NetApp Ransomware Resilience documentation

NetApp Ransomware Resilience

NetApp
October 06, 2025

This PDF was generated from https://docs.netapp.com/us-en/data-services-ransomware-resilience/index.html on October 06, 2025. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Ransomware Resilience documentation

Release notes

What’s new in NetApp Ransomware Resilience

Learn what’s new in NetApp Ransomware Resilience.

06 October 2025

BlueXP ransomware protection is now NetApp Ransomware Resilience

BlueXP ransomware replication has been renamed to NetApp Ransomware Resilience.

BlueXP is now NetApp Console

BlueXP has been renamed and redesigned to better reflect its role in managing your data infrastructure.

The NetApp Console provides centralized management of storage and data services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration.

For details on what has changed, see the NetApp Console release notes.

15 July 2025

SAN workload support

This release includes support for SAN workloads in BlueXP ransomware protection. You can now protect SAN workloads in addition to NFS and CIFS workloads.

For more information, refer to BlueXP ransomware protection prerequisites.

Improved workload protection

This release improves the configuration process for workloads with snapshot and backup policies from other NetApp tools such as SnapCenter or BlueXP backup and recovery. In previous releases, BlueXP ransomware protection discovered the policies from other tools, only allowing you to change the detection policy. With this release, you can now replace snapshot and backup policies with BlueXP ransomware protection policies or continue to use the policies from other tools.

For details, refer to Protect workloads.

Email notifications

If BlueXP ransomware protection detects a possible attack, a notification appears in the BlueXP Notifications, and an email is sent to the email address that you configured.

The email includes information about the severity, the impacted workload, and a link to the alert in the BlueXP ransomware protection **Alerts** tab.

If you configured a security and event management (SIEM) system in BlueXP ransomware protection, the service sends alert details to your SIEM system.

For details, refer to Handle detected ransomware alerts.

9 June 2025

Landing page updates

This release includes updates to the landing page for BlueXP ransomware protection that makes starting the free trial and discovery easier.

Readiness drill updates

Previously, you could run a ransomware readiness drill by simulating an attack on a new sample workload. With this feature, you can investigate the simulated attack and recover the workload. Use this feature to test alert notifications, response, and recovery. Run and schedule these drills as often as needed.

With this release, you can use a new button on the BlueXP ransomware protection Dashboard to run a ransomware readiness drill on a test workload, making it easier for you to simulate ransomware attacks, investigate their impact, and recover workloads efficiently, all within a controlled environment.

You can now run readiness drills on CIFS (SMB) workloads in addition to NFS workloads.

For details, refer to Conduct a ransomware attack readiness drill.

Enable BlueXP classification updates

Before you use BlueXP classification within the BlueXP ransomware protection service, you need to enable BlueXP classification to scan your data. Classifying data helps you find personally identifiable information (PII), which can increase security risks.

You can deploy BlueXP classification on a file share workload from within BlueXP ransomware protection. In the **Privacy exposure** column, select the **Identify exposure** option. If you've enabled the classification service, this action identifies the exposure. Otherwise, with this release, a dialog box presents the option to deploy BlueXP classification. Select **Deploy** to go to the BlueXP classification service landing page, where you can deploy that service. W

For details, refer to Deploy BlueXP classification in the cloud and to use the service within BlueXP ransomware protection, refer to Scan for personally identifiable information with BlueXP classification.

13 May 2025

Reporting of unsupported working environments in BlueXP ransomware protection

During the discovery workflow, BlueXP ransomware protection reports more details when you hover over Supported or Unsupported Workloads. This will help you understand why some of your workloads are not discovered by the BlueXP ransomware protection service.

There are many reasons why the service doesn't support a working environment, for example, the ONTAP version on your working environment could be below the required version. When you hover over an unsupported working environment, a tooltip displays the reason.

You can view the unsupported working environments during initial discovery, where you can also download the results. You can also view the results of discovery from the **Workload discovery** option in the Settings page.

For details, refer to Discover workloads in BlueXP ransomware protection.

29 April 2025

Support for Amazon FSx for NetApp ONTAP

This release supports Amazon FSx for NetApp ONTAP. This feature helps you protect your FSx for ONTAP workloads with BlueXP ransomware protection.

FSx for ONTAP is a fully managed service that provides the power of NetApp ONTAP storage in the cloud. It provides the same features, performance, and administrative capabilities that you use on-premises with the agility and scalability of a native AWS service.

The following changes were made to the BlueXP ransomware protection workflow:

- Discovery includes workloads in FSx for ONTAP 9.15 working environments.
- The Protection tab shows workloads in FSx for ONTAP environments. In this environment, you should perform backup operations using the FSx for ONTAP backup service. You can restore these workloads using BlueXP ransomware protection snapshots.

  > Backup policies for a workload running on FSx for ONTAP can’t be set in BlueXP. Any existing backup policies set in Amazon FSx for NetApp ONTAP remain unchanged.

- Alert incidents show the new FSx for ONTAP working environment.

For details, refer to Learn about BlueXP ransomware protection and working environments.

For information about the supported options, refer to the BlueXP ransomware protection limitations.

BlueXP access role needed

You now need one of the following access roles to view, discover, or manage BlueXP ransomware protection: Organization admin, Folder or project admin, Ransomware protection admin, or Ransomware protection viewer.

Learn about BlueXP access roles for all services.

14 April 2025

Readiness drill reports

With this release, you can review ransomware attack readiness drill reports. A readiness drill enables you to simulate a ransomware attack on a newly created, sample workload. Then, investigate the simulated attack and recover the sample workload. This feature helps you know that you are prepared in the event of an actual ransomware attack by testing alert notification, response, and recovery processes.

For details, refer to Conduct a ransomware attack readiness drill.

New role-based access control roles and permissions

Previously, you could assign roles and permissions to users based on their responsibilities, which helps you manage user access to BlueXP ransomware protection. With this release, there are two new roles specific to BlueXP ransomware protection with updated permissions. The new roles are:

- Ransomware protection admin

- Ransomware protection viewer

For details about permissions, refer to BlueXP ransomware protection role-based access to features.

Payment improvements

This release includes several improvements to the payment process.

For details, refer to Set up licensing and payment options.

10 March 2025

Simulate an attack and respond

With this release, simulate a ransomware attack to test your response to a ransomware alert. This feature helps you know that you are prepared in the event of an actual ransomware attack by testing alert notification, response, and recovery processes.

For details, refer to Conduct a ransomware attack readiness drill.

Enhancements to discovery process

This release includes enhancements to the selective discovery and rediscovery processes:

- With this release, you can discover newly created workloads that were added to the previously selected working environments.
- You can also select *new* working environments in this release. This feature helps you protect new workloads that are added to your environment.
- You can perform these discovery processes during the discovery process initially or within the Settings option.

For details, refer to Discover newly created workloads for previously selected working environments and Configure features with the Settings option.

Alerts raised when high encryption is detected

With this release, you can view alerts when high encryption is detected on your workloads even without high file extension changes. This feature, which uses ONTAP Autonomous Ransomware Protection (ARP) AI, helps you identify workloads that are at risk of ransomware attacks. Use this feature and download the entire list of impacted files with or without extension changes.

For details, refer to Respond to a detected ransomware alert.

16 December 2024

Detect anomalous user behavior using Data Infrastructure Insights Storage Workload Security

With this release, you can use Data Infrastructure Insights Storage Workload Security to detect anomalous user behavior in your storage workloads. This feature helps you identify potential security threats and block potentially malicious users to protect your data.

For details, refer to Respond to a detected ransomware alert.

Before you use Data Infrastructure Insights Storage Workload Security to detect anomalous user behavior, you need to configure the option by using the BlueXP ransomware protection **Settings** option.

Refer to Configure BlueXP ransomware protection settings.

Select workloads to discover and protect

With this release, you can now do the following:

- Within each Connector, select the working environments where you want to discover workloads. You might benefit from this feature if you want to protect specific workloads in your environment and not others.
- During workload discovery, you can enable automatic discovery of workloads per Connector. This feature lets you select the workloads that you want to protect.
- Discover newly created workloads for previously selected working environments.

Refer to Discover workloads.

7 November 2024

Enable data classification and scan for personally identifiable information (PII)

With this release, you can enable BlueXP classification, a core component of the BlueXP family, to scan and classify data in your file share workloads. Classifying data helps you identify whether your data includes personal or private information, which can increase security risks. This process also impacts workload importance and helps you ensure that you are protecting workloads with the right level of protection.

Scanning for PII data in BlueXP ransomware protection is generally 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.

Refer to Configure BlueXP ransomware protection settings.

To initiate scanning, on the Protection page, click **Identify exposure** in the Privacy exposure column.

Scan for personally identifiable sensitive data with BlueXP classification.

SIEM integration with Microsoft Sentinel

You can now send data to your security and event management system (SIEM) for threat analysis and detection using Microsoft Sentinel. Previously, you could select the AWS Security Hub or Splunk Cloud as your SIEM.

Learn more about configuring BlueXP ransomware protection settings.

Free trial now 30 days

With this release, new deployments of BlueXP ransomware protection now have 30 days for a free trial. Previously, BlueXP ransomware protection provided 90 days as a free trial. If you are already in the 90-day free trial, that offer continues for the 90 days.

Restore application workload at the file level for Podman

Before you restore an application workload at the file level, you can now view a list of files that might have been impacted by an attack and identify those you want to restore. Previously, if the BlueXP Connectors in an organization (previously an account) were using Podman, this feature was disabled. It is now enabled for Podman. You can let BlueXP ransomware protection choose the files to restore, you can upload a CSV file that lists all the files impacted by an alert, or you can manually identify which files you want to restore.

Learn more about recovering from a ransomware attack.

30 September 2024

Custom grouping of file share workloads

With this release, you can now group file shares into groups to make it easier for you to protect your data estate. The service can protect all volumes in a group at the same time. Previously, you needed to protect each volume separately.

Learn more about grouping file share workloads in ransomware protection strategies.

2 September 2024

Security risk assessment from Digital Advisor

BlueXP ransomware protection now gathers information about high and critical security risks related to a cluster from NetApp Digital Advisor. If any risk is found, BlueXP ransomware protection provides a recommendation in the Dashboard's **Recommended actions** pane: "Fix a known security vulnerability on the cluster <name>." From the recommendation on the Dashboard, clicking **Review and fix** suggests to review Digital Advisor and a Common Vulnerability & Exposure (CVE) article to resolve the security risk. If there are multiple security risks, review information in Digital Advisor.

Refer to Digital Advisor documentation.

Back up to Google Cloud Platform

With this release, you can set a backup destination to a Google Cloud Platform bucket. Previously, you could add backup destinations only to NetApp StorageGRID, Amazon Web Services, and Microsoft Azure.

Learn more about configuring BlueXP ransomware protection settings.

Support for Google Cloud Platform

The service now supports Cloud Volumes ONTAP for Google Cloud Platform for storage protection. Previously, the service supported only Cloud Volumes ONTAP for Amazon Web Services and Microsoft Azure along with on-premises NAS.

Learn about BlueXP ransomware protection and supported data sources, backup destinations, and working environments.

Role-based access control

You can now limit access to specific activities with role-based access control (RBAC). BlueXP ransomware protection uses two roles from BlueXP: BlueXP Account Admin and Non-Account Admin (Viewer).

For details about the actions that each role can perform, see Role-based access control privileges.

5 August 2024

Threat detection with Splunk Cloud

You can automatically send data to your security and event management system (SIEM) for threat analysis and detection. With previous releases, you could select only the AWS Security Hub as your SIEM. With this release, you can select the AWS Security Hub or Splunk Cloud as your SIEM.

Learn more about configuring BlueXP ransomware protection settings.

1 July 2024

Bring your own license (BYOL)

With this release, you can use a BYOL license, which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep.

Learn more about setting up licensing.

Restore application workload at the file level

Before you restore an application workload at the file level, you can now view a list of files that might have been impacted by an attack and identify those you want to restore. You can let BlueXP ransomware protection choose the files to restore, you can upload a CSV file that lists all the files impacted by an alert, or you can manually identify which files you want to restore.

> ⓘ With this release, if all BlueXP Connectors in an account are not using Podman, the single file restore feature is enabled. Otherwise, it is disabled for that account.

Learn more about recovering from a ransomware attack.

Download a list of impacted files

Before restoring an application workload at the file level, you can now access the Alerts page to download a list of impacted files in a CSV file and then use the Recovery page to upload the CSV file.

Learn more about downloading impacted files before restoring an application.

Delete protection plan

With this release, you can now delete a ransomware protection strategy.

Learn more about protecting workloads and managing ransomware protection strategies.

10 June 2024

Snapshot copy locking on primary storage

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.

Learn more about protecting workloads and enabling backup locking in a ransomware protection strategy.

Support for Cloud Volumes ONTAP for Microsoft Azure

This release supports Cloud Volumes ONTAP for Microsoft Azure as a system in addition to Cloud Volumes ONTAP for AWS and on-premises ONTAP NAS.

Quick start for Cloud Volumes ONTAP in Azure

Learn about BlueXP ransomware protection.

Microsoft Azure added as a backup destination

You can now add Microsoft Azure as a backup destination along with AWS and NetApp StorageGRID.

Learn more about how to Configure protection settings.

14 May 2024

Licensing updates

You can sign up for a 90-day free trial. Soon you be will be able to purchase a pay-as-you-go subscription with Amazon Web Services Marketplace or bring your own NetApp license.

Learn more about setting up licensing.

CIFS protocol

The service now supports on-premises ONTAP and Cloud Volumes ONTAP in AWS systems using both NFS and CIFS protocols. The previous release supported only the NFS protocol.

Workload details

This release now provides more details in the workload information from the Protection and other pages for improved workload protection assessment. From the workload details, you can review the currently assigned policy and review the configured backup destinations.

Learn more about viewing workload details in the Protection pages.

Application-consistent and VM-consistent protection and recovery

You can now perform application-consistent protection with NetApp SnapCenter Software and VM-consistent protection with SnapCenter Plug-in for VMware vSphere, achieving a quiescent and consistent state to avoid potential data loss later if recovery is needed. If recovery is required, you can restore the application or VM back to any of the previously available states.

Learn more about protecting workloads.

Ransomware protection strategies

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 this service:

- Snapshot policy
- Backup policy

- Detection policy

Learn more about protecting workloads.

Threat detection

Enable threat detection is now available using a third-party security and event management (SIEM) system. The Dashboard now shows a new recommendation to "Enable threat detection" which can be configured on the Settings page.

Learn more about configuring Settings options.

Dismiss false positive alerts

From the Alerts tab, you can now dismiss false positives or decide to recover your data immediately.

Learn more about responding to a ransomware alert.

Detection status

New detection statuses appear on the Protection page showing the status of the ransomware detection applied to the workload.

Learn more about protecting workloads and viewing protection statuses.

Download CSV files

You can download CSV files* from the Protection, Alerts, and Recovery pages.

Learn more about downloading CSV files from the Dashboard and other pages.

Documentation link

View documentation link is now included in the UI. You can access this documentation from the Dashboard vertical **Actions** ⋮ option. Select **What's new** to view details in the Release Notes or **Documentation** to view the BlueXP ransomware protection documentation Home page.

BlueXP backup and recovery

The BlueXP backup and recovery service no longer needs to be already enabled on the system. See prerequisites. The BlueXP ransomware protection service helps configure a backup destination through the Settings option. See Configure settings.

Settings option

You can now set up backup destinations in BlueXP ransomware protection Settings.

Learn more about configuring Settings options.

5 March 2024

Protection policy management

In addition to using predefined policies, you can now create policies. Learn more about managing policies.

Immutability on secondary storage (DataLock)

You can now make the backup immutable in secondary storage using NetApp DataLock technology in the object store. Learn more about creating protection policies.

Automatic backup to NetApp StorageGRID

In addition to using AWS, you can now choose StorageGRID as your backup destination. Learn more about configuring backup destinations.

Additional features to investigate potential attacks

You can now view more forensic details to investigate the detected potential attack. Learn more about responding to a detected ransomware alert.

Recovery process

The recovery process was enhanced. Now, you can recover volume by volume or all volumes for a workload. Learn more about recovering from a ransomware attack (after incidents have been neutralized).

Learn about BlueXP ransomware protection.

6 October 2023

The BlueXP ransomware protection service is a SaaS solution for protecting data, detecting potential attacks, and recovering data from a ransomware attack.

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 on AWS (using the NFS protocol) across BlueXP organizations individually and backs up data to Amazon Web Services cloud storage.

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

- View ransomware protection on all your workloads at a glance.
- Gain insight into ransomware protection recommendations
- Improve protection posture based on BlueXP ransomware protection recommendations.
- Assign ransomware protection policies to protect your top workloads and high-risk data against ransomware attacks.
- Monitor the health of your workloads against ransomware attacks looking for data anomalies.
- Quickly assess the impact of ransomware incidents on your workload.
- Recover from ransomware incidents intelligently by restoring data and ensuring that reinfection from stored data does not occur.

Learn about BlueXP ransomware protection.

Known limitations of NetApp Ransomware Resilience

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

Readiness drill Reset option issue

If you select an ONTAP 9.11.1 volume for the ransomware attack readiness drill, Ransomware Resilience sends an alert. If you recover the data using the "clone-to-volume" option and reset the drill, the reset operation fails.

Amazon FSx for NetApp ONTAP limitations

The Amazon FSx for NetApp ONTAP system is supported in Ransomware Resilience. The following limitations apply to this system:

- Backup policies are not supported for Fsx for ONTAP. In this environment, you should perform backup operations using the Amazon FSx for backups. You can restore these workloads using Ransomware Resilience.
- Restore operations are performed from snapshots only.

Get started

Learn about NetApp Ransomware Resilience

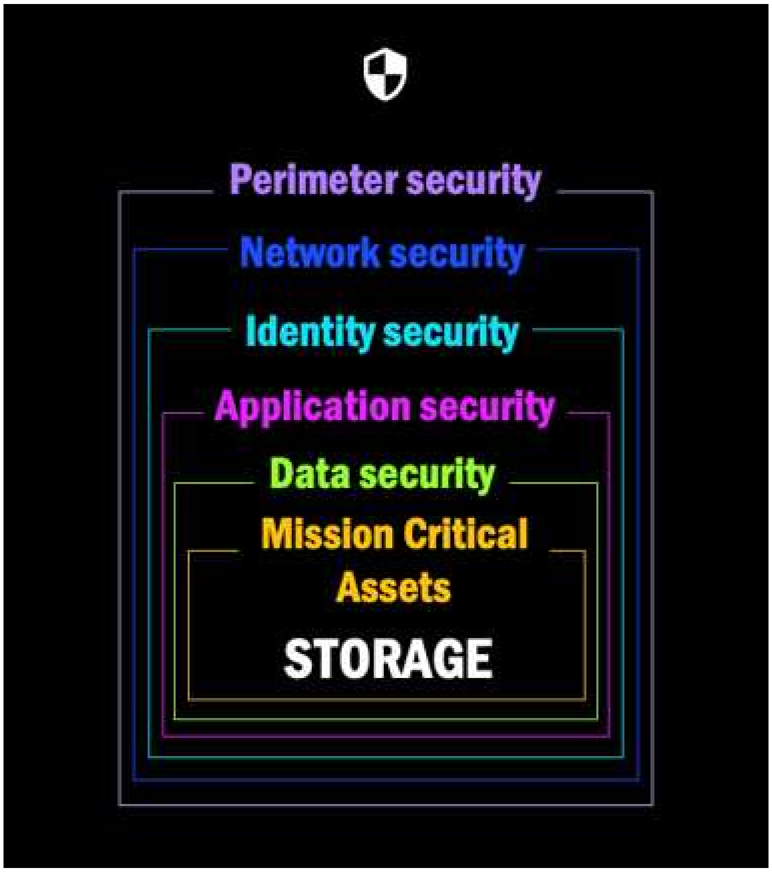
Ransomware attacks can block access to your data and attackers can ask for ransom in exchange for the release of data or decryption. According to the IDC, it is not uncommon for victims of ransomware to experience multiple ransomware attacks. The attack can disrupt access to your data for anywhere from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

NetApp Ransomware Resilience protects your data from ransomware attacks. In Ransomware Resilience, protection is available for application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage (using the NFS and CIFS protocols) and SAN storage (FC, iSCSI, and NVMe) as well as Cloud Volumes ONTAP for Amazon Web Services, Cloud Volumes ONTAP for Google Cloud, Cloud Volumes ONTAP for Microsoft Azure, and Amazon FSx for NetApp ONTAP across the NetApp Console. You can back up data to Amazon Web Services, Google Cloud, Microsoft Azure cloud storage, and NetApp StorageGRID.

Ransomware Resilience at the data layer

Your security posture typically encompasses multiple layers of defense to protect against a range of cyber threats.

- **Outermost layer**: This is your first line of defense using firewalls, intrusion detection systems, and virtual private networks to safeguard network boundaries.
- **Network security**: This layer builds upon the foundation with network segmentation, traffic monitoring, and encryption.
- **Identity security**: Uses authentication methods, access controls, and identity management to ensure only authorized users can access sensitive resources.
- **Application security**: Protects software applications using secure coding practices, security testing, and runtime application self-protection.
- **Data security**: Safeguards your data with data protection, backups, and recovery strategies. Ransomware Resilience operates on this layer.



What you can do with Ransomware Resilience

Ransomware Resilience 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 (NFS or CIFS) and SAN (FC, iSCSI, and NVMe) systems across the NetApp Console, projects, and Console agents. Ransomwware Resilience categorizes the data priority and provides recommendations to you for ransomware resilience improvements.
- **Protect** your workloads by enabling backups, snapshot copies, and ransomware protection strategies on your data.
- **Detect** anomalies that might be ransomware attacks. [1]
- **Respond** to potential ransomware attacks by automatically initiating a tamper-proof NetApp ONTAP snapshot that is locked so that the copy cannot be deleted accidentally or maliciously. Your backup data will stay immutable and protected end to end from ransomware attacks at the source and in the destination.
- **Recover** your workloads that help accelerate workload uptime by orchestrating several NetApp technologies. You can choose to recover specific volumes. Ransomware Resilience provides recommendations on the best options.
- **Govern**: Implement your ransomware protection strategy and monitor the outcomes.

