up to the cloud.

Provider settings	Defined by provider selection
Networking	Defined by provider selection
Backup lock	Defined by provider selection

3. Select **Amazon Web Services**.
4. Select the Down arrow next to each setting and enter or select values:
   - **Provider settings**:
     - Create a new bucket, select an existing bucket if one already exists in BlueXP, or bring your own bucket that will store the backups.
     - AWS account, region, access key and secret key for AWS credentials

       If you want to bring your own bucket, refer to Add S3 buckets.
   - **Encryption**: If you are creating a new S3 bucket, enter encryption key information given to you from the provider. If you chose an existing bucket, encryption information is already available.

     Data in the bucket is encrypted with AWS-managed keys by default. You can continue to use AWS-managed keys, or you can manage the encryption of your data using your own keys.
   - **Networking**: Choose the IPspace and whether you'll be using a Private Endpoint.
     - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
     - Optionally, choose whether you'll use an AWS private endpoint (PrivateLink) that you previously configured.

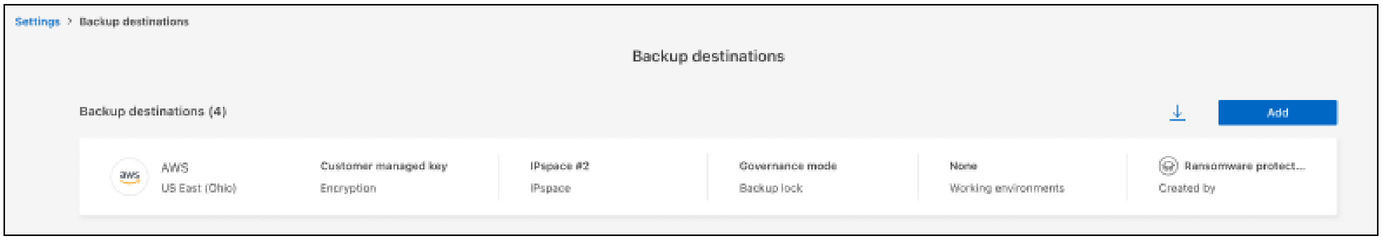
       If you want to use AWS PrivateLink, refer to AWS PrivateLink for Amazon S3.
   - **Backup lock**: Choose whether you want the service to protect backups from being modified or deleted. This option uses the NetApp DataLock technology. Each backup will be locked during the retention period, or for a minimum of 30 days, plus a buffer period of up to 14 days.

     > ! If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

     - **Governance mode**: Specific users (with s3:BypassGovernanceRetention permission) can overwrite or delete protected files during the retention period.
     - **Compliance mode**: Users cannot overwrite or delete protected backup files during the retention period.
5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Settings > Backup destinations

Backup destinations

Backup destinations (4)

AWS	Customer managed key	IPspace #2	Governance mode	None	Ransomware protect...
US East (Ohio)	Encryption	IPspace	Backup lock	Working environments	Created by

Frequently asked questions for BlueXP ransomware protection

This FAQ can help if you're just looking for a quick answer to a question.

Access

What's the BlueXP ransomware protection URL?
For the URL, in a browser, enter: https://console.bluexp.netapp.com/ to access the BlueXP console.

Do you need a license to use BlueXP ransomware protection?
A NetApp License File (NLF) is not required. The BlueXP ransomware protection preview itself does not require any special licensing. All preview licenses are Evaluation licenses.

The preview version of this service requires a BlueXP backup and recovery service license.

For the preview version, NetApp helps to set up the evaluation and any required licenses.

How do you enable BlueXP ransomware protection?
BlueXP ransomware protection does not require any enablement. The ransomware protection option is automatically enabled on the BlueXP left navigation.

For the preview version, you need to sign up or reach out to your NetApp Sales rep to try out this service. Then, when you use the BlueXP Connector, it will include the appropriate capabilities for the service.

Does BlueXP ransomware protection available in standard, restricted, and private modes?
At this time, BlueXP ransomware protection is available only in standard mode. Stay tuned for more.

For an explanation about these modes across all BlueXP services, refer to BlueXP deployment modes.

How are access permissions handled?
Only account admins have the ability to initiate the service and discover workloads (because this involves committing to usage of a resource). Subsequent interactions can be done by any role.

What device resolution is best?
The recommended device resolution for BlueXP ransomware protection is 1920x1080 or better.

Which browser should I use?
Any modern browser will work.

Interaction with other services

Is BlueXP ransomware protection aware of protection settings made in NetApp ONTAP?
Yes, BlueXP ransomware protection discovers Snapshot schedules set in ONTAP.

If you set a policy using BlueXP ransomware protection, do you have to make future changes only in this service?
We recommend that you make policy changes from the BlueXP ransomware protection service.

Workloads

What makes up a workload?
A workload includes all volumes that are used by a single application instance. For example, an Oracle DB instance deployed on ora3.host.com can have vol1 and vol2 for its data and logs, respectively. Those volumes together constitute the workload for that specific instance of the Oracle DB instance.

How does BlueXP ransomware protection prioritize workload data?
Data priority for the Preview version is determined by the Snapshot copies made and backups that are scheduled.

The workload priority is determined by the following Snapshot frequencies:

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

New volume added, but doesn’t appear yet
If you added a new volume to your environment, initiate discovery again and apply protection policies to protect that new volume.

The Dashboard doesn’t show all my workloads. What might be wrong?
Currently, only NFS volumes are supported. iSCSI volumes, CIFS volumes and other non-supported configurations are filtered out and do not appear on the Dashboard.

Protection policies

Do BlueXP ransomware policies co-exist with the other kinds of workload policies?
At this time, BlueXP backup and recovery (Cloud Backup) supports one backup policy per volume. So, BlueXP backup and recovery and BlueXP ransomware protection share backup policies.

Snapshot copies are not limited and can be added separately from each service.

Copyright information

Trademark information