Benefits of using Ransomware Resilience

Ransomware Resilience offers the following benefits:

- Discovers workloads and their existing snapshot and backup schedules, 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. Ransomware Resilience orchestrates recovery from ransomware incidents by using several NetApp recovery services, including NetApp Backup and Recovery (formerly Cloud Backup) and SnapCenter.
- Uses role-based access control (RBAC) to govern access to features and operations.

Cost

NetApp doesn’t charge you for using the trial version of Ransomware Resilience.

> ⓘ With the October 2024 release, new deployments of Ransomware Resilience offer a 30-day free trial. Previously, Ransomware Resilience provided a 90-day free trial. If you’ve enrolled already in the 90-day free trial, that trial is valid for the 90 days.

If you have both Backup and Recovery and Ransomware Resilience, any common data protected by both products is billed by Ransomware Resilience only.

After you purchase a license or PayGo subscription, any workload that has a ransomware detection policy (Autonomous Ransomware Protection) enabled (discovered or set by Ransomware Resilience), and at least one snapshot or backup policy, Ransomware Resilience classifies it "Protected" and it counts against purchased capacity or the PayGo subscription. If a workload is discovered without a detection policy even if it has backup or snapshot policies, it is classified “At risk” and it does *not* count against purchased capacity.

Protected workloads count against purchased capacity or the subscription after the 90-day trial period ends. Ransomware Resilience is charged on a per GB basis for the data associated with protected workloads before efficiencies.

Licensing

With Ransomware Resilience, you can use different licensing plans including a free trial, a pay-as-you-go subscription, or bring your own license.

Ransomware Resilience requires a NetApp ONTAP One license.

The Ransomware Resilience license does not include additional NetApp products. Ransomware Resilience can use Backup and Recovery even if you don’t have a license for it.

To detect anomalous user behavior, Ransomware Resilience uses NetApp Autonomous Ransomware Protection, a machine learning (ML) model within ONTAP that detects malicious file activity. This model is included in the Ransomware Resilience license. You can additionally use Data Infrastructure Insights (formerly Cloud Insights) Workload Security (license required) to investigate user behavior and block specific users from further activity.

For details, see Set up licensing.

NetApp Console

Ransomware Resilience is accessible through the NetApp Console.

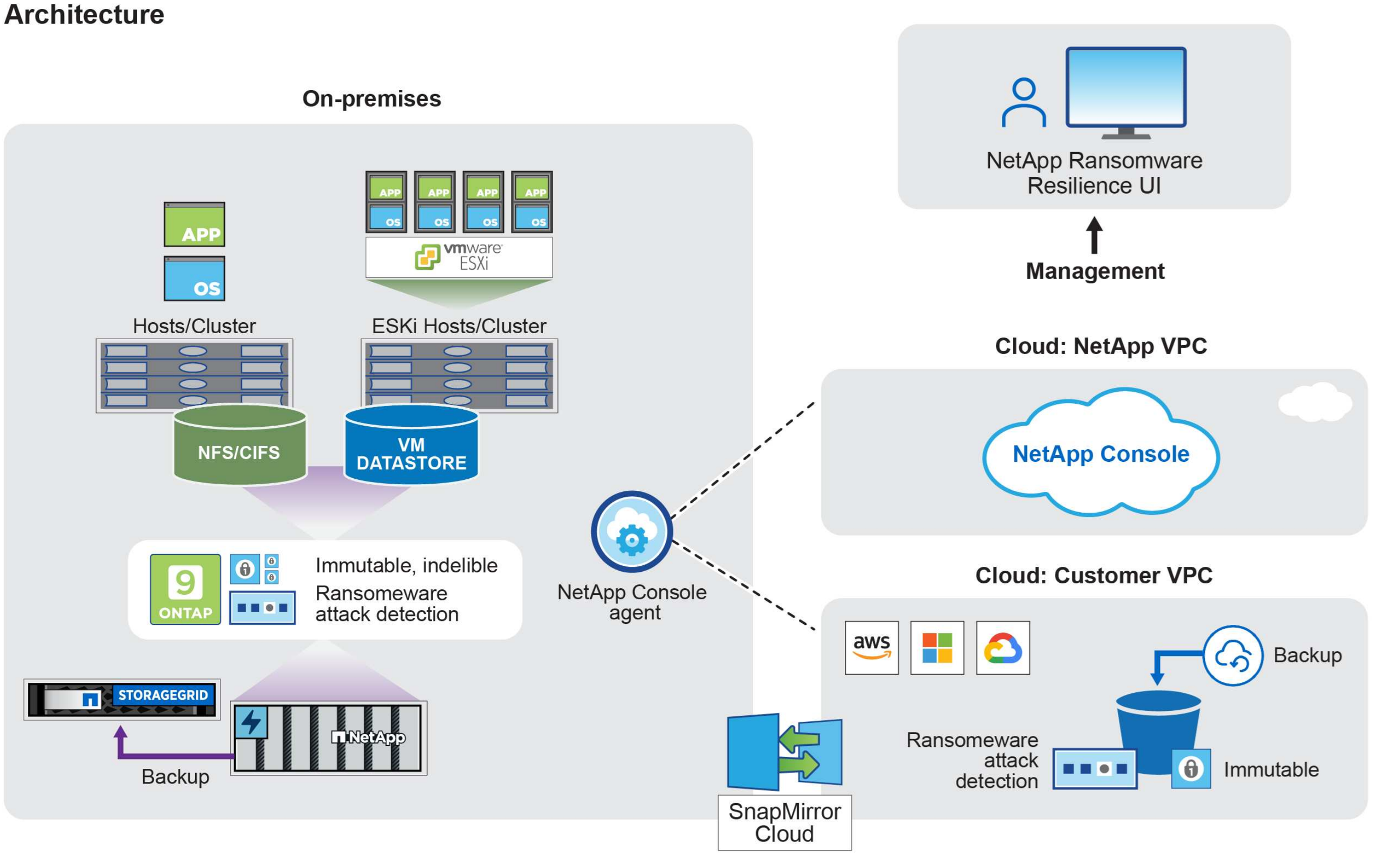
The NetApp Console provides centralized management of NetApp storage and data services across on-premises and cloud environments at enterprise grade. The Console is required to access and use NetApp data services. As a management interface, it enables you to manage many storage resources from one interface. Console administrators can control access to storage and services for all systems within the enterprise.

You don't need a license or subscription to start using NetApp Console and you only incur charges when you need to deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

Learn more about the NetApp Console.

How Ransomware Resilience works

Ransomware Resilience uses NetApp Backup and Recovery to discover and set snapshot and backup policies for file share workloads, and SnapCenter or SnapCenter for VMware to discover and set snapshot and backup policies for application and VM workloads. In addition, Ransomware Resilience uses Backup and Recovery and SnapCenter / SnapCenter for VMware to perform file- and workload-consistent recovery.



Feature	Description
IDENTIFY	• Finds all customer on-premises NAS (NFS and CIFS protocols), SAN (FC, iSCSI, and NVMe), and Cloud Volumes ONTAP data connected to the Console. • Identifies customer data from ONTAP and SnapCenter 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. Ransomware Resilience then associates this protection posture with the workloads by using Backup andRrecovery, ONTAP services, and NetApp technologies such as Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version), FPolicy, Backup policies, and snapshot policies. Learn more about Autonomous Ransomware Protection, NetApp Backup and Recovery, 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. Workload priority is based on snapshot frequencies already applied to each volume associated with the workload.
PROTECT	• Actively monitors workloads and orchestrates the use of Backup and Recovery, SnapCenter, and ONTAP APIs by applying policies to each of the identified workloads.
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. Ransomware Resilience 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 (ARP or ARP/AI depending on your ONTAP version), Data Infrastructure Insights (formerly Cloud Insights) Workload Security, 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 (ARP or ARP/AI depending on your ONTAP version), and FPolicy.
RECOVER	• Determines the best snapshot or backup and recommends the best recovery point actual (RPA) by using Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version), and FPolicy technologies and services. • Orchestrates the recovery of workloads including VMs, file shares, block storage, and databases with application consistency.

Feature	Description
GOVERN	• Assigns the ransomware protection strategies • Helps you monitor the outcomes.

Supported backup targets, systems, and workload data sources

Ransomware Resilience supports the following backup targets, systems, and data sources:

Supported backup targets

- Amazon Web Services (AWS) S3
- Google Cloud Platform
- Microsoft Azure Blob
- NetApp StorageGRID

Supported systems

- On-premises ONTAP NAS (using NFS and CIFS protocols) with ONTAP version 9.11.1 and greater
- On-premises ONTAP SAN (using FC, iSCSI, and NVMe protocols) with ONTAP version 9.17.1 and greater
- Cloud Volumes ONTAP 9.11.1 or greater for AWS (using NFS and CIFS protocols)
- Cloud Volumes ONTAP 9.11.1 or greater for Google Cloud Platform (using NFS and CIFS protocols)
- Cloud Volumes ONTAP 9.12.1 or greater for Microsoft Azure (using NFS and CIFS protocols)
- Cloud Volumes ONTAP 9.17.1 or greater for AWS, Google Cloud Platform, and Microsoft Azure (using FC, iSCSI, and NVMe protocols)
- Amazon FSx for NetApp ONTAP, which uses Autonomous Ransomware Protection (ARP and not ARP/AI)

  ⓘ ARP/AI requires ONTAP 9.16 or greater.

ⓘ The following are not supported: FlexGroup volumes, ONTAP versions older than 9.11.1, mount point volumes, mount path volumes, offline volumes, and Data protection (DP) volumes.

Supported workload data sources

Ransomware Resilience protects the following application-based workloads on primary data volumes:

- NetApp file shares
- Block storage
- VMware datastores
- Databases (MySQL and Oracle)
- More coming soon

In addition, if you are using SnapCenter or SnapCenter for VMware, all workloads supported by those products are also identified in Ransomware Resilience. Ransomware Resilience can protect and recover these in a workload-consistent manner.

Terms that might help you with ransomware protection

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

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

NetApp Ransomware Resilience prerequisites

Get started with NetApp Ransomware Resilience by verifying the readiness of your operational environment, login, network access, and web browser.

To use Ransomware Resilience, you'll need the prerequisites.

In the NetApp Console

- A NetApp Console user account with Organization Admin privileges for discovering resources.
- A Console organization with at least one active Console agent connecting to on-premises ONTAP clusters or to Cloud Volumes ONTAP in AWS or in Azure.
- The Console agent must have the `cloudmanager-ransomware-protection` container in an active state.
- At least one Console system with a NetApp on-premises ONTAP cluster or Cloud Volumes ONTAP in AWS or Azure. Ransomware Resilience supports both NAS (NFS and SMB) and SAN (iSCSI, FC, and NVMe) protocols.
    - ONTAP or Cloud Volumes ONTAP clusters with ONTAP OS version 9.11.1 or greater are supported.

      ⓘ SAN workloads are supported only in ONTAP 9.17.1 and later.

    - If your on-premises ONTAP clusters or Cloud Volumes ONTAP in AWS or in Azure cloud are not already onboarded in the Console, you need a Console agent.

      Refer to Learn how to configure a Console agent and standard Console requirements.

      ⓘ If you have multiple Console agents in a single Console organization, the Ransomware Resilience will scan ONTAP resources across all Console agents beyond the one that is currently selected in the Console UI.

In ONTAP 9.11.1 and later

- An ONTAP One license is enabled on the on-premises ONTAP instance.
- A license for NetApp Autonomous Ransomware Protection, used by Ransomware Resilience, enabled on the on-premises ONTAP instance, depending on the version of ONTAP you are using. Refer to Autonomous Ransomware Protection overview.

> The general release of Ransomware Resilience, unlike the Preview release, includes a license for NetApp Autonomous Ransomware Protection technology. Refer to Autonomous Ransomware Protection overview for details.

For more licensing details, refer to Learn about Ransomware Resilience.

- To apply protection configurations (such as enabling Autonomous Ransomware Protection and others), Ransomware Resilience needs admin permissions on the ONTAP cluster. The ONTAP cluster should have been onboarded using ONTAP cluster admin user credentials only.
- If the ONTAP cluster is already onboarded in the Console using non-admin user credentials, then the non-admin user permissions must be updated with necessary permissions by logging into the ONTAP cluster, described on this page.

For data backups

- An account in NetApp StorageGRID, AWS S3, Azure Blob, or Google Cloud Platform for backup targets and the access permissions set.

  Refer to the AWS, Azure, or S3 permissions list for details.

- NetApp Backup and Recovery does not need to be enabled on the system.

  Ransomware Resilience helps configure a backup destination through the Settings option. See Configure settings.

Update non-admin user permissions in an ONTAP system

If you need to update non-admin user permissions for a particular system, complete these steps.

1. Log in to the Console and look for the system that needs its ONTAP user permissions updated.
2. Select the system to see details.
3. Select **View additional information** to display the username.
4. Log in to the ONTAP cluster CLI using the admin user.
5. Display the existing roles for that user. Enter:

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

6. Change the role for the user. Enter:

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

7. Return to the Ransomware Resilience UI to use it.

Quick start for NetApp Ransomware Resilience

Here’s an overview of the steps needed to get started with NetApp Ransomware Resilience. The links within each step take you to a page that provides more details.

1 **Review prerequisites**

Ensure your system meets these requirements.

2 **Set up Ransomware Resilience**

- Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform, or Microsoft Azure as a backup destination.
- Configure a Console agent.
- Set up licensing.
- Discover workloads in the Console.
- Configure backup destinations.
- Optionally enable threat detection.
- Optionally, conduct a ransomware attack readiness drill.

3 **What’s next?**

After you set up Ransomware Resilience, 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 NetApp Ransomware Resilience

You can easily deploy NetApp Ransomware Resilience. 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
- Google Cloud Platform
- Microsoft Azure

After you configure options in the backup destination itself, you will later configure it as a backup destination in

Ransomware Resilience. For details about how to configure the backup destination in Ransomware Resilience, refer to Configure backup destinations.

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 the Console, refer to Manage your Amazon S3 buckets.

Prepare Azure to become a backup destination

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

For details about managing your Azure storage in the Console, refer to Manage your Azure storage accounts.

Set up the NetApp Console

The next step is to set up the Console and Ransomware Resilience.

Review Console requirements for standard mode.

Create a Console agent

Contact your NetApp Sales Rep to try out or use this service. Then, when you use the Console agent, it will include the appropriate capabilities for Ransomware Resilience.

To create a Console agent using Ransomware Resilience, contact your Console organization admin who has permissions to create Console agents, and refer to the documentation that describes how to create a Console agent.

> ⓘ If you have multiple Console agents, the Ransomware Resilience scan datas across all Console agents beyond the one that currently shows in the Console. This service discovers all projects and all Console agents associated with this organization.

Access NetApp Ransomware Resilience

Log in to NetApp Ransomware Resilience through the NetApp Console.

To log in to the Console, 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.

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 BlueXP access roles for all services.

Steps

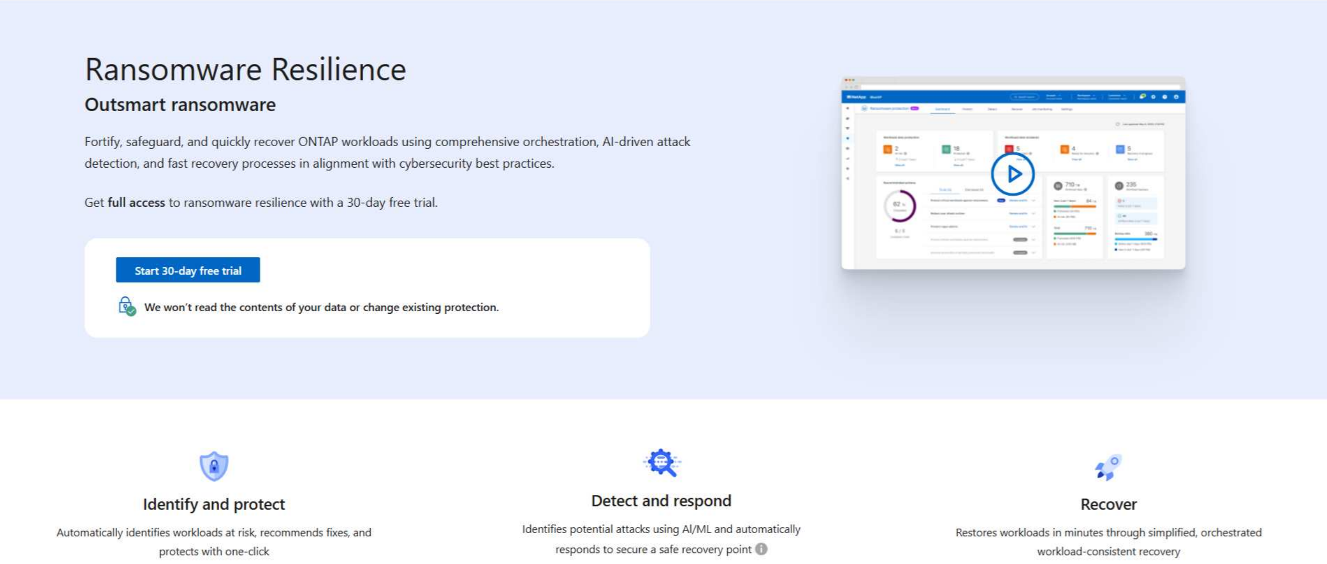
1. Open a web browser and go to the Console.

   The Console login page appears.

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

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

   > If you don’t have a Console agent or it’s not the one for this service, you need to deploy one. Learn how to set up a Console agent.

   Ransomware Resilience

   Outsmart ransomware

   Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

   Get **full access** to ransomware resilience with a 30-day free trial.

   Start 30-day free trial

   We won’t read the contents of your data or change existing protection.

   Identify and protect

   Automatically identifies workloads at risk, recommends fixes, and protects with one-click

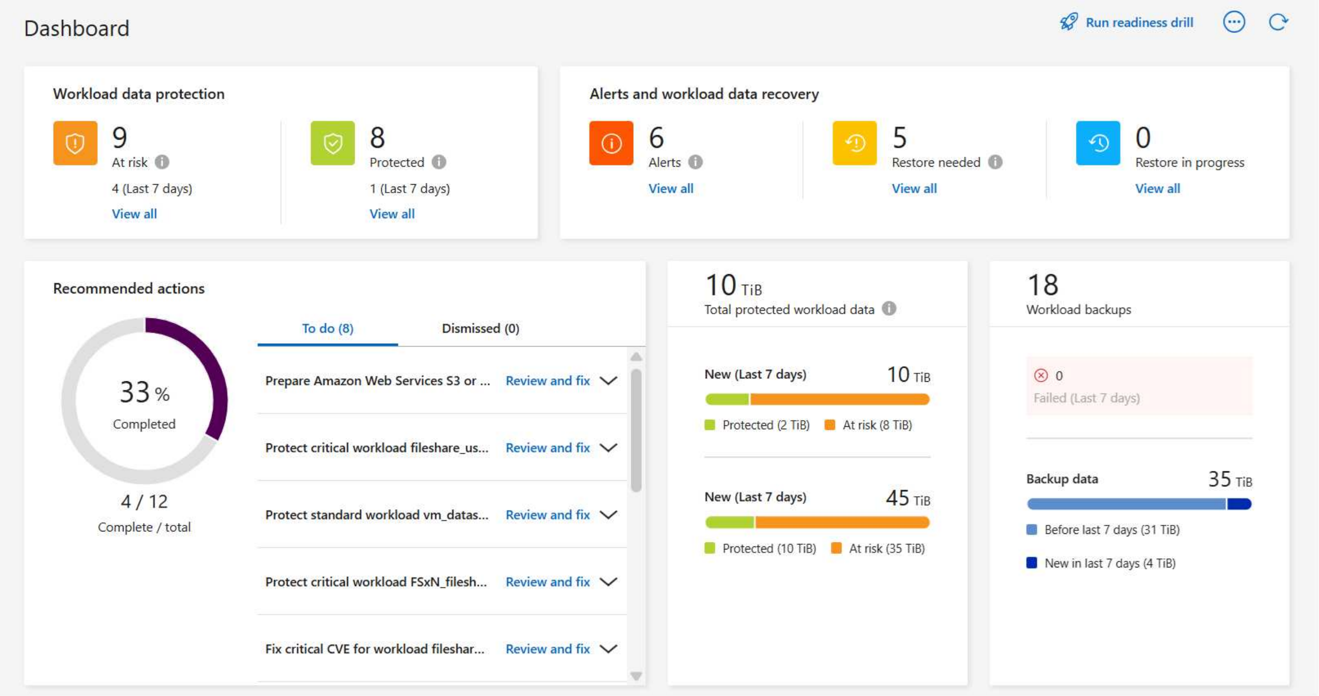
   Detect and respond

   Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

   Recover

   Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

   Otherwise, the Ransomware Resilience dashboard appears.



4. If you haven't done so already, select the **Discover Workloads** option.

   Refer to Discover Workloads.

Set up licensing for NetApp Ransomware Resilience

With NetApp Ransomware Resilience, you can use different licensing plans.

To perform this task, you need the Organization admin, Folder or project admin role. Learn about Console access roles.

License types
You can use the following license types:

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription with Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace, or Azure Marketplace.
- Bring your own license (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in the Console.

After you set up your BYOL or purchase a PAYGO subscription, you can see the license in the Licenses and subscriptions section of the Console.

After the free trial ends or the license or subscription expires, you can still do the following in Ransomware Resilience:

- View workloads and workload health.
- Delete any resource, such as a policy.
- Run all scheduled operations that were created during the trial period or under the license.

Other licenses

The Ransomware Resilience license does not include additional NetApp products. Ransomware Resilience can use NetApp Backup and Recovery even if you don't have a license for it.

> ⓘ If you have both Backup and Recovery and Ransomware Resilience, any common data protected by both products will be billed by Ransomware Resilience only.

You can view anomalous user behavior with Data Infrastructure Insights Workload Security. This requires a license for Data Infrastructure Insights Workload Security and that you enable it in Ransomware Resilience. For an overview of Data Infrastucture Insights Workload Security, review About Workload Security

> 💡 If you don't have a license for Data Infrastructure Insights Workload Security and don't enable it in Ransomware Resilience, you won't see the anomalous user behavior information.

Try it out using a 30-day free trial

You can try Ransomware Resilience out by using a 30-day free trial. You must be an Console Organization administrator to start the free trial.

> ⓘ With the October 2024 release, new deployments of Ransomware Resilience now have 30 days for a free trial. Previously, Ransomware Resilience provided 90 days as a free trial. If you are already in the 90-day free trial, that offer continues for the 90 days.

No capacity limits are enforced during the trial.

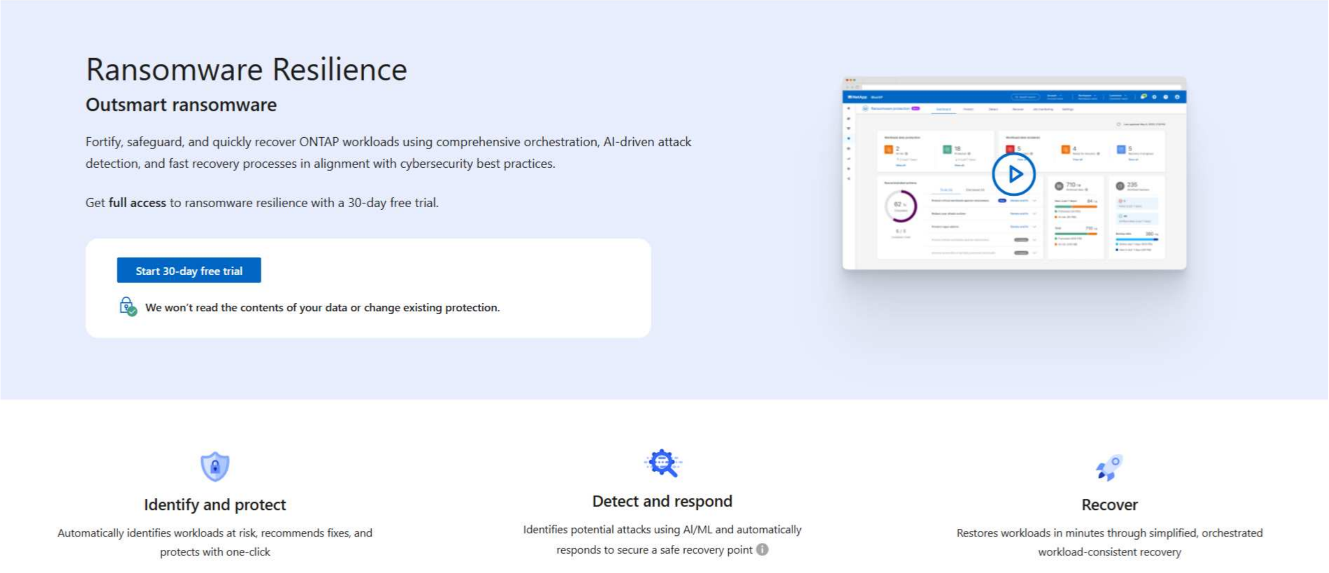
You can get a license or subscribe at any time and you will not be charged until the 30-day trial ends. To continue after the 30-day trial, you'll need to purchase a BYOL license or PAYGO subscription.

During the trial, you have full functionality.

Steps

1. Access the Console.
2. Log in to the Console.
3. From the NetApp Console, select **Protection** > **Ransomware Resilience**.

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



Ransomware Resilience

Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

Start 30-day free trial

We won't read the contents of your data or change existing protection.

Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

4. If you haven't already added a Connector for other services, add one.

   To add a Console agent, refer to Learn about Console agents.

5. After you set up a Console agent, in the Ransomware Resilience landing page, the button to add a Console agent changes to a button for discovering workloads. Select **Start by discovering workloads**.
6. To review the free trial information, select the drop-down option in the top right.

After the trial ends, obtain a subscription or license

After the free trial ends, you can either subscribe through one of the Marketplaces or purchase a license from NetApp.

If you already have a PAYGO subscription, the license is automatically switched to the subscription after the free trial ends.

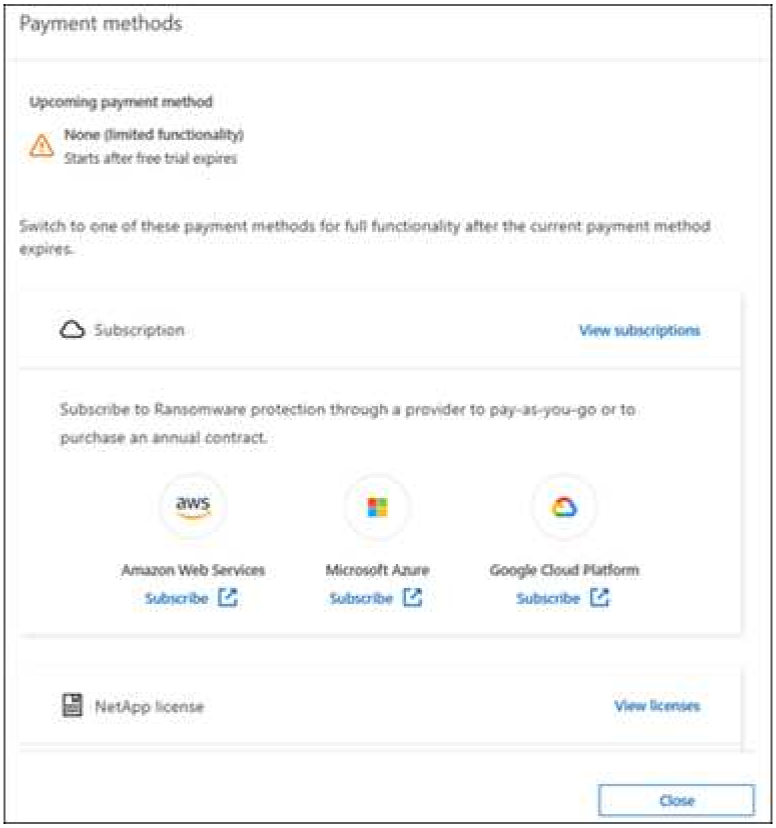
Subscribe through AWS Marketplace
Subscribe through Microsoft Azure Marketplace
Subscribe through Google Cloud Platform Marketplace
Bring your own license (BYOL)

Subscribe through AWS Marketplace

This procedure provides a high level overview of how to subscribe directly in the AWS Marketplace.

Steps

1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven't started the trial, select the **Free trial** notice at the top right then **View payment methods**.



Payment methods

Upcoming payment method

None (limited functionality)
Starts after free trial expires

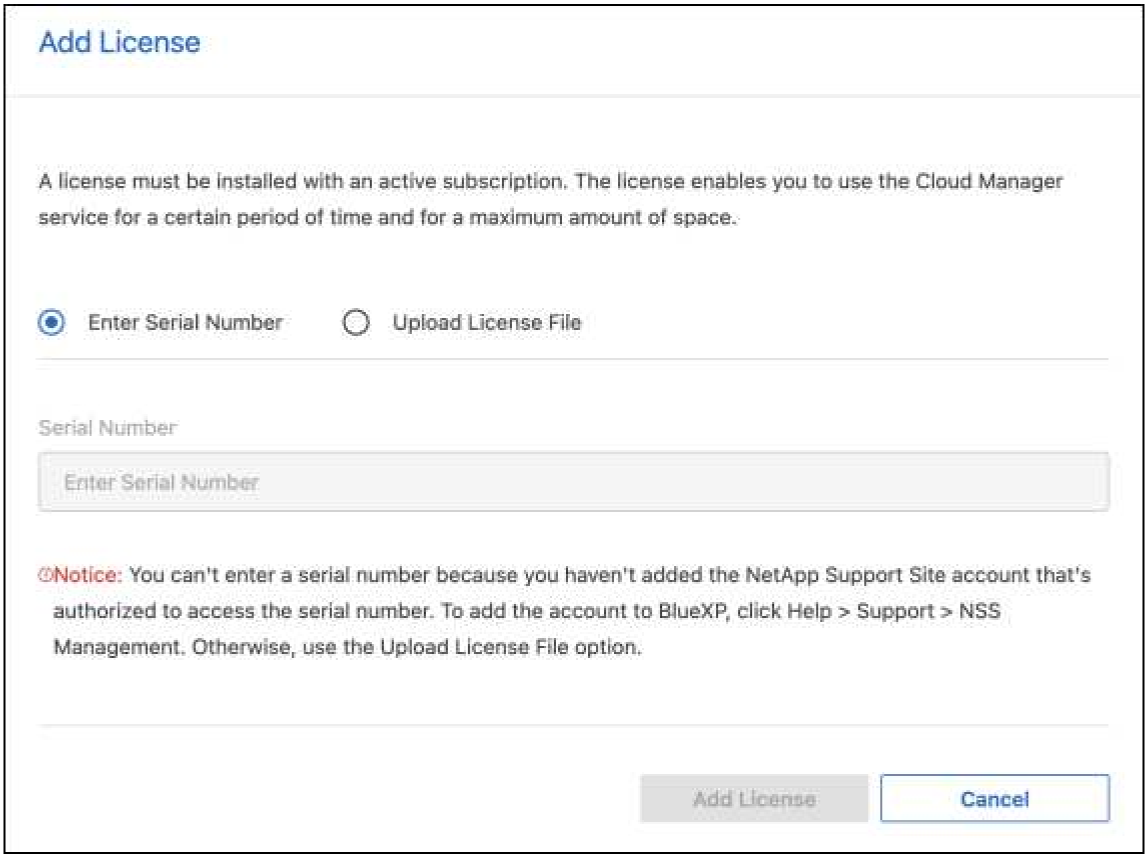
Switch to one of these payment methods for full functionality after the current payment method expires.

Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for **Amazon Web Services**.
3. In AWS Marketplace, select **View purchase options**.
4. Use AWS Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.
5. When you return to Ransomware Resilience, a message states that you are subscribed.

   ⓘ An email is sent to you that includes the Ransomware Resilience serial number, and indicates that Ransomware Resilience is subscribed in AWS Marketplace.

6. Return to the Ransomware Resilience payment methods page.
7. Add the license to the Console by selecting **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

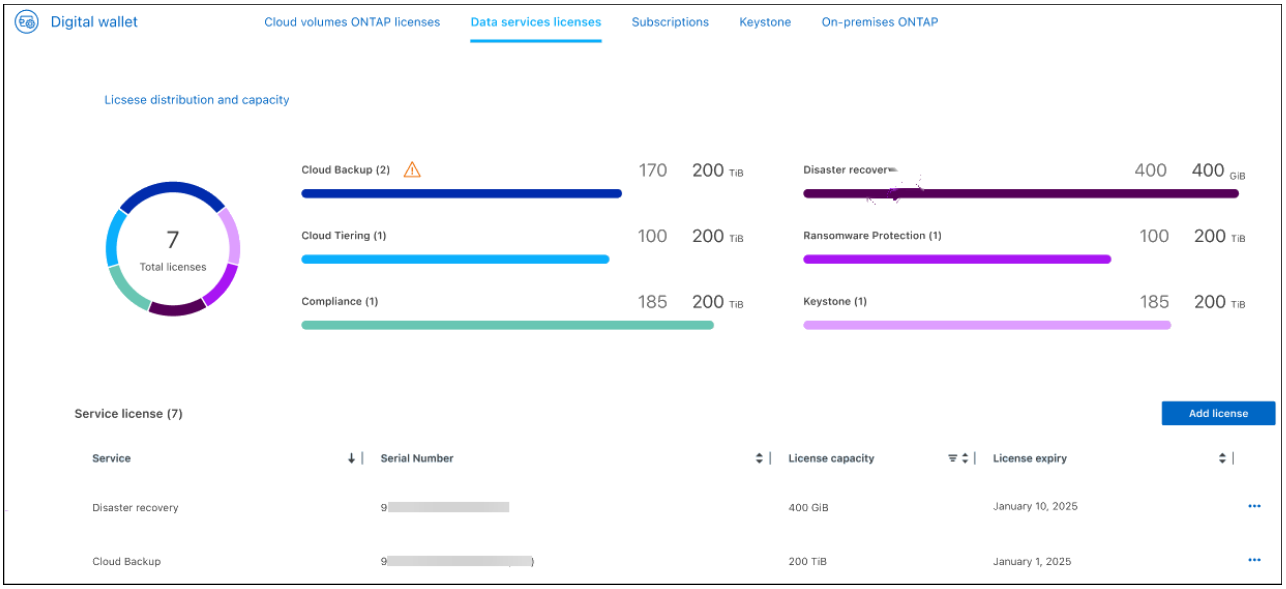
● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

ⓘNotice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number**, enter the serial number that was included in the email sent to you, and select **Add License**.
9. To view license details, from the Console left navigation, select **Administration** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.



Cloud Backup (2) ⚠ 170 200 TiB

Cloud Tiering (1) 100 200 TiB

Compliance (1) 185 200 TiB

Disaster recover 400 400 GiB

Ransomware Protection (1) 100 200 TiB

Keystone (1) 185 200 TiB

Service license (7)

Service	Serial Number	License capacity	License expiry	
Disaster recovery	9[redacted]	400 GiB	January 10, 2025	•••
Cloud Backup	9[redacted]	200 TiB	January 1, 2025	•••

10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

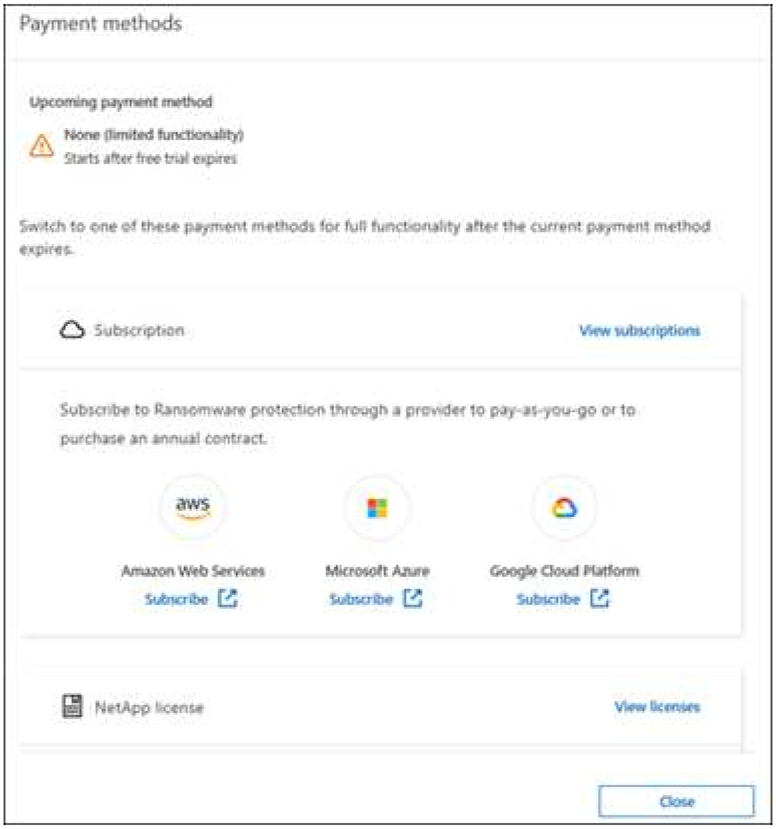
A message appears indicating that a license has been added.

Subscribe through Microsoft Azure Marketplace

This procedure provides a high level overview of how to subscribe directly in the Azure Marketplace.

Steps

1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven't started the trial, select the **Free trial** notice at the top right then **View payment methods**.



Payment methods

Upcoming payment method

None (limited functionality)

Starts after free trial expires

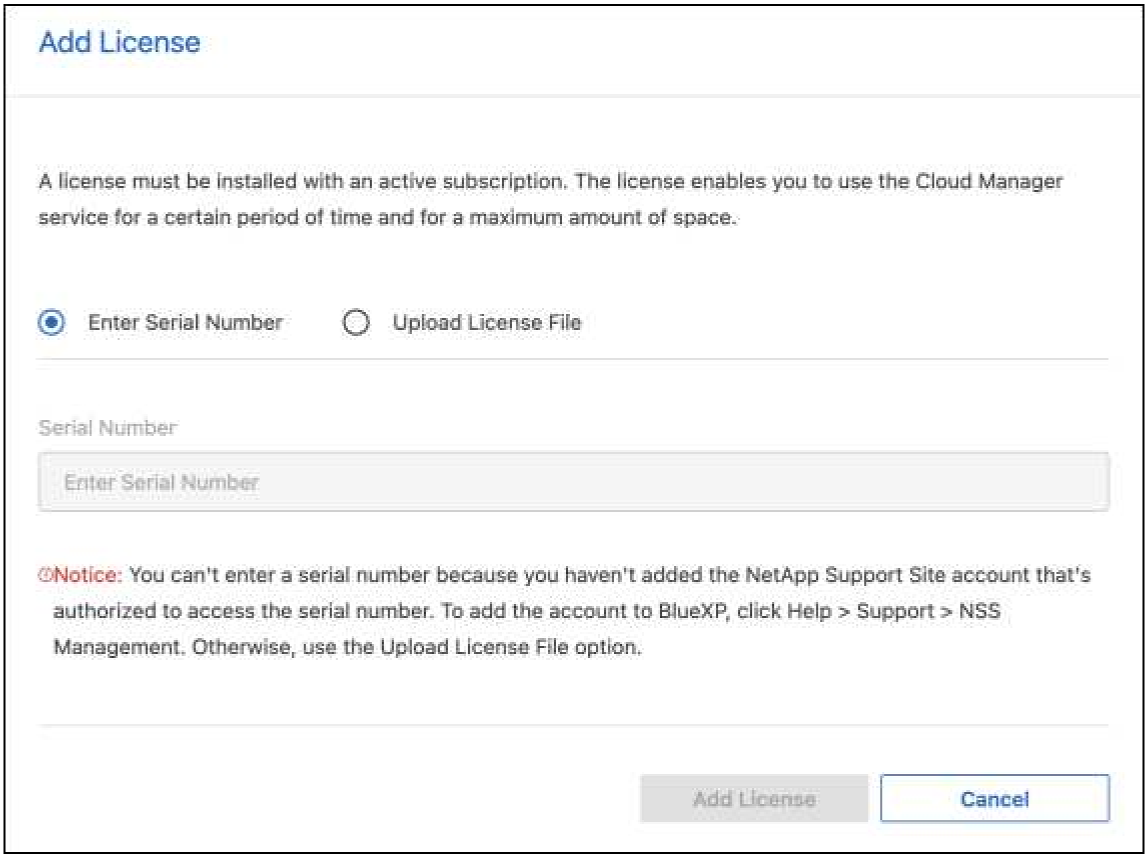
Switch to one of these payment methods for full functionality after the current payment method expires.

Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for **Microsoft Azure Marketplace**.
3. In Azure Marketplace, select **View purchase options**.
4. Use Azure Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.
5. When you return to Ransomware Resilience, a message states that you are subscribed.

   > ⓘ An email is sent to you that includes the Ransomware Resilience serial number, and indicates that Ransomware Resilience is subscribed in Azure Marketplace.

6. Return to Ransomware Resilience Payment methods page.
7. To add the license, select **Add a license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

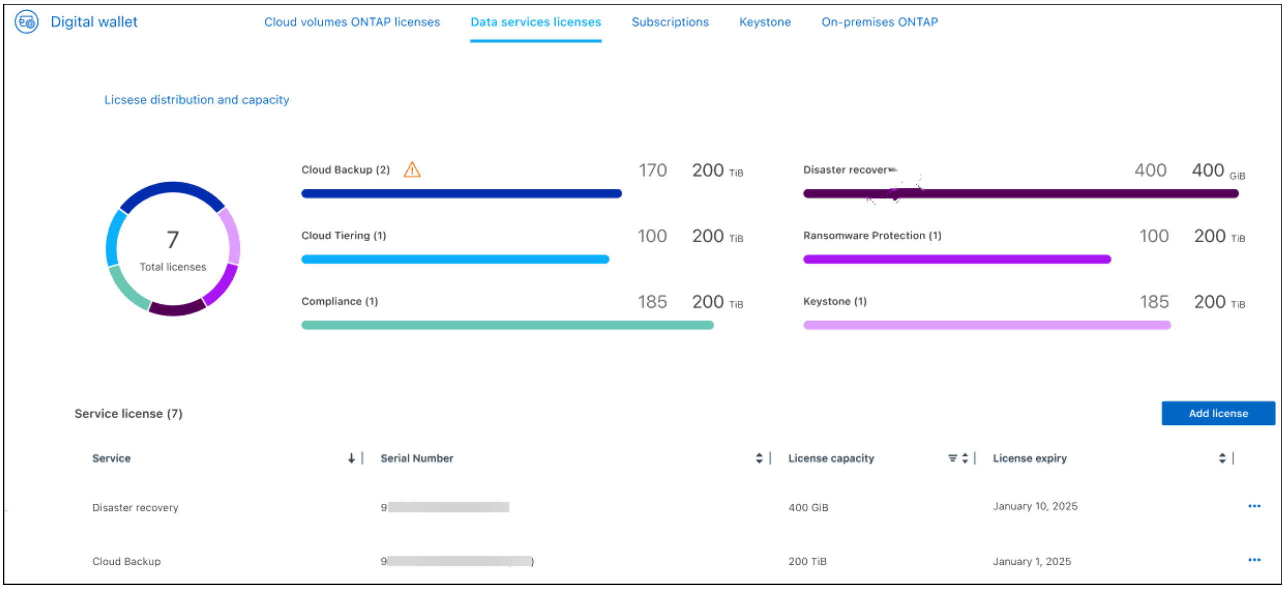
● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

ⓘNotice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number** then enter the serial number frin the email sent to you. Select **Add License**.
9. To view license details in Licenses and subscriptions, from the Console left navigation, select **Governance** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.



Digital wallet
Cloud volumes ONTAP licenses
Data services licenses
Subscriptions
Keystone
On-premises ONTAP
Licsese distribution and capacity
7
Total licenses
Cloud Backup (2) ⚠ 170 200 TiB
Cloud Tiering (1) 100 200 TiB
Compliance (1) 185 200 TiB
Disaster recover 400 400 GiB
Ransomware Protection (1) 100 200 TiB
Keystone (1) 185 200 TiB
Add license

Service license (7)

Service	Serial Number	License capacity	License expiry
Disaster recovery	9[redacted]	400 GiB	January 10, 2025
Cloud Backup	9[redacted]	200 TiB	January 1, 2025

10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

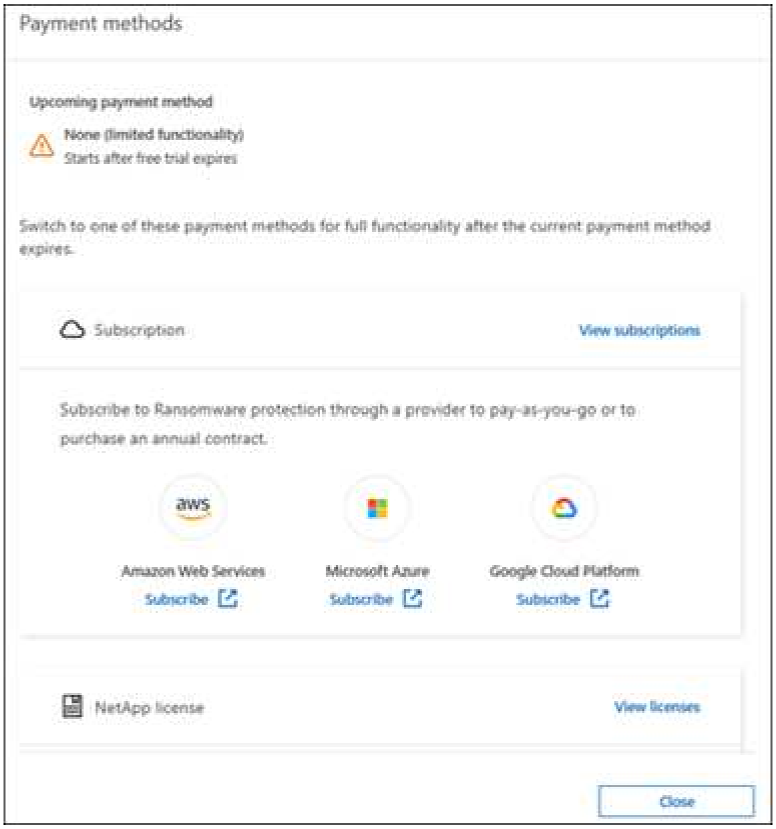
A message appears indicating that a license has been added.

Subscribe through Google Cloud Platform Marketplace

This procedure provides a high level overview of how to subscribe directly in the Google Cloud Platform Marketplace.

Steps

1. In the Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven’t started the trial, select the **Free trial** notice at the top right then **View payment methods**.

   Payment methods

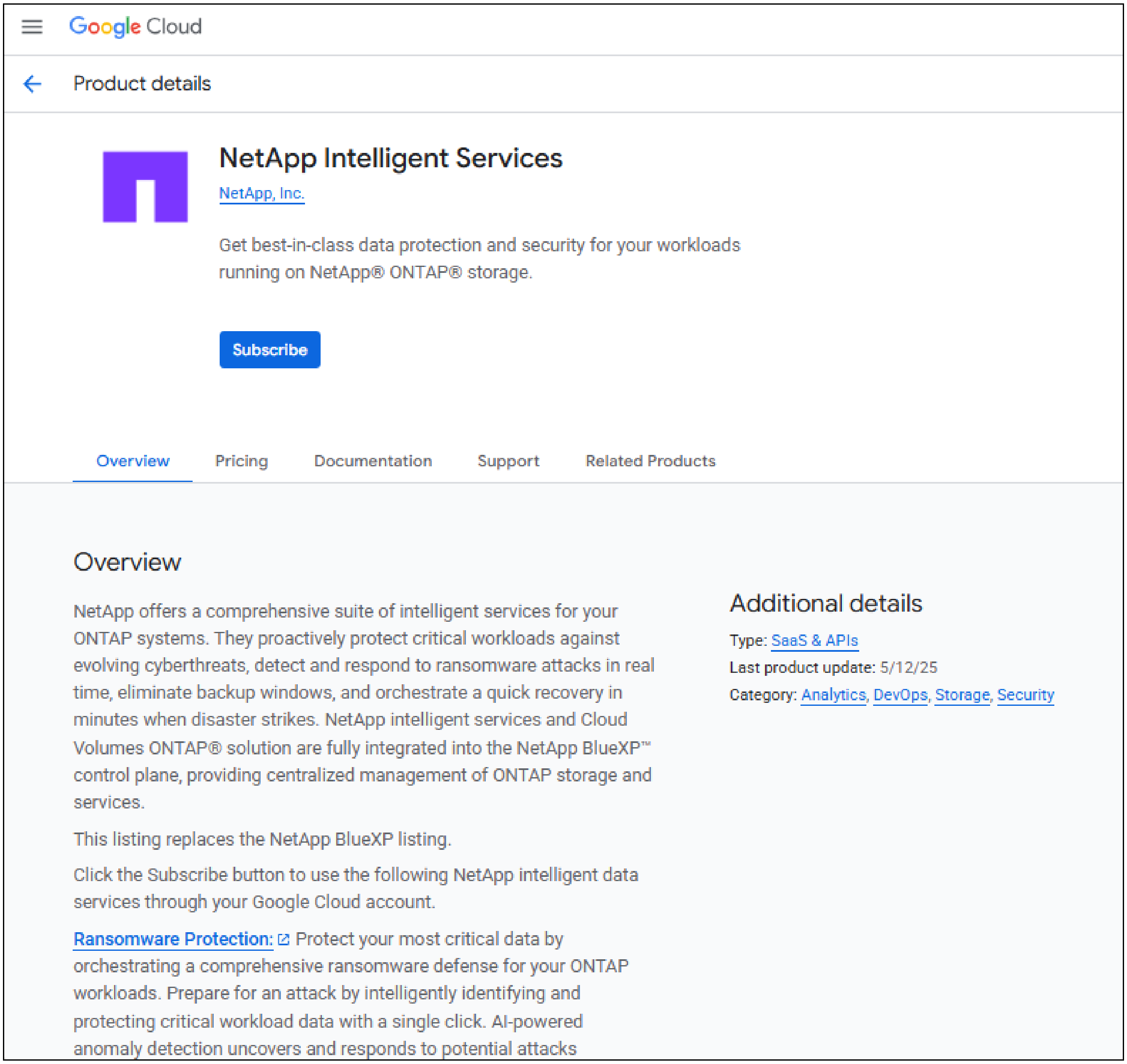
   Upcoming payment method

   None (limited functionality)
   Starts after free trial expires

   Switch to one of these payment methods for full functionality after the current payment method expires.

   Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for Google Cloud Platform Marketplace*.
3. In Google Cloud Platform Marketplace, select **Subscribe**.
4. Use Google Cloud Platform Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.



NetApp Intelligent Services

NetApp, Inc.

Get best-in-class data protection and security for your workloads running on NetApp® ONTAP® storage.

Overview

NetApp offers a comprehensive suite of intelligent services for your ONTAP systems. They proactively protect critical workloads against evolving cyberthreats, detect and respond to ransomware attacks in real time, eliminate backup windows, and orchestrate a quick recovery in minutes when disaster strikes. NetApp intelligent services and Cloud Volumes ONTAP® solution are fully integrated into the NetApp BlueXP™ control plane, providing centralized management of ONTAP storage and services.

This listing replaces the NetApp BlueXP listing.

Click the Subscribe button to use the following NetApp intelligent data services through your Google Cloud account.

Ransomware Protection: Protect your most critical data by orchestrating a comprehensive ransomware defense for your ONTAP workloads. Prepare for an attack by intelligently identifying and protecting critical workload data with a single click. AI-powered anomaly detection uncovers and responds to potential attacks

Additional details

Type: SaaS & APIs

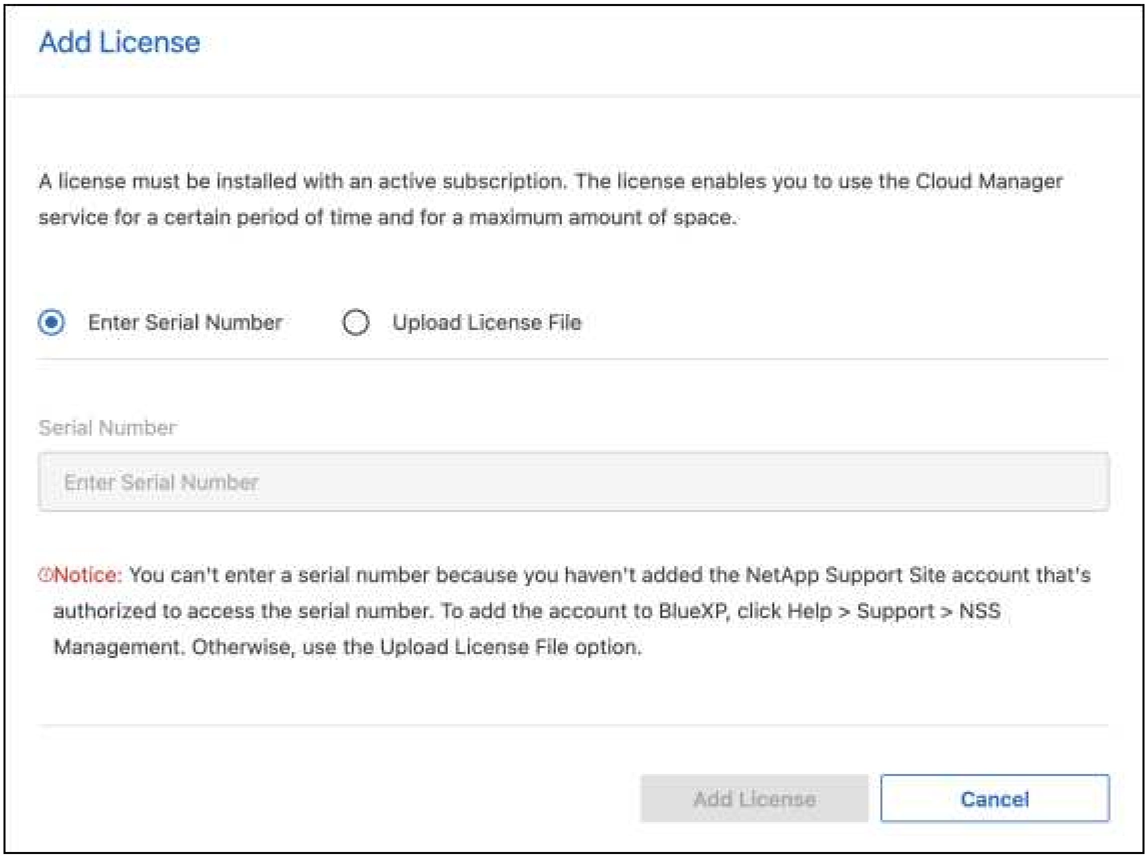
Last product update: 5/12/25

Category: Analytics, DevOps, Storage, Security

5. When you return to Ransomware Resilience, a message states that you are subscribed.

   > ⓘ An email is sent to you that includes the Ransomware Resilience serial number and indicates that Ransomware Resilience is subscribed in Google Cloud Platform Marketplace.

6. Return to Ransomware Resilience Payment methods page.
7. To add the license to the Console, select **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

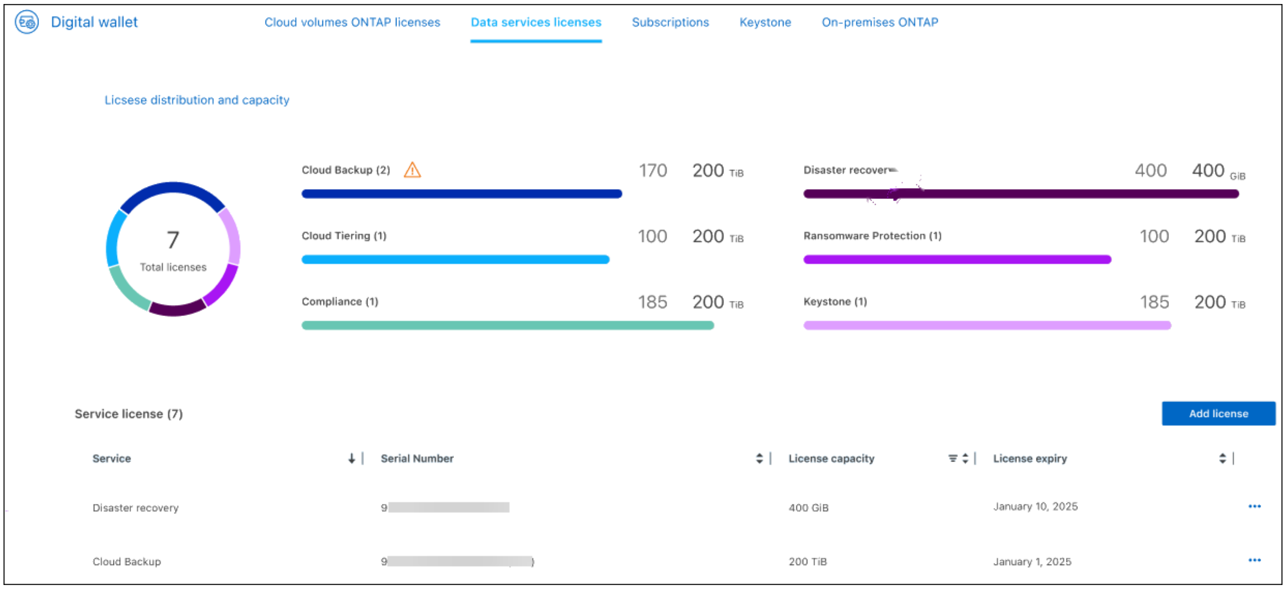
● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number**. Enter the serial number in the email sent to you. Select **Add License**.
9. To view license details, from the Console left navigation, select **Governance** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.



Cloud Backup (2) ⚠ 170 200 TiB

Cloud Tiering (1) 100 200 TiB

Compliance (1) 185 200 TiB

Disaster recover 400 400 GiB

Ransomware Protection (1) 100 200 TiB

Keystone (1) 185 200 TiB

Service license (7)

Service	Serial Number	License capacity	License expiry	
Disaster recovery	9[redacted]	400 GiB	January 10, 2025	•••
Cloud Backup	9[redacted]	200 TiB	January 1, 2025	•••

10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

A message appears indicating that a license has been added.

Bring your own license (BYOL)

If you want to bring your own license (BYOL), you need to purchase the license, get the NetApp License File (NLF), then add the license to the Console.

Add your license file to the Console

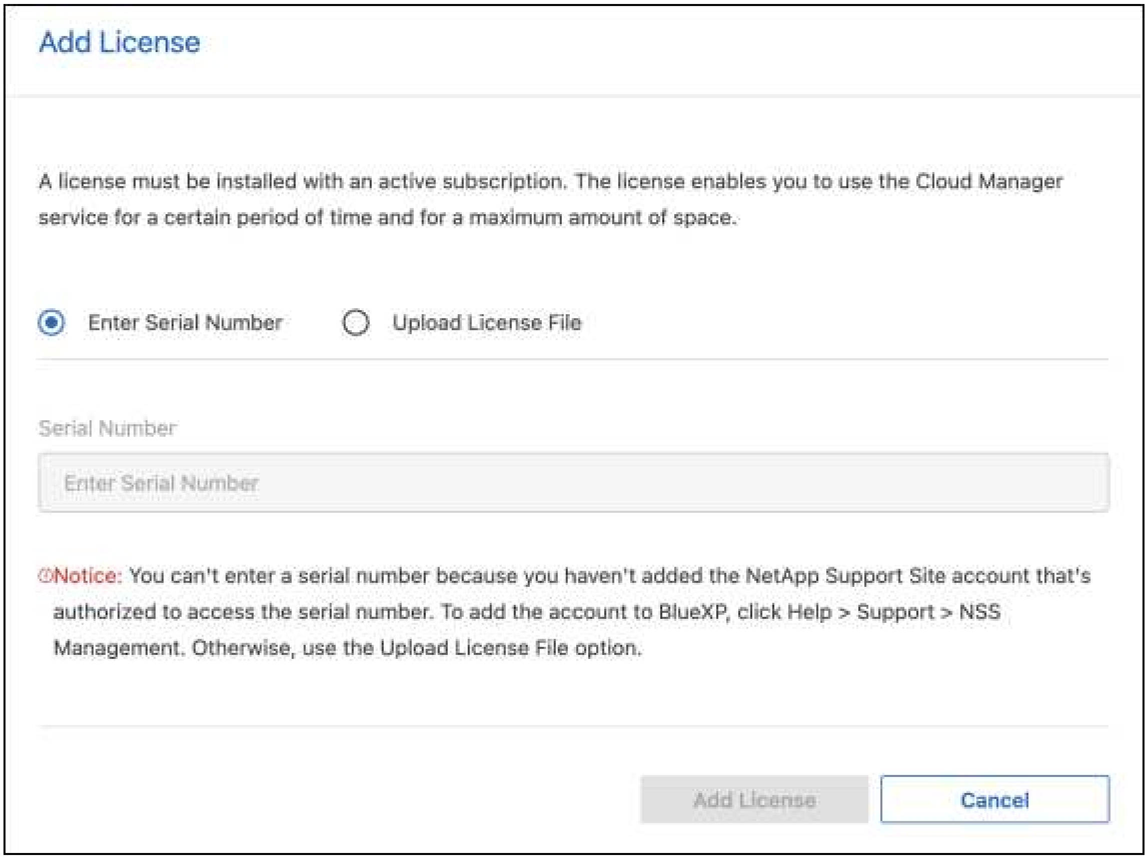
After you've purchased your Ransomware Resilience license from your NetApp sales rep, you activate the license by entering the Ransomware Resilience serial number and NetApp Support Site (NSS) account information.

Before you begin

You need the Ransomware Resilience serial number. Locate this number from your sales order, or contact the account team for this information.

Steps

1. After you obtain the license, return to Ransomware Resilience. Select the **View payment methods** option in the upper right. Or, in the message that the free trial is expiring, select **Subscribe or purchase a license**.
2. Select **Add license** to go to the Console Licesnses and subscriptions page.
3. From the **Data Services Licenses** tab, select **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

4. In the Add License page, enter the serial number and NetApp Support Site account information.
   - If you have the Console license serial number and know your NSS account, select the **Enter Serial**

Number option and enter that information.

  If your NetApp Support Site account isn't available from the drop-down list, add the NSS account to the Console.

  - If you have the zvondolr license file (required when installed in a dark site), select the **Upload License File** option and follow the prompts to attach the file.

5. Select **Add License**.

Result

The Licenses and subscriptions page shows Ransomware Resilience has a license.

Update your Console license when it expires

If your licensed term is nearing the expiration date, or if your licensed capacity is reaching the limit, you'll be notified in the Ransomware Resilience UI. You can update your Ransomware Resilience license before it expires so there's no interruption in your ability to access your scanned data.

> This message also appears in Licenses and subscriptions and in Notification settings.

Steps

1. You can send an email to support to request an update to your license.

   After you pay for the license and it is registered with the NetApp Support Site, the Console automatically updates the license. The Data Services Licenses page will reflect the change in 5 to 10 minutes.

2. If the Console can't automatically update the license, you need need to manually upload the license file.
   a. You can obtain the license file from the NetApp Support Site.
   b. In the Console, select **Administration** > **Licenses and subscriptions**.
   c. Select the **Data Services Licenses** tab, select the **Actions …** icon for the serial number you are updating then select **Update License**.

End the PAYGO subscription

If you want to end your PAYGO subscription, you can do so at any time.

Steps

1. In Ransomware Resilience, at the top right, select the license option.
2. Select **View payment methods**.
3. In the drop-down details, uncheck the box **Use after current payment method expires**.
4. Select **Save**.

Discover workloads in NetApp Ransomware Resilience

Before you can use NetApp Ransomware Resilience, it needs to first discover data. During discovery, Ransomware Resilience analyzes all volumes and files in systems across all Console agents and projects within an organization.

Required Console role

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

What does Ransomware Resilience discover?
Ransomware Resilience assesses MySQL applications, Oracle applications, VMware datastores, file shares, and block storage.

> Ransomware Resilience does not discover workloads with volumes that use FlexGroup.

Ransomware Resilience discovers and displays both supported and unsupported system configurations in the Dashboard.

Ransomware Resilience checks your current backup protection, snapshot copies, and NetApp Autonomous Ransomware Protection options. It then recommends ways to improve your ransomware protection.

How can you discover workloads?
You can do the following:

- Within each Console agent, select the systems where you want to discover workloads. You might benefit from this feature if you want to protect specific workloads in your environment and not others.
- Discover newly created workloads for previously selected systems.
- Discover new systems.

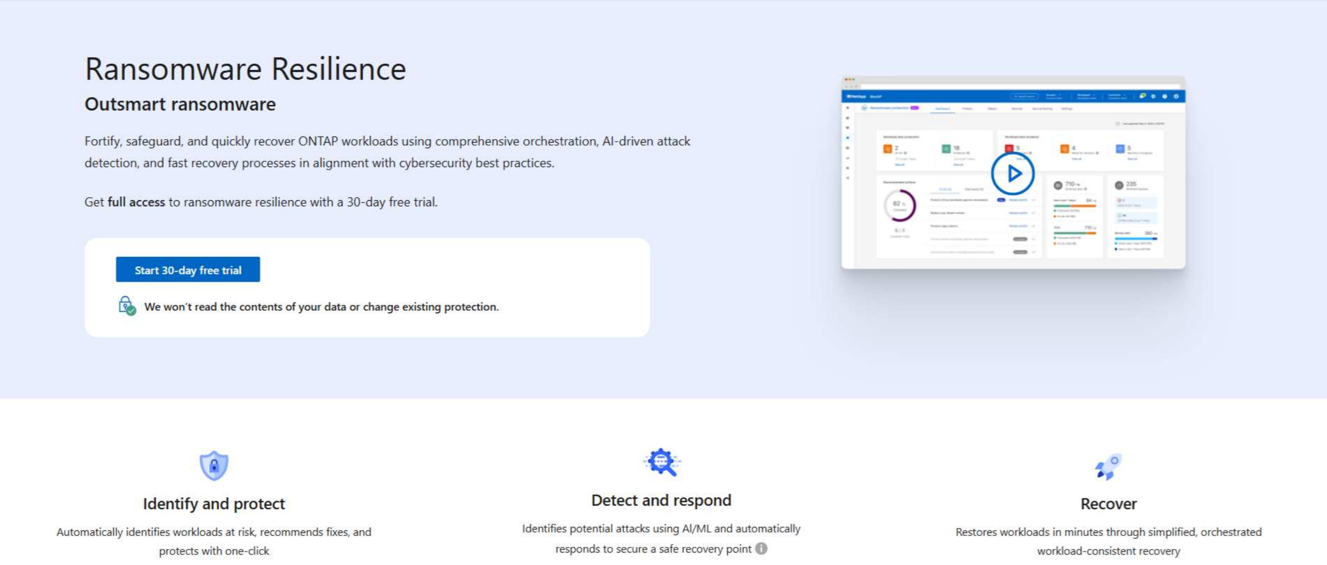
Select workloads to discover and protect

Within each Console agent, select the systems where you want to discover workloads.

Steps

1. From the NetApp Console, select **Protection** > **Ransomware protection**.

   If this is your first login, the landing page appears.



Ransomware Resilience

Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

Start 30-day free trial

We won't read the contents of your data or change existing protection.

Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

> If you started the free trial, the **Start 30-day free trial** button label changes to **Start by discovering workloads**.

2. From the initial landing page, select **Start by discovering workloads**.

   Ransomware Resilience finds both supported and unsupported systems. This process might take a few minutes.

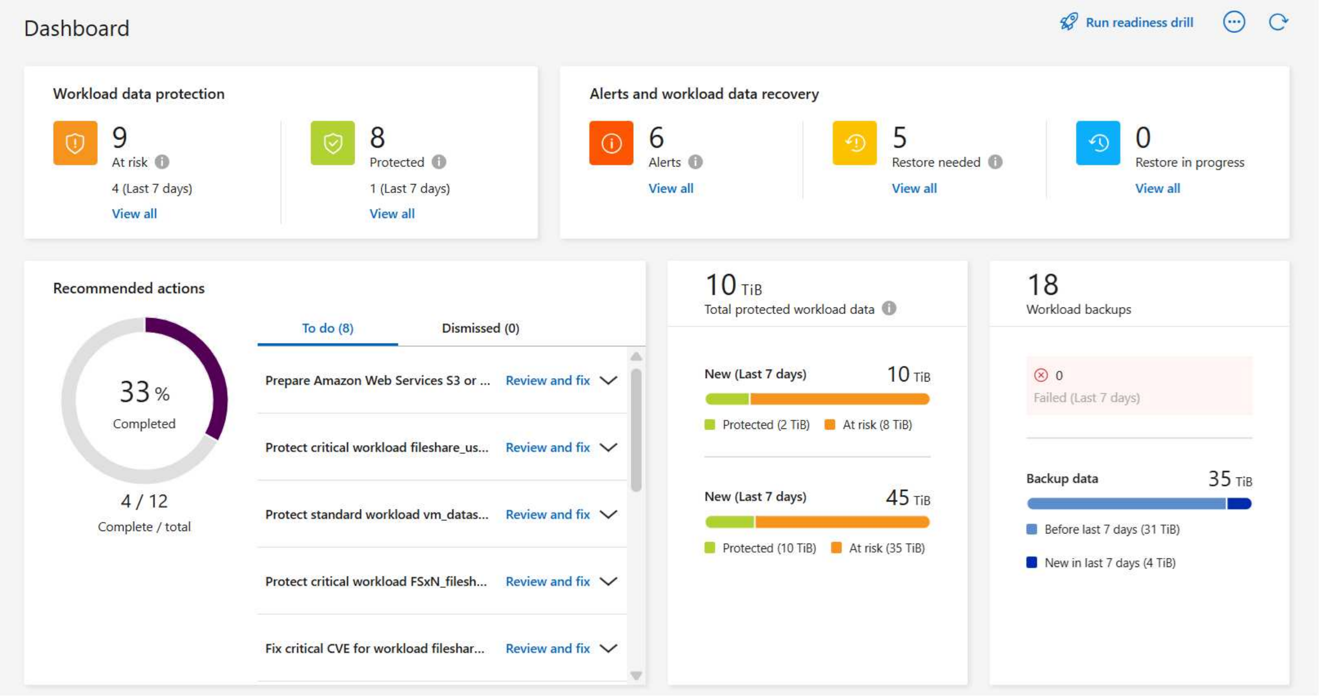
   [Discover workloads screenshot]

3. To discover workloads for a specific Console agent, select **Select systems** next to the Console agent where you want to discover workloads.
4. Select the systems where you want to discover workloads.
5. Select **Discover**.

   Ransomware Resilience discovers workload data only for those Console agents with selected systems. This process might take a few minutes.

6. To download the list of discovered workloads, select **Download results**.
7. To display the Ransomware Resilience dashboard, select **Go to Dashboard**.

   The Dashboard shows data protection health. The number of at-risk or protected workloads updates as new workloads are discovered.



Dashboard

Run readiness drill

Workload data protection

9 At risk
4 (Last 7 days)
View all

8 Protected
1 (Last 7 days)
View all

Alerts and workload data recovery

6 Alerts
View all

5 Restore needed
View all

0 Restore in progress
View all

Recommended actions

33 % Completed

4 / 12 Complete / total

To do (8) | Dismissed (0)

Prepare Amazon Web Services S3 or ...	Review and fix
Protect critical workload fileshare_us...	Review and fix
Protect standard workload vm_datas...	Review and fix
Protect critical workload FSxN_filesh...	Review and fix
Fix critical CVE for workload fileshar...	Review and fix

10 TiB
Total protected workload data

New (Last 7 days) 10 TiB
Protected (2 TiB) At risk (8 TiB)

New (Last 7 days) 45 TiB
Protected (10 TiB) At risk (35 TiB)

18
Workload backups

0
Failed (Last 7 days)

Backup data 35 TiB
Before last 7 days (31 TiB)
New in last 7 days (4 TiB)

   Learn what the Dashboard shows you.

Discover newly created workloads for previously selected systems

If you have already selected systems for discovery, you can discover newly created workloads for those environments from the Dashboard.

Steps

1. To identify the date of the last discovery, look at the date and time stamp next to **Refresh** icon at the top right of the Ransomware Resilience dashboard.

2. From the Dashboard, select the **Refresh icon** to find new workloads.

Discover new systems

If you have already discovered systems, you can find new or previously unselected ones.

Steps

1. From the Ransomware Resilience menu, select the vertical ⋮ … option at the top right. From the drop-down menu, select **Settings**.
2. In the Workload discovery card, select **Discover workloads**.

   This process might take a few minutes, and a loading icon shows the progress.

3. Ransomware Resilience discovers both supported and unsupported systems. Ransomware Resilience does not support a system if its ONTAP version is below the required version. When you hover over an unsupported system, a tooltip displays the reason. Select the systems where you want to discover workloads.
4. Select **Discover**.

Conduct a ransomware attack readiness drill in NetApp Ransomware Resilience

Run a ransomware attack readiness drill by simulating an attack on a new sample workload. Investigate the simulated attack and recover the workload. Use this feature to test alert notifications, response, and recovery. Run the drill as often as needed.

Your real workload data is not impacted.

You can run readiness drills on NFS and CIFS (SMB) workloads.

Configure a ransomware attack readiness drill

Before you run a simulation, set up a drill on the Settings page. Access the Settings page from the Actions option in the top menu.

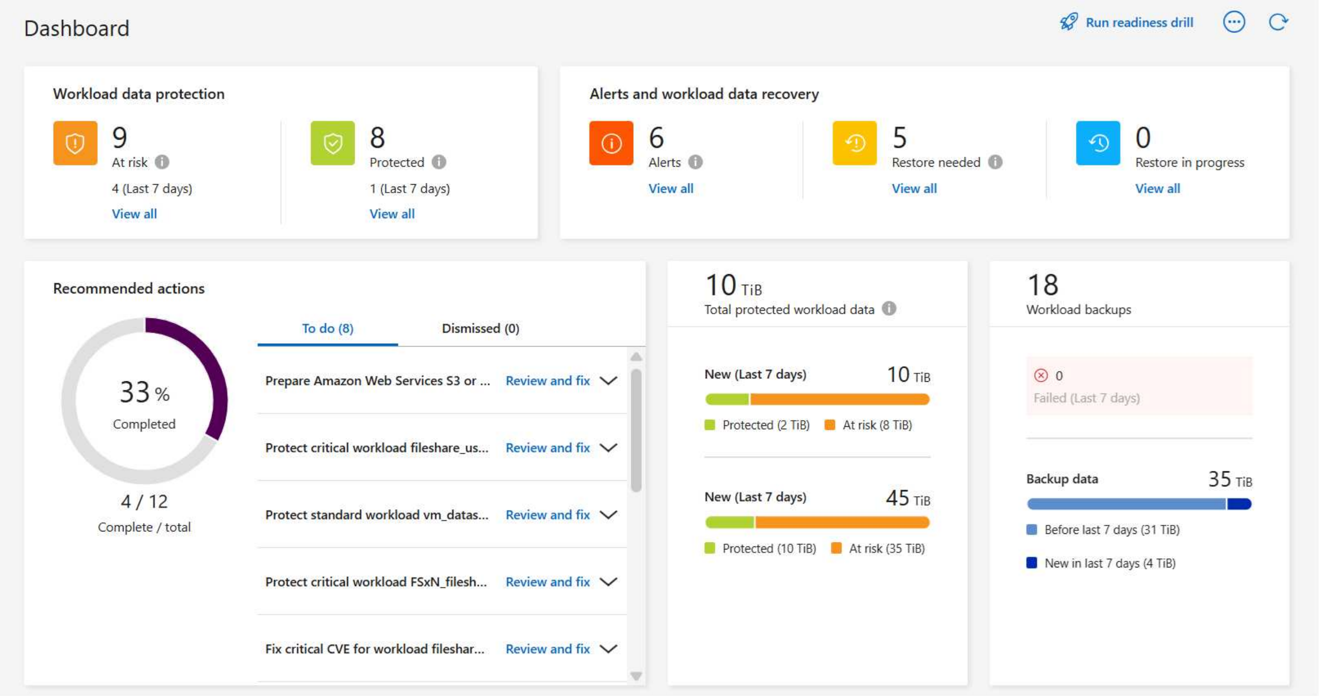
You need to enter a user name and password for the following situations:

- If user name or password changes occurred for the previously selected storage VM
- If you select a different CIFS (SMB) storage VM
- If you enter a different test workload name

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

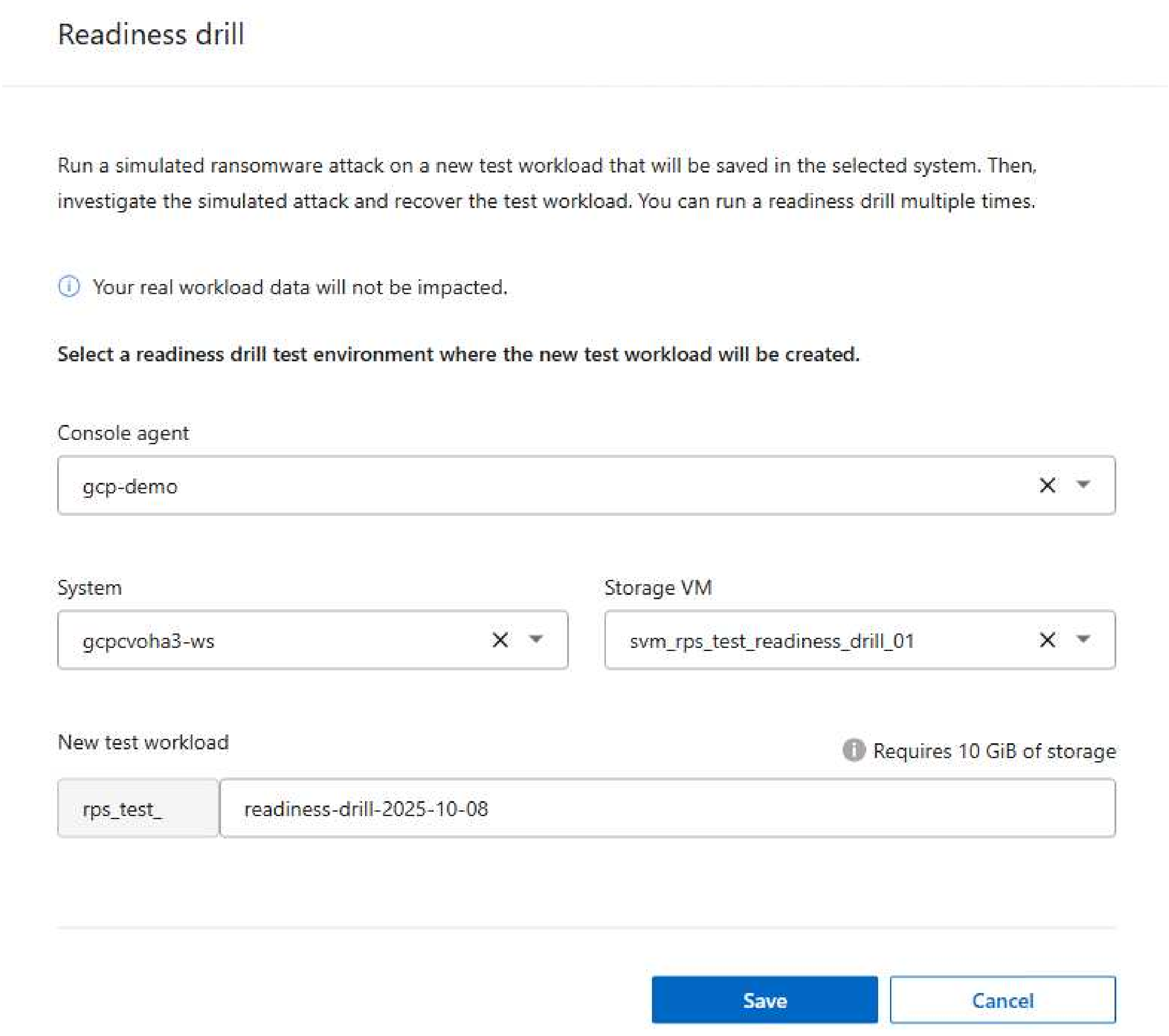
Steps

1. From the NetApp Ransomware Resilience menu, select the **Run readiness drill** button at the top right.



2. In the Readiness drill card on the Settings page, select **Configure**.

   The Console displays the Configure readiness drill page.



Readiness drill

Run a simulated ransomware attack on a new test workload that will be saved in the selected system. Then, investigate the simulated attack and recover the test workload. You can run a readiness drill multiple times.

Your real workload data will not be impacted.

Select a readiness drill test environment where the new test workload will be created.

Console agent

gcp-demo

System

gcpcvoha3-ws

Storage VM

svm_rps_test_readiness_drill_01

New test workload

rps_test_ readiness-drill-2025-10-08

Requires 10 GiB of storage

3. Do the following:
   a. Select the Console agent you want to use for the readiness drill.
   b. Select a test system.
   c. Select a test storage SVM.
   d. If you selected a CIFS (SMB) storage VM, **User name** and **Password** fields appear. Enter the user name and password for the storage VM.
   e. Enter the name of a new test workload to be created. Do not include dashes in the name.
4. Select **Save**.

You can edit the readiness drill configuration later using the Settings page.

Start a readiness drill

After you configure the readiness drill, you can start the drill.

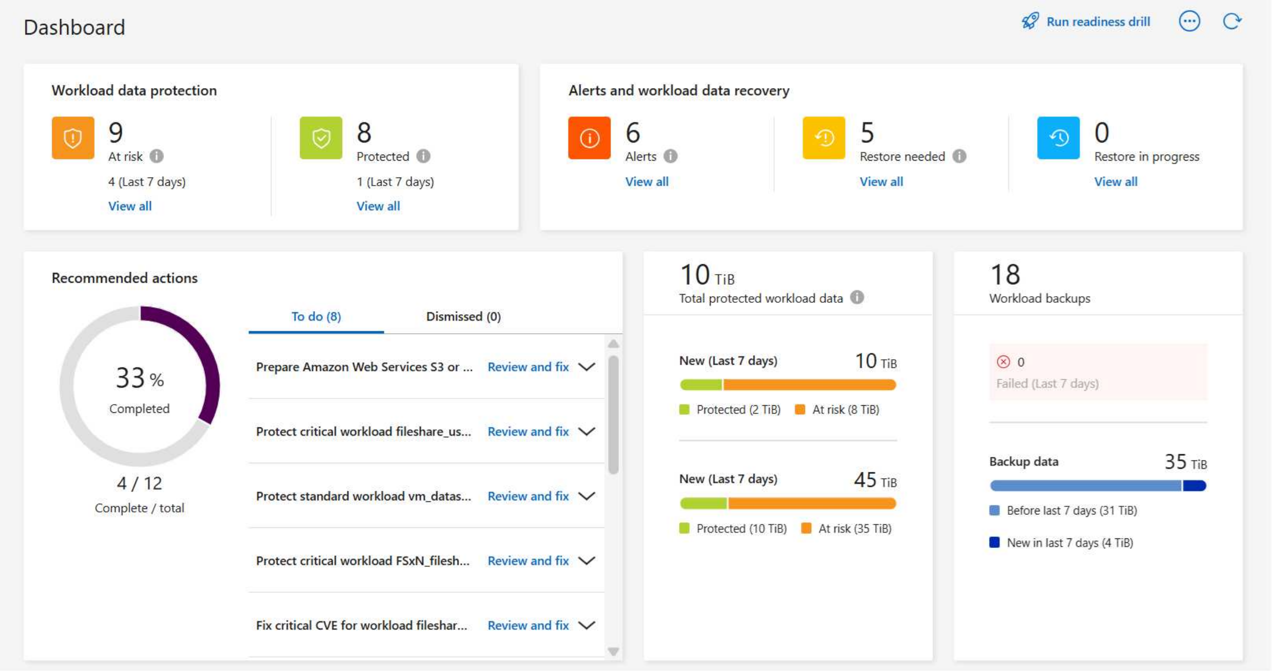
Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Console access roles for all services.

When you start the readiness drill, Ransomware Resilience skips the learning mode and starts the drill in active mode. The detection status of the workload is Active.

> A workload can have a ransomware detection **Learning mode** status when a detection policy is recently assigned and Ransomware Resilience scans workloads.

Steps

1. Do one of the following:
   - From the Ransomware Resilience menu, select the **Run readiness drill** button at the top right.



   - OR, from the Settings page, in the Readiness drill card, select **Start**.
2. If you already configured the readiness drill, after selecting **Start**, the readiness drill begins.

> After the drill has started, you cannot edit the readiness drill configuration. You can reset it to start again.

Respond to a readiness drill alert

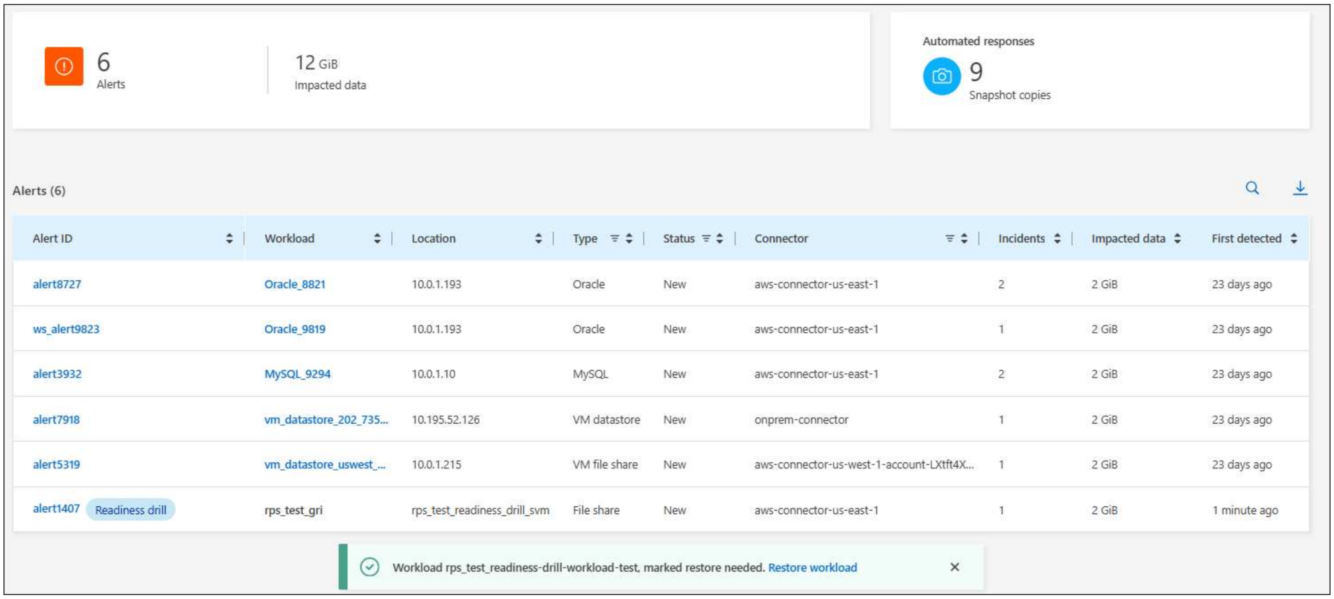
Test your readiness by responding to a readiness drill alert.

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

Steps

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

   The Console displays the Alerts page. In the Alert ID column, you see "Readiness drill" next to the ID.



6 Alerts

12 GiB Impacted data

Automated responses

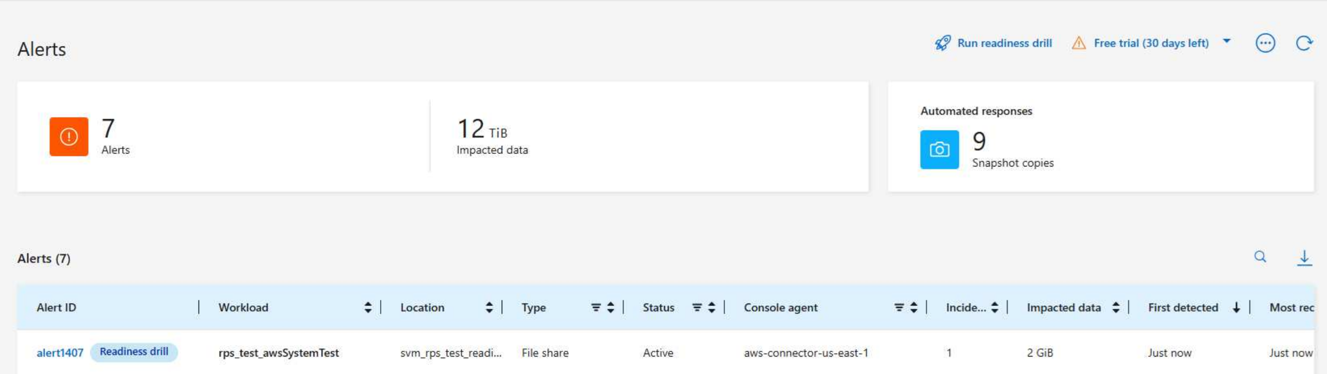
9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
alert8727	Oracle_8821	10.0.1.193	Oracle	New	aws-connector-us-east-1	2	2 GiB	23 days ago
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	New	aws-connector-us-east-1	1	2 GiB	23 days ago
alert3932	MySQL_9294	10.0.1.10	MySQL	New	aws-connector-us-east-1	2	2 GiB	23 days ago
alert7918	vm_datastore_202_735...	10.195.52.126	VM datastore	New	onprem-connector	1	2 GiB	23 days ago
alert5319	vm_datastore_uswest_...	10.0.1.215	VM file share	New	aws-connector-us-west-1-account-LXtft4X...	1	2 GiB	23 days ago
alert1407 Readiness drill	rps_test_gri	rps_test_readiness_drill_svm	File share	New	aws-connector-us-east-1	1	2 GiB	1 minute ago

Workload rps_test_readiness-drill-workload-test, marked restore needed. Restore workload

2. Select the alert with the "Readiness drill" indication. A list of incident alerts appears on the Alerts details page.



Alerts

7 Alerts

12 TiB Impacted data

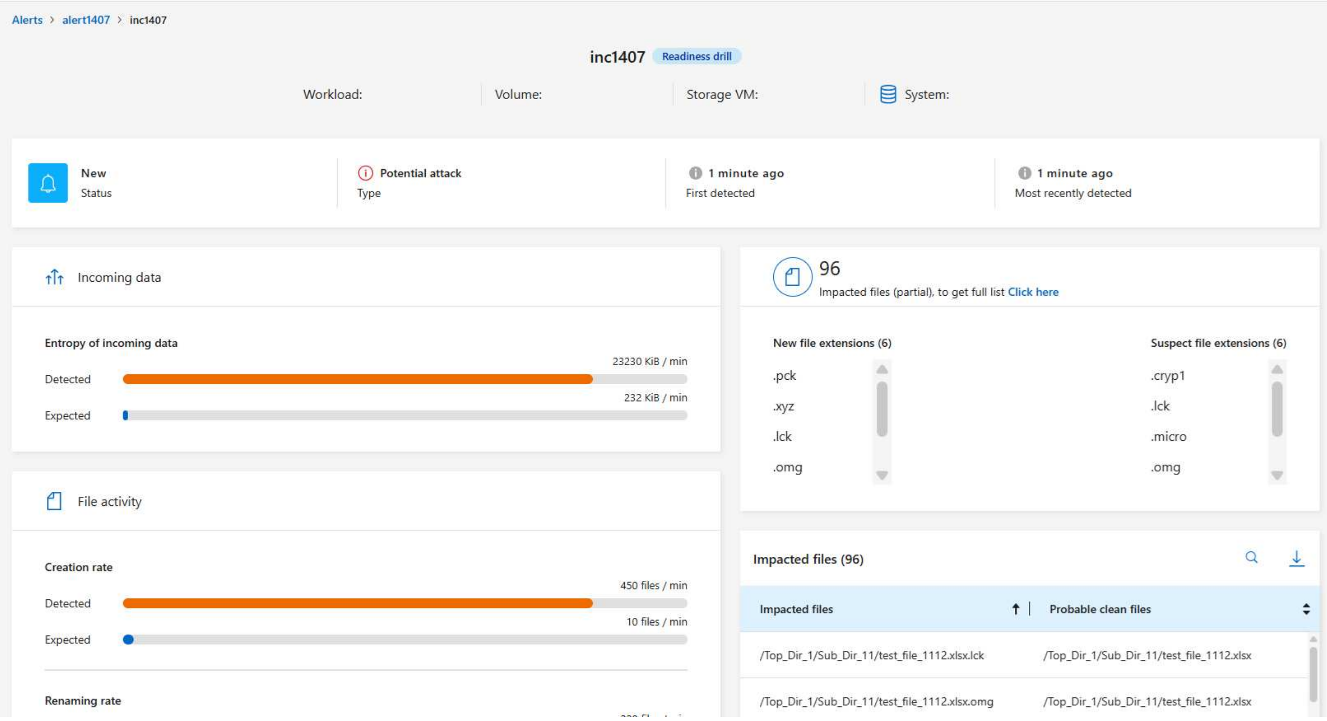
Automated responses

9 Snapshot copies

Alerts (7)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data	First detected	Most rec
alert1407 Readiness drill	rps_test_awsSystemTest	svm_rps_test_readi...	File share	Active	aws-connector-us-east-1	1	2 GiB	Just now	Just now

3. Review the alert incidents.
4. Select an alert incident.



Alerts > alert1407 > inc1407

inc1407 Readiness drill

Workload: | Volume: | Storage VM: | System:

New
Status

Potential attack
Type

1 minute ago
First detected

1 minute ago
Most recently detected

Incoming data

Entropy of incoming data

Detected: 23230 KiB / min

Expected: 232 KiB / min

96
Impacted files (partial), to get full list Click here

New file extensions (6)	Suspect file extensions (6)
.pck	.cryp1
.xyz	.lck
.lck	.micro
.omg	.omg

File activity

Creation rate

Detected: 450 files / min

Expected: 10 files / min

Renaming rate

Impacted files (96)

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.lck	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.omg	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx

Here are some things to look for:

- Look at the Potential attack Type.

  If the Type indicates that a user is suspected of malicious activity, review the user name. You might want to investigate the user more in Data Infrastructure Insights Workload Security by selecting **Investigate in Workload security**.

- Look at the file activity and suspected processes:
  - Look at the incoming detected data compared to the expected data.
  - Look at the creation rate of files that is detected compared to the expected rate.
  - Look at the file renaming rate that is detected compared to the expected rate.
  - Look at the deletion rate compared to the expected rate.
- Look at the list of impacted files. Look at the extensions that might be causing the attack.
- Determine the impact and breadth of the attack by reviewing the number of impacted files and directories.

Restore the test workload

After reviewing the readiness drill alert, restore the test workload if needed.

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

Steps

1. Return to the Alert details page.
2. If the test workload should be restored, do the following:

- Select **Mark restore needed**.
- Review the confirmation, and select **Mark restore needed** in the confirmation box.
  - From the Ransomware Resilience menu, select **Recovery**.
  - Select the test workload marked with "Readiness drill" that you want to restore.
  - Select **Restore**.
  - In the Restore page, provide information for the restore:
- Select the source snapshot copy.
- Select the destination volume.

3. In the restore Review page, select **Restore**.

   The Console displays the status of the Readiness drill restore as "In progress" on the Recovery page.

   After the restore is complete, the Console changes the status of the workload to **Restored**.

4. Review the restored workload.

> For details about the restore process, see Recover from a ransomware attack (after incidents are neutralized).

Change the Alerts status after the readiness drill

After reviewing the readiness drill alert and restoring the workload, change the alert status if needed.

Required the Console role
Organization admin, Folder or project admin, or Ransomware Resilience admin. Learn about Console access roles for all services.

Steps

1. Return to the Alert details page.
2. Select the alert again.
3. Indicate the status by selecting **Edit status** and change the status to one of the following:
   - Dismissed: If you suspect that the activity is not a ransomware attack, change the status to Dismissed.

     > After you dismiss an attack, you cannot chanage it back. If you dismiss a workload, all snapshot copies taken automatically in response to the potential ransomware attack will be permanently deleted. If you dismiss the alert, the readiness drill is considered complete.

   - Resolved: The incident has been mitigated.

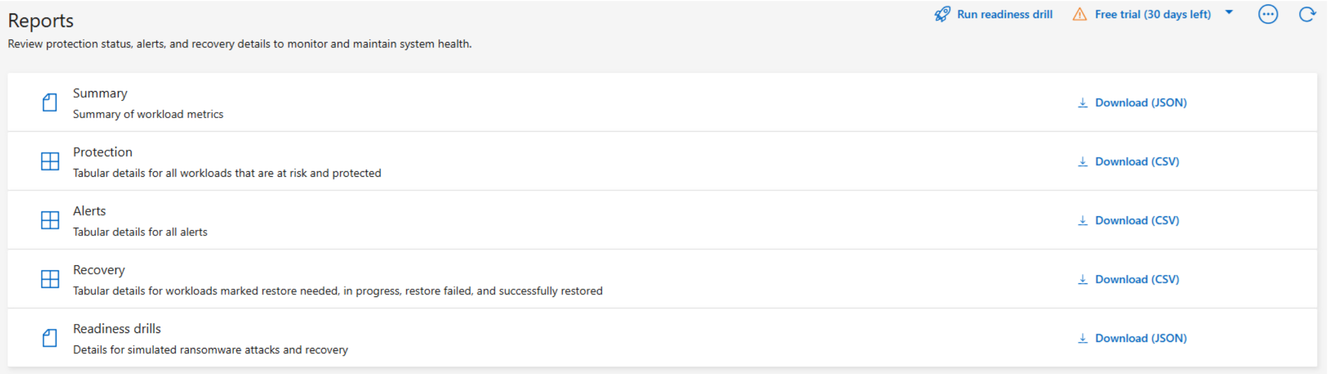
Review reports on the readiness drill

After the readiness drill is complete, you might want to review and save a report on the drill.

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 BlueXP access roles for all services.

Steps

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



Reports

Review protection status, alerts, and recovery details to monitor and maintain system health.

Summary Summary of workload metrics	Download (JSON)
Protection Tabular details for all workloads that are at risk and protected	Download (CSV)
Alerts Tabular details for all alerts	Download (CSV)
Recovery Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored	Download (CSV)
Readiness drills Details for simulated ransomware attacks and recovery	Download (JSON)

2. Select **Readiness drills** and **Download** to download the readiness drill report.

Configure protection settings in NetApp Ransomware Resilience

You can configure backup destinations, send data to an external security and event management (SIEM) system, conduct an attack readiness drill, configure workload discovery, or configure connection to Data Infrastructure Insights Workload security by accessing the **Settings** option.

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

What can you do in the Settings page?
From the Settings page, you can do the following:

- Simulate a ransomware attack by conducting a readiness drill and respond to a simulated ransomware alert. For details, see Conduct a ransomware attack readiness drill.
- Configure workload discovery.
- Configure the connection to Data Infrastructure Insights Workload security to see suspected user information in ransomware alerts.
- Add a backup destination.
- Connect your security and event management system (SIEM) for threat analysis and detection. Enabling threat detection automatically sends data to your SIEM for threat analysis.

Access the Settings page directly

You can easily access the Settings page from the Actions option near the top menu.

1. From the Ransomware Resilience, select the vertical ⋮ … option at the top right.
2. From the drop-down menu, select **Settings**.

Simulate a ransomware attack

Conduct a ransomware readiness drill by simulating a ransomware attack on a newly created, sample workload. Then, investigate the simulated attack and recover the sample workload. This feature helps you know that you are prepared in the event of an actual ransomware attack by testing alert notification, response, and recovery processes. You can run a ransomware readiness drill multiple times.

For details, refer to Conduct a ransomware attack readiness drill.

Configure workload discovery

You can configure workload discovery to automatically discover new workloads in your environment.

1. In the Settings page, locate the **Workload discovery** tile.
2. In the **Workload discovery** tile, select **Discover workloads**.

   This page shows Console agents with systems that were not selected earlier, newly available Console agents, and newly available systems. This page doesn’t show those systems that were previously selected.

3. Select the Console agent where you want to discover workloads.
4. Review the list of systems.
5. Check the systems where you want to discover workloads or select the box at the top of the table to discover workloads in all discovered workload environments.
6. Do this for other systems as needed.
7. Select **Discover** to have Ransomware Resilience automatically discover new workloads in the selected Console agent.

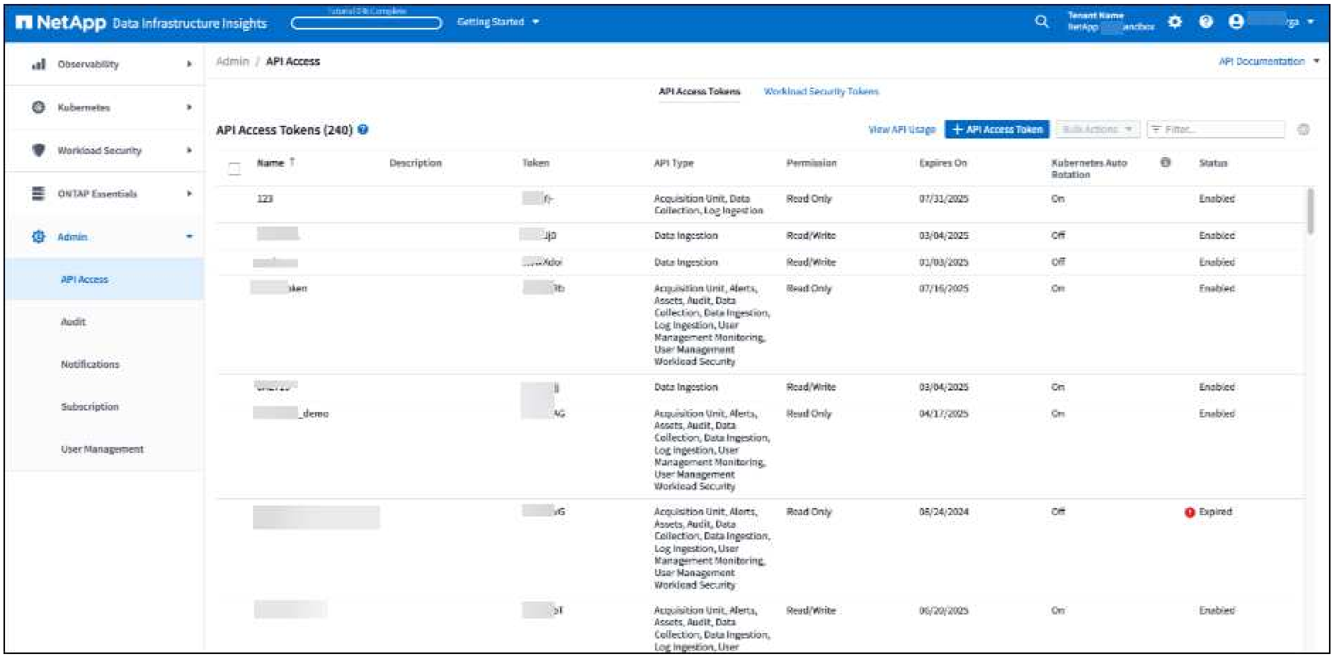
See suspected anomalous user behavior by connecting to Data Infrastructure Insights Workload security

Before you can view details of suspected anomalous user behavior in Ransomware Resilience, you need to configure the connection to the Data Infrastructure Insights Workload security system.

Obtain an API access token from the Data Infrastructure Insights Workload security system

Obtain an API access token from the Data Infrastructure Insights Workload security system.

1. Log in to the Data Infrastructure Insights Workload security system.
2. From the left navigation, select **Admin** > **API Access**.



API Access Tokens (240)

Name	Description	Token	API Type	Permission	Expires On	Kubernetes Auto Rotation	Status
123		[redacted]fi-	Acquisition Unit, Data Collection, Log Ingestion	Read Only	07/31/2025	On	Enabled
[redacted]		[redacted]ljO	Data Ingestion	Read/Write	03/04/2025	Off	Enabled
[redacted]		[redacted]Xdoi	Data Ingestion	Read/Write	01/03/2025	Off	Enabled
[redacted]ken		[redacted]Tb	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management Workload Security	Read Only	07/16/2025	On	Enabled
[redacted]		[redacted]lj	Data Ingestion	Read/Write	03/04/2025	On	Enabled
[redacted]_demo		[redacted]AG	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management Workload Security	Read Only	04/17/2025	On	Enabled
[redacted]		[redacted]vG	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management Workload Security	Read Only	05/24/2024	Off	● Expired
[redacted]		[redacted]bT	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User	Read/Write	06/20/2025	On	Enabled

3. Either create an API access token or use an existing one.
4. Copy the API access token.

Connect to Data Infrastructure Insights Workload security

1. From the Ransomware Resilience Settings menu, locate the **Workload security connection** tile.
2. Select **Connect**.
3. Enter the URL for the Data Infrastructure Workload security UI.
4. Enter the API access token that provides access to Workload security.
5. Select **Connect**.

Add a backup destination

Ransomware Resilience 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)
- Google Cloud Platform
- Microsoft Azure

> Backup destinations are not available for workloads in Amazon FSx for NetApp ONTAP. Perform backup operations using the FSx for ONTAP backup service.

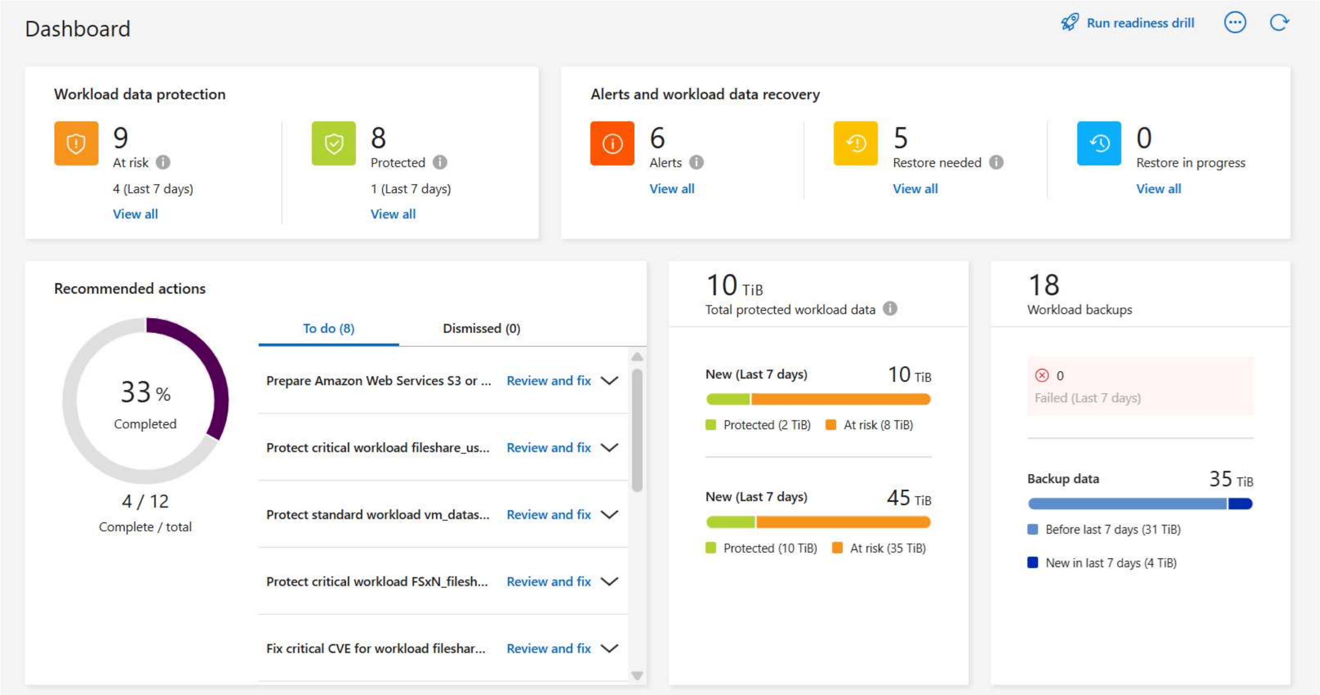
You can add a backup destination based on a recommended action from the Dashboard or from accessing the Settings option on the menu.

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. In the Ransomware Resilience dashboard, review the Recommended actions pane.



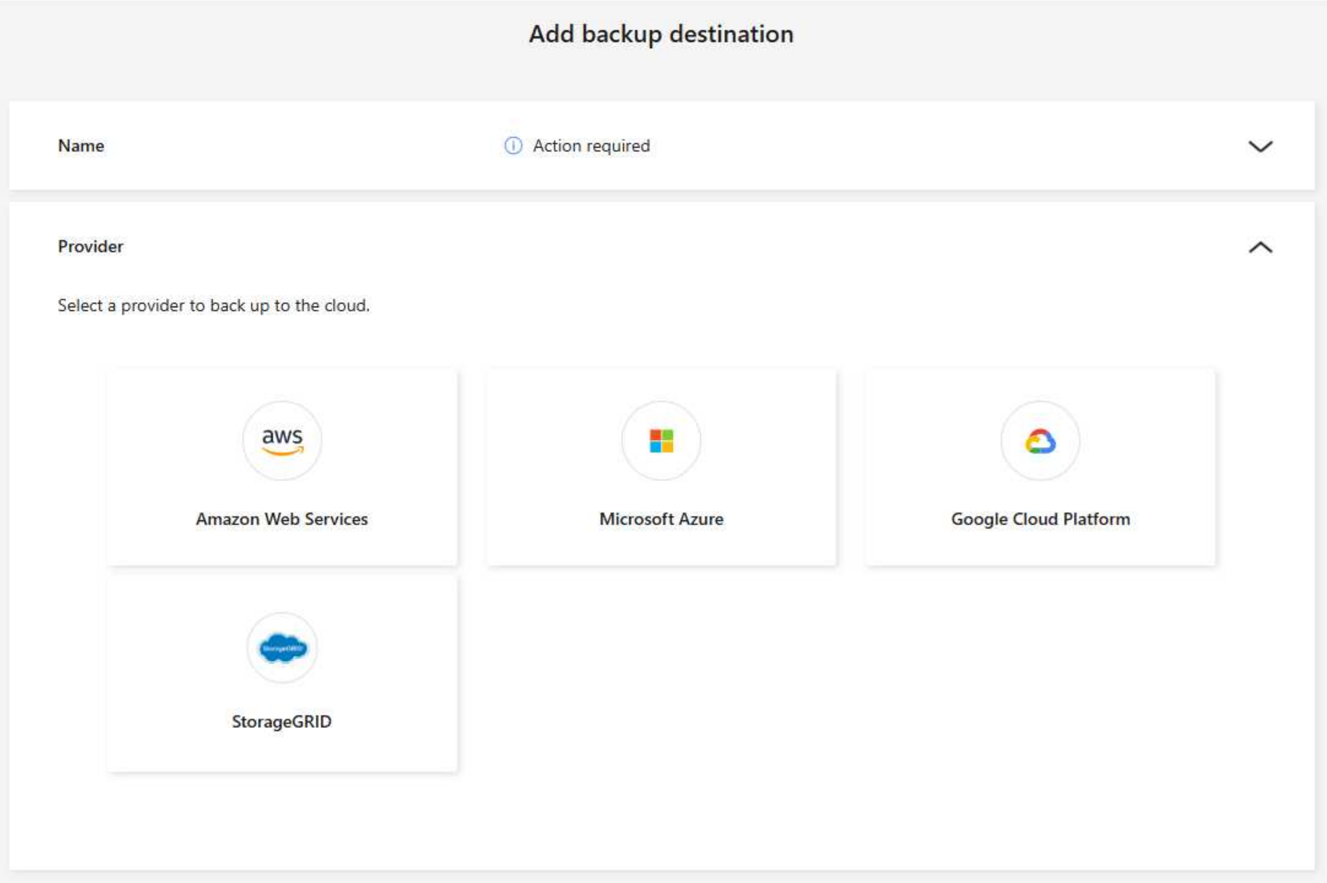
2. From the Dashboard, select **Review and fix** for the recommendation of "Prepare <backup provider> as a backup destination."
3. Continue with instructions depending on the backup provider.

Add StorageGRID as a backup destination

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

Steps

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



Add backup destination

Name — Action required

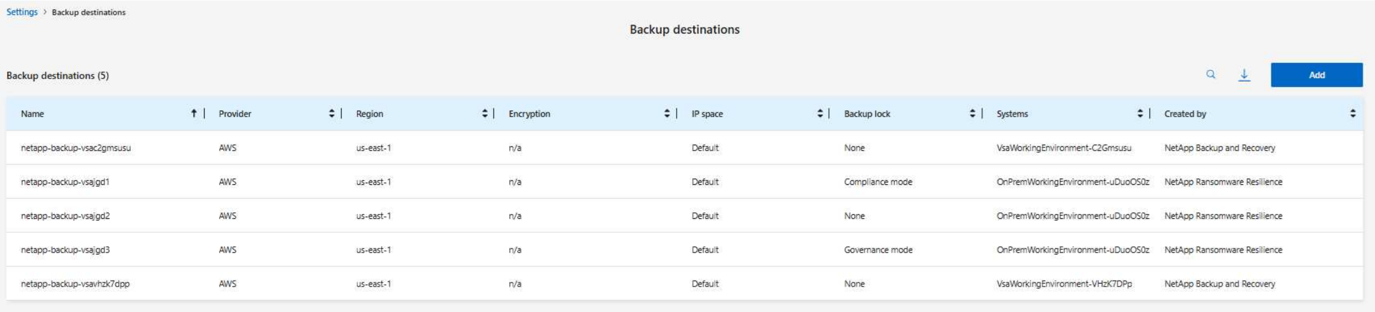
Provider

Select a provider to back up to the cloud.

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.
5. Select **Add**.

Result

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



Backup destinations

Backup destinations (5)

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsavhzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	NetApp Backup and Recovery

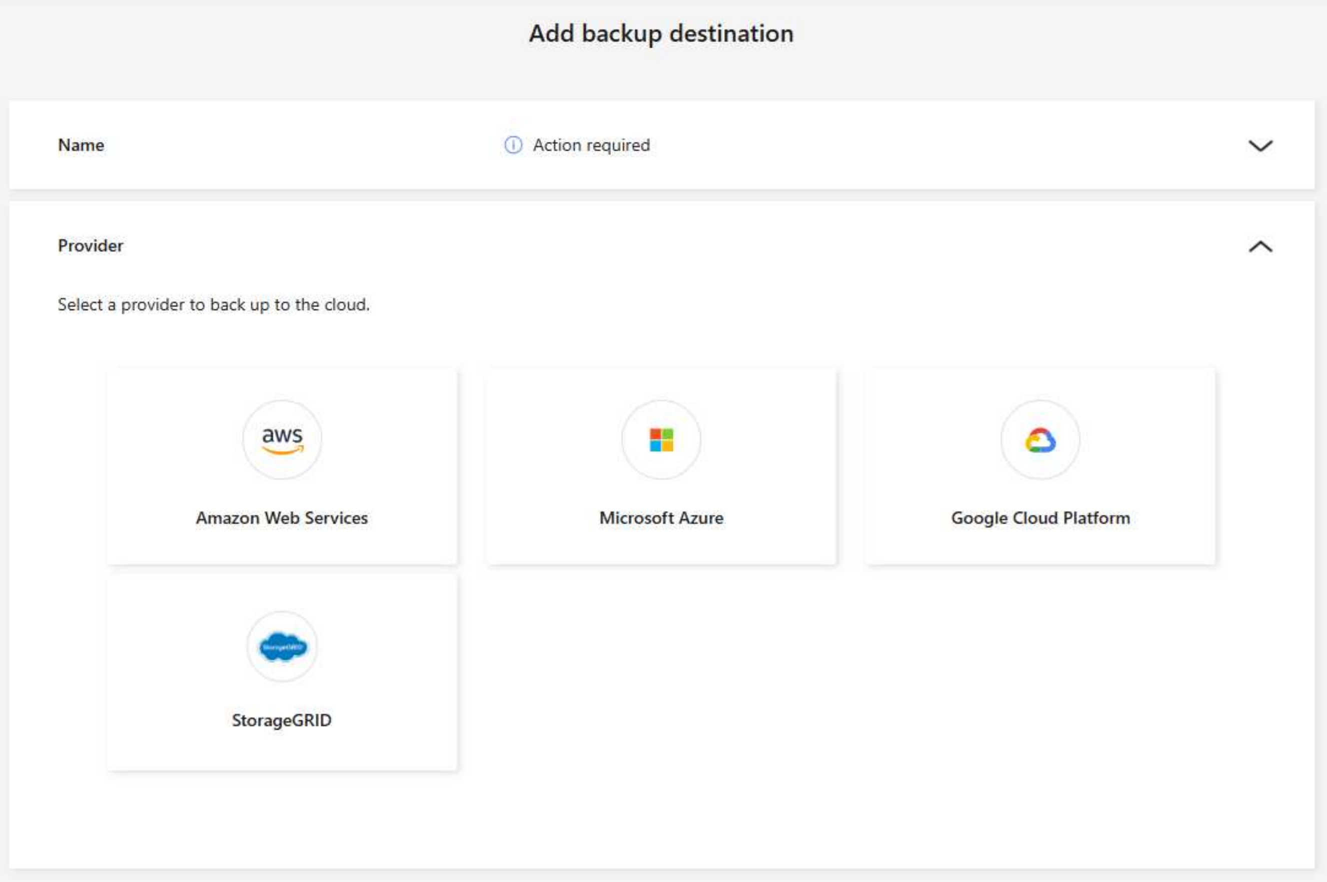
Add Amazon Web Services as a backup destination

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

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

Steps

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



Add backup destination

Name ⓘ Action required

Provider

Select a provider to back up to the cloud.

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 the Console, 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 Ransomware Resilience 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.

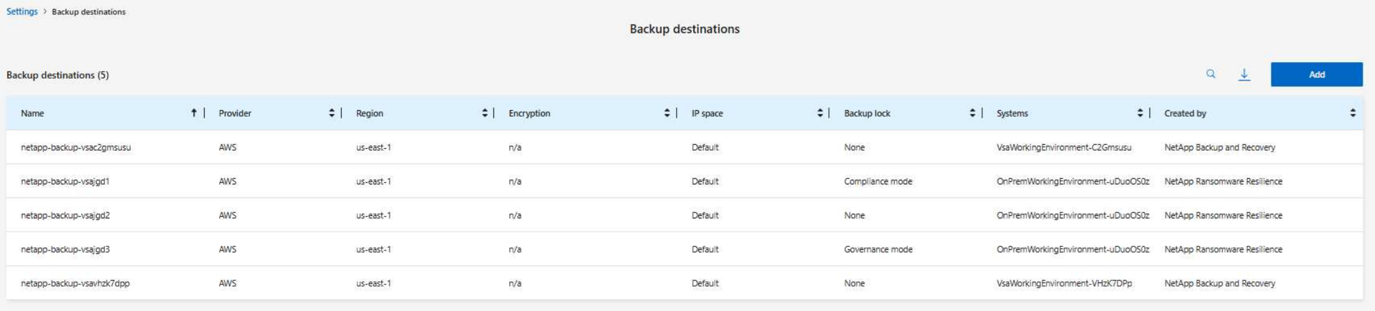
      > If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

        - **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.



Backup destinations

Backup destinations (5)

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsavhzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	NetApp Backup and Recovery

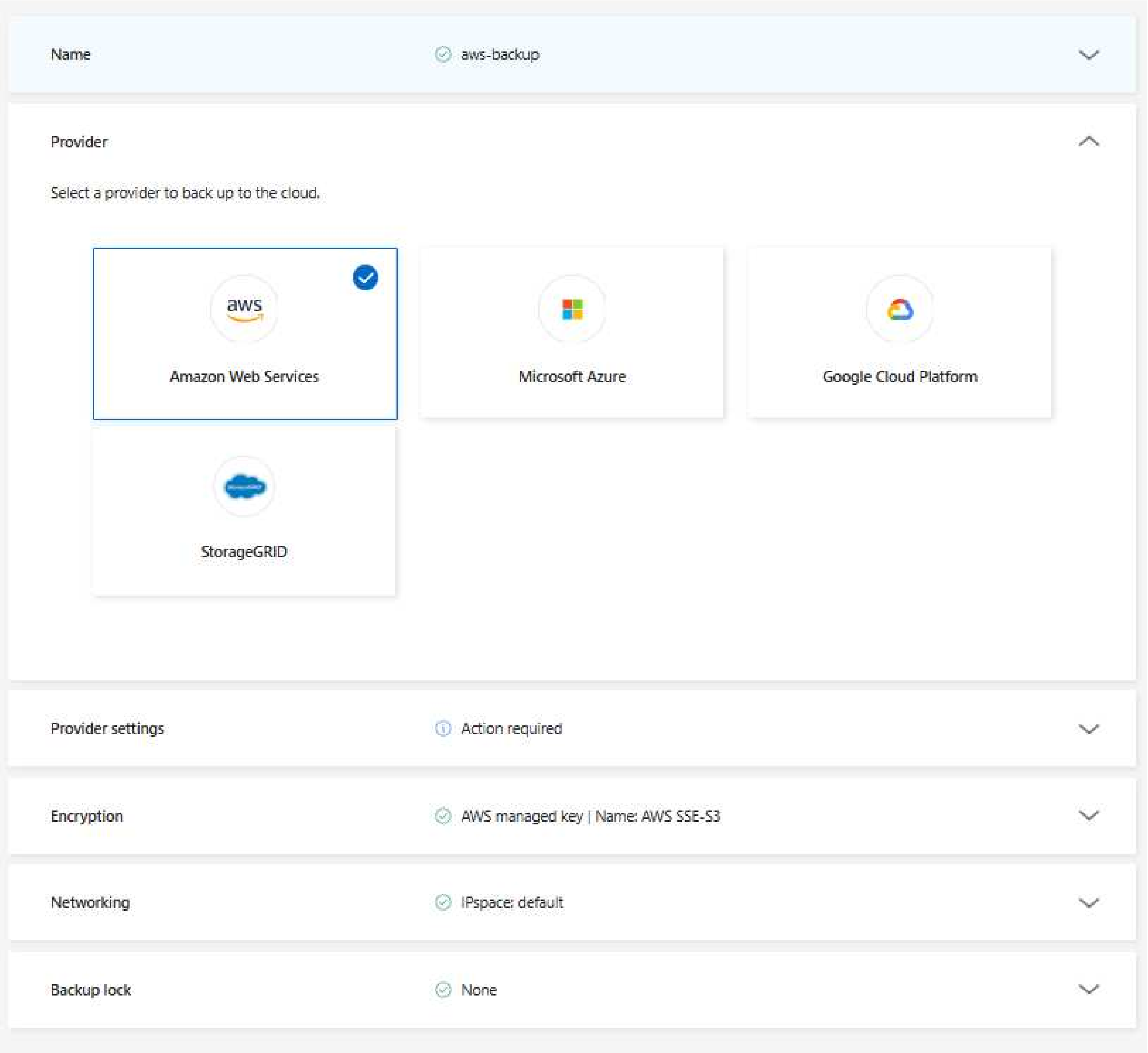
Add Google Cloud Platform as a backup destination

To set up Google Cloud Platform (GCP) as a backup destination, enter the following information.

For details about managing your GCP storage in the Console, refer to Console agent installation options in Google Cloud.

Steps

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



Name ✓ aws-backup

Provider

Select a provider to back up to the cloud.

Provider settings ⓘ Action required

Encryption ✓ AWS managed key | Name: AWS SSE-S3

Networking ✓ IPspace: default

Backup lock ✓ None

3. Select **Google Cloud Platform**.
4. Select the Down arrow next to each setting and enter or select values:
   - **Provider settings**:
     - Create a new bucket. Enter the access key and secret key.
     - Enter or select your Google Cloud Platform project and region.
   - **Encryption**: If you are creating a new 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 Google-managed keys by default. You can continue to use Google-managed 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 GCP private endpoint (PrivateLink) that you previously

configured.

5. Select **Add**.

Result

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

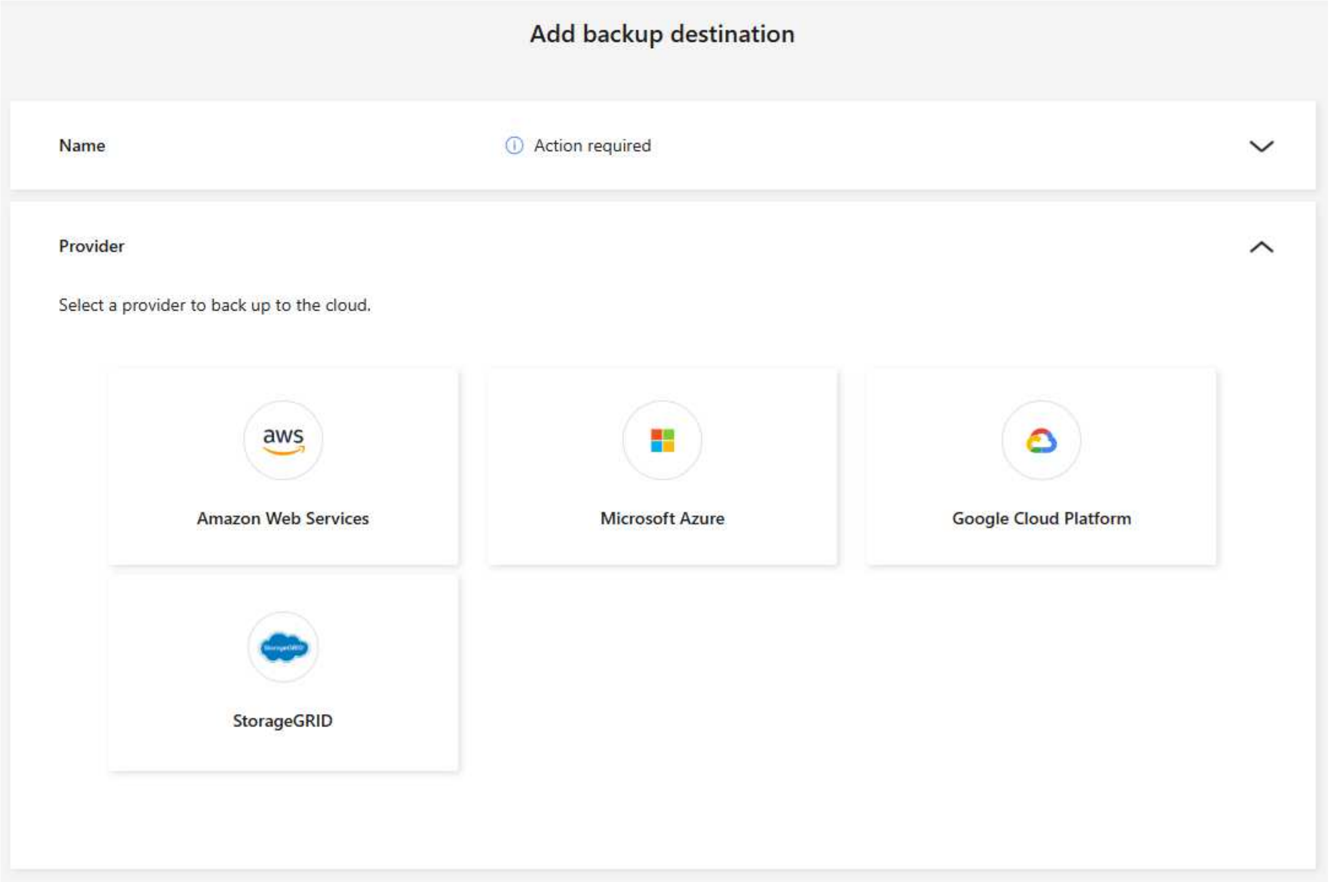
Add Microsoft Azure as a backup destination

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

For details about managing your Azure credentials and marketplace subscriptions in the Console, refer to Manage your Azure credentials and marketplace subscriptions.

Steps

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



Add backup destination

Name — ⓘ Action required

Provider

Select a provider to back up to the cloud.

3. Select **Azure**.
4. Select the Down arrow next to each setting and enter or select values:
   - **Provider settings**:
     - Create a new storage account, select an existing one if one already exists in the Console, or bring your own storage account that will store the backups.
     - Azure subscription, region, and resource group for Azure credentials

     If you want to bring your own storage account, refer to Add Azure Blob storage accounts.

   - **Encryption**: If you are creating a new storage account, enter encryption key information given to you from the provider. If you chose an existing account, encryption information is already available.

     Data in the account is encrypted with Microsoft-managed keys by default. You can continue to use Microsoft-managed keys, or you can manage the encryption of your data using your own keys.

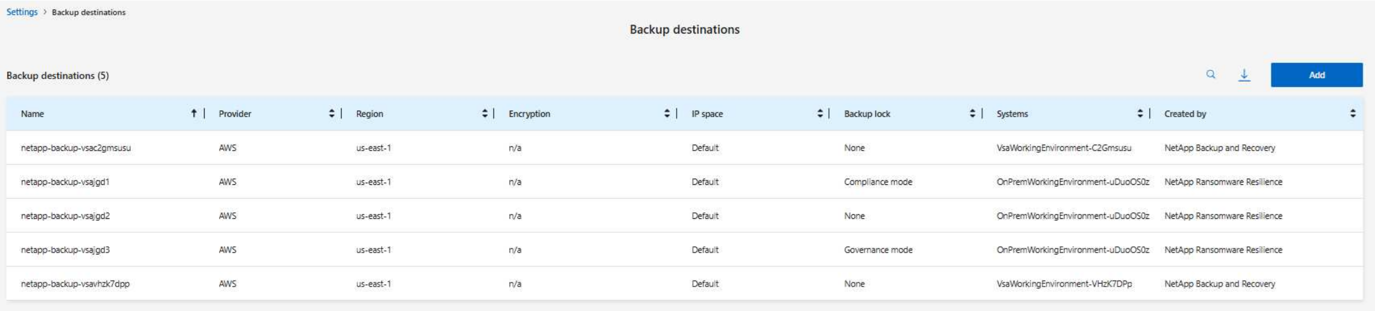
   - **Networking**: Choose the IPspace and whether you'll be using a Private Endpoint.
     - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
     - Optionally, choose whether you'll use an Azure private endpoint that you previously configured.

       If you want to use Azure PrivateLink, refer to Azure PrivateLink.

5. Select **Add**.

Result

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



Backup destinations

Backup destinations (5)

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsavhzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	NetApp Backup and Recovery

Connect to a security and event management system (SIEM) for threat analysis and detection

You can automatically send data to your security and event management system (SIEM) for threat analysis and detection. You can select the AWS Security Hub, Microsoft Sentinel, or Splunk Cloud as your SIEM.

Before you enable SIEM in Ransomware Resilience, you need to configure your SIEM system.

About the event data sent to a SIEM

Ransomware Resilience can send the following event data to your SIEM system:

- **context**:
  - **os**: This is a constant with the value of ONTAP.
  - **os_version**: The version of ONTAP running on the system.
  - **connector_id**: The ID of the Console agent managing the system.
  - **cluster_id**: The cluster ID reported by ONTAP for the system.
  - **svm_name**: The name of the SVM where the alert was found.
  - **volume_name**: The name of the volume on which the alert is found.
  - **volume_id**: The ID of the volume reported by ONTAP for the system.
- **incident**:
  - **incident_id**: The incident ID generated by Ransomware Resilience for the volume under attack in

  Ransomware Resilience.
  - **alert_id**: The ID generated by Ransomware Resilience for the workload.
  - **severity**: One of the following alert levels: "CRITICAL", "HIGH", "MEDIUM", "LOW".
  - **description**: Details about the alert that was detected, for example, "A Potential ransomware attack detected on workload arp_learning_mode_test_2630"

Configure AWS Security Hub for threat detection

Before you enable AWS Security Hub in Ransomware Resilience, you'll need to do the following high level steps in AWS Security Hub:

- Set up permissions in AWS Security Hub.
- Set up the authentication access key and secret key in AWS Security Hub. (These steps are not provided here.)

Steps to set up permissions in AWS Security Hub

1. Go to **AWS IAM console**.
2. Select **Policies**.
3. Create a policy using the following code in JSON format:

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

Configure Microsoft Sentinel for threat detection

Before you enable Microsoft Sentinel in Ransomware Resilience, you'll need to do the following high level steps in Microsoft Sentinel:

- **Prerequisites**
  - Enable Microsoft Sentinel.

    - Create a custom role in Microsoft Sentinel.
- **Registration**
    - Register Ransomware Resilience to receive events from Microsoft Sentinel.
    - Create a secret for the registration.
- **Permissions**: Assign permissions to the application.
- **Authentication**: Enter authentication credentials for the application.

Steps to enable Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Create a **Log Analytics workspace**.
3. Enable Microsoft Sentinel to use the Log Analytics workspace you just created.

Steps to create a custom role in Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Select **Subscription** > **Access control (IAM)**.
3. Enter a Custom role name. Use the name **Ransomware Resilience Sentinel Configurator**.
4. Copy the following JSON and paste it into the **JSON** tab.

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

      ]
    }
    ```

5. Review and save your settings.

Steps to register Ransomware Resilience to receive events from Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Select **Entra ID** > **Applications** > **App registrations**.
3. For the **Display name** for the application, enter "**Ransomware Resilience**".
4. In the **Supported account type** field, select **Accounts in this organizational directory only**.
5. Select a **Default Index** where events will be pushed.
6. Select **Review**.
7. Select **Register** to save your settings.

    After registration, the Microsoft Entra admin center displays the application Overview pane.

Steps to create a secret for the registration

1. Go to Microsoft Sentinel.

2. Select **Certificates & secrets** > **Client secrets** > **New client secret**.
3. Add a description for your application secret.
4. Select an **Expiration** for the secret or specify a custom lifetime.

   > A client secret lifetime is limited to two years (24 months) or less. Microsoft recommends that you set an expiration value of less than 12 months.

5. Select **Add** to create your secret.
6. Record the secret to use in the Authentication step. The secret is never displayed again after you leave this page.

Steps to assign permissions to the application

1. Go to Microsoft Sentinel.
2. Select **Subscription** > **Access control (IAM)**.
3. Select **Add** > **Add role assignment**.
4. For the **Privileged administrator roles** field, select **Ransomware Resilience Sentinel Configurator**.

   > This is the custom role that you created earlier.

5. Select **Next**.
6. In the **Assign access to** field, select **User, group, or service principal**.
7. Select **Select Members**. Then, select **Ransomware Resilience Sentinel Configurator**.
8. Select **Next**.
9. In the **What user can do** feld, select **Allow user to assign all roles except privileged administrator roles Owner, UAA, RBAC (Recommended)**.
10. Select **Next**.
11. Select **Review and assign** to assign the permissions.

Steps to enter authentication credentials for the application

1. Go to Microsoft Sentinel.
2. Enter the credentials:
   a. Enter the tenant ID, the client application ID, and the client application secret.
   b. Click **Authenticate**.

      > After the authentication is successful, an "Authenticated" message appears.

3. Enter the Log Analytics workspace details for the application.
   a. Select the subscription ID, the resource group, and the Log Analytics workspace.

Configure Splunk Cloud for threat detection

Before you enable Splunk Cloud in Ransomware Resilience, you’ll need to do the following high level steps in Splunk Cloud:

- Enable an HTTP Event Collector in Splunk Cloud to receive event data via HTTP or HTTPS from the

Console.

- Create an Event Collector token in Splunk Cloud.

Steps to enable an HTTP Event Collector in Splunk

1. Go to Splunk Cloud.
2. Select **Settings** > **Data Inputs**.
3. Select **HTTP Event Collector** > **Global Settings**.
4. On the All Tokens toggle, select **Enabled**.
5. To have the Event Collector listen and communicate over HTTPS rather than HTTP, select **Enable SSL**.
6. Enter a port in **HTTP Port Number** for the HTTP Event Collector.

Steps to create an Event Collector token in Splunk

1. Go to Splunk Cloud.
2. Select **Settings** > **Add Data**.
3. Select **Monitor** > **HTTP Event Collector**.
4. Enter a Name for the token and select **Next**.
5. Select a **Default Index** where events will be pushed, then select **Review**.
6. Confirm that all settings for the endpoint are correct, then select **Submit**.
7. Copy the token and paste it in another document to have it ready for the Authentication step.

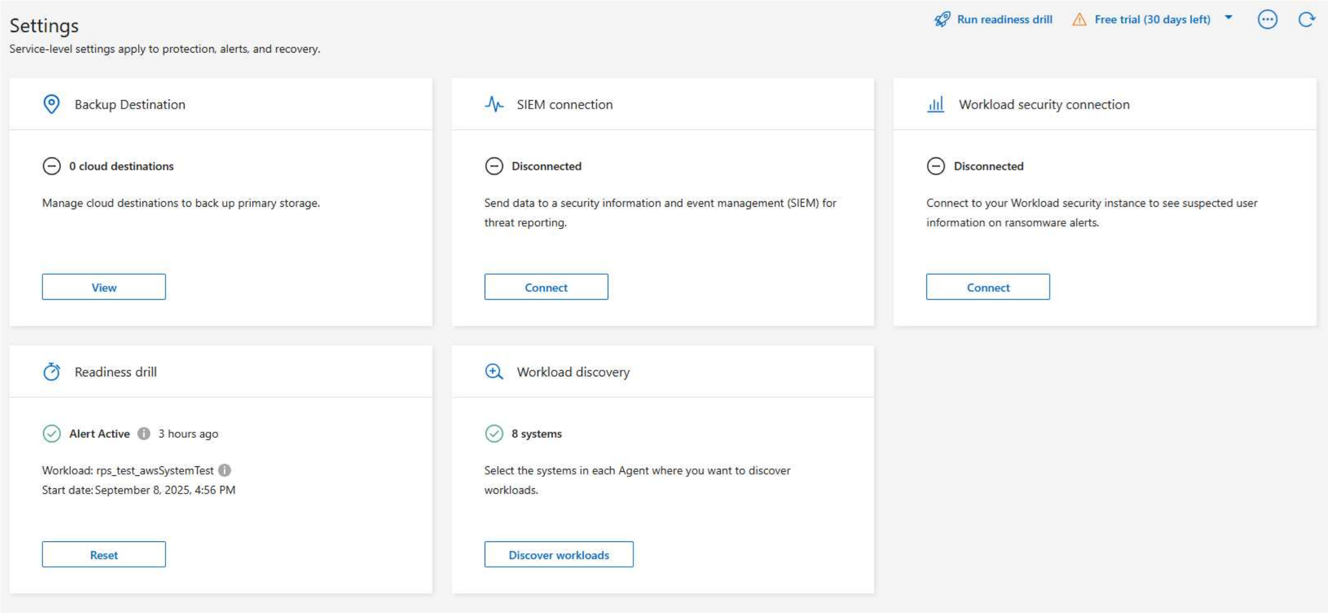
Connect SIEM in Ransomware Resilience

Enabling SIEM sends data from Ransomware Resilience to your SIEM server for threat analysis and reporting.

Steps

1. From the Console menu, select **Protection** > **Ransomware Resilience**.
2. From the Ransomware Resilience menu, select the vertical ⋮ … option at the top right.
3. Select **Settings**.

   The Settings page appears.



Settings

Service-level settings apply to protection, alerts, and recovery.

Backup Destination

0 cloud destinations

Manage cloud destinations to back up primary storage.

SIEM connection

Disconnected

Send data to a security information and event management (SIEM) for threat reporting.

Workload security connection

Disconnected

Connect to your Workload security instance to see suspected user information on ransomware alerts.

Readiness drill

Alert Active 3 hours ago

Workload: rps_test_awsSystemTest

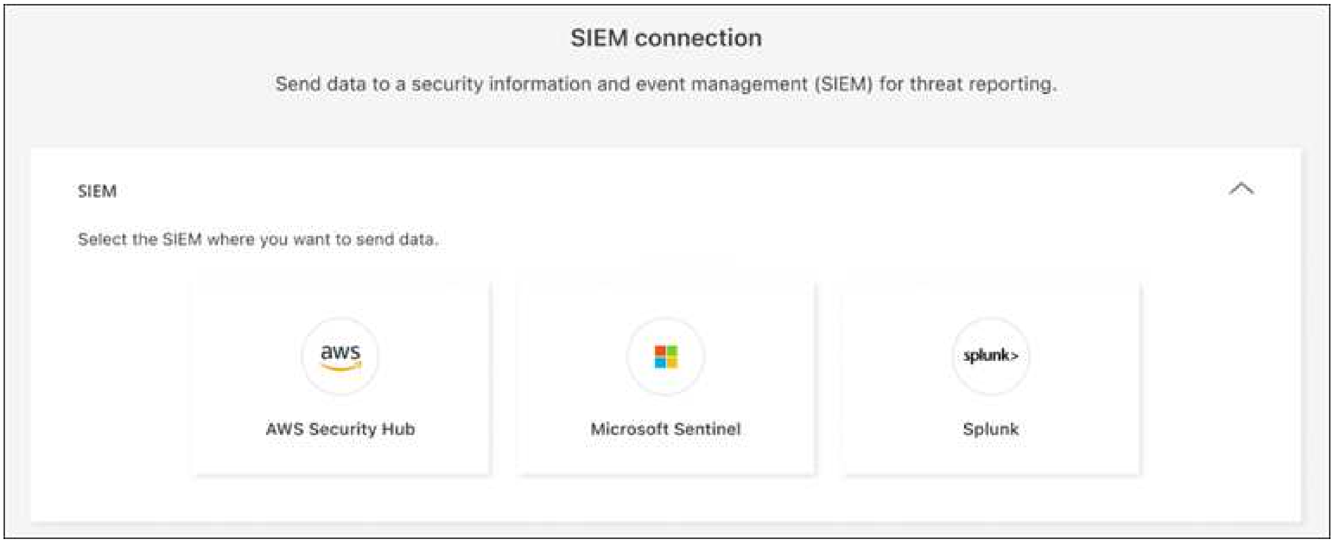
Start date: September 8, 2025, 4:56 PM

Workload discovery

8 systems

Select the systems in each Agent where you want to discover workloads.

4. In the Settings page, select **Connect** in the SIEM connection tile.



SIEM connection

Send data to a security information and event management (SIEM) for threat reporting.

SIEM

Select the SIEM where you want to send data.

5. Choose one of the SIEM systems.
6. Enter the token and authentication details you configured in AWS Security Hub or Splunk Cloud.

   The information that you enter depends on the SIEM you selected.

7. Select **Enable**.

   The Settings page shows "Connected."

[1] Although it’s possible that an attack might go undetected, our research indicates NetApp technology has resulted in a high degree of detection for certain file encryption-based ransomware attacks.

Use Ransomware Resilience

Use NetApp Ransomware Resilience

With NetApp Ransomware Resilience, you can view workload health and protect workloads.

- Discover workloads in Ransomware Resilience.
- View protection and workload health from the Dashboard.
  - Review and act on ransomware protection recommendations.
- Protect workloads:
  - Assign a ransomware protection strategy to workloads.
  - Increase application protection to prevent future ransomware attacks.
  - Create, change, or delete a protection strategy.
- Respond to detection of potential ransomware attacks.
- Recover from an attack (after incidents are neutralized).
- Configure protection settings.

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.

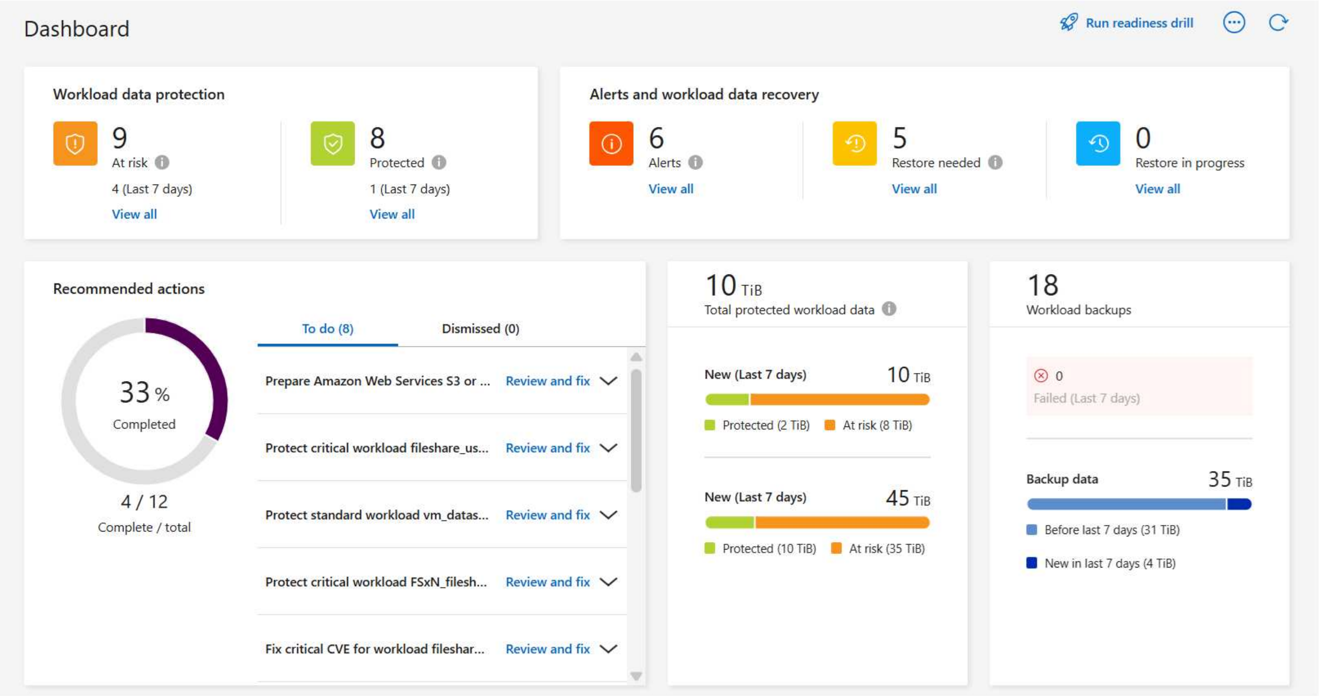
Use the Dashboard to review protection suggestions, change settings, download reports, and view documentation.

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 BlueXP access roles for all services.

Review workload health using the Dashboard

Steps

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



Dashboard

Run readiness drill

Workload data protection

9 At risk
4 (Last 7 days)
View all

8 Protected
1 (Last 7 days)
View all

Alerts and workload data recovery

6 Alerts
View all

5 Restore needed
View all

0 Restore in progress
View all

Recommended actions

33 % Completed

4 / 12 Complete / total

To do (8) Dismissed (0)

Prepare Amazon Web Services S3 or ... Review and fix

Protect critical workload fileshare_us... Review and fix

Protect standard workload vm_datas... Review and fix

Protect critical workload FSxN_filesh... Review and fix

Fix critical CVE for workload fileshar... Review and fix

10 TiB
Total protected workload data

New (Last 7 days) 10 TiB
🟩 Protected (2 TiB) 🟧 At risk (8 TiB)

New (Last 7 days) 45 TiB
🟩 Protected (10 TiB) 🟧 At risk (35 TiB)

18
Workload backups

⊗ 0
Failed (Last 7 days)

Backup data 35 TiB
🟦 Before last 7 days (31 TiB)
🟦 New in last 7 days (4 TiB)

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" tooltip 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.
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.

Recommendation	Description	How to resolve
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 completed or you change a dismissed item to a To Do action, the Total actions 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 that page's data.

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

Steps

1. From 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 Console access roles for all services.

Understand ransomware protection strategies

Ransomware protection strategies encompass both *detection* and *protection* policies.

- **Detection policies** detect ransomware threats and optionally block suspicious file extensions.
- **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

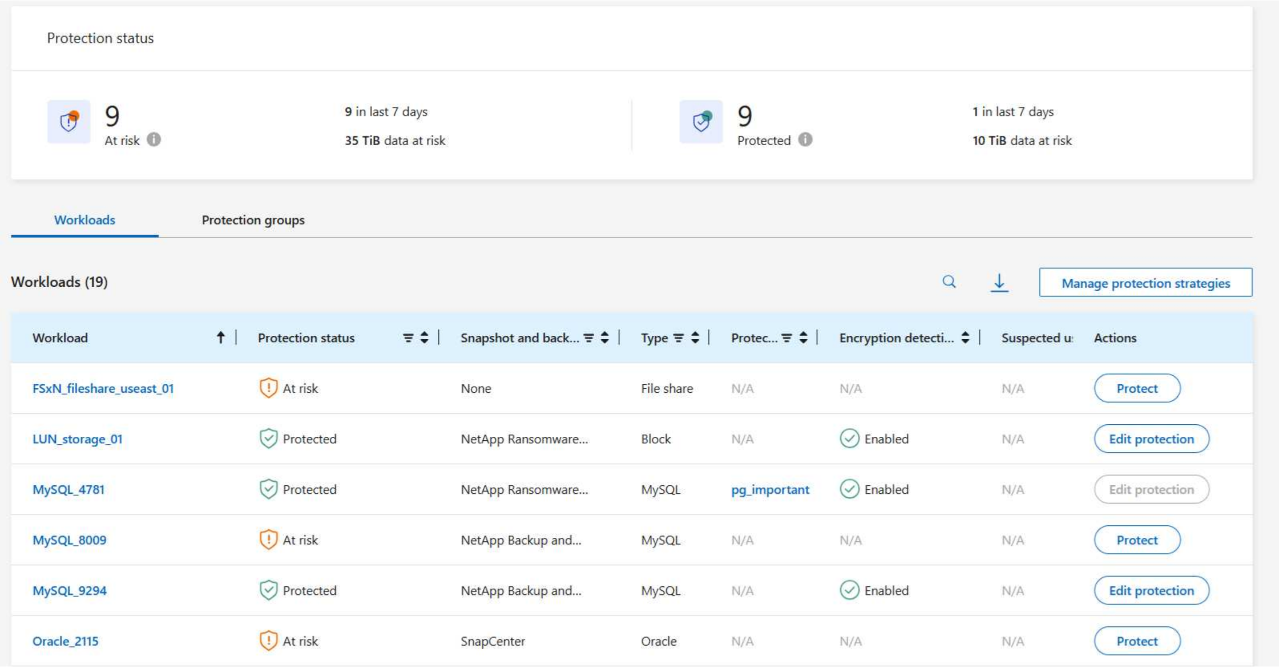
One of the first steps in protecting workloads is viewing your current workloads and their protection status. You can see the following types of workloads:

- 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**.



Protection status

9 At risk — 9 in last 7 days, 35 TiB data at risk

9 Protected — 1 in last 7 days, 10 TiB data at risk

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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:

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

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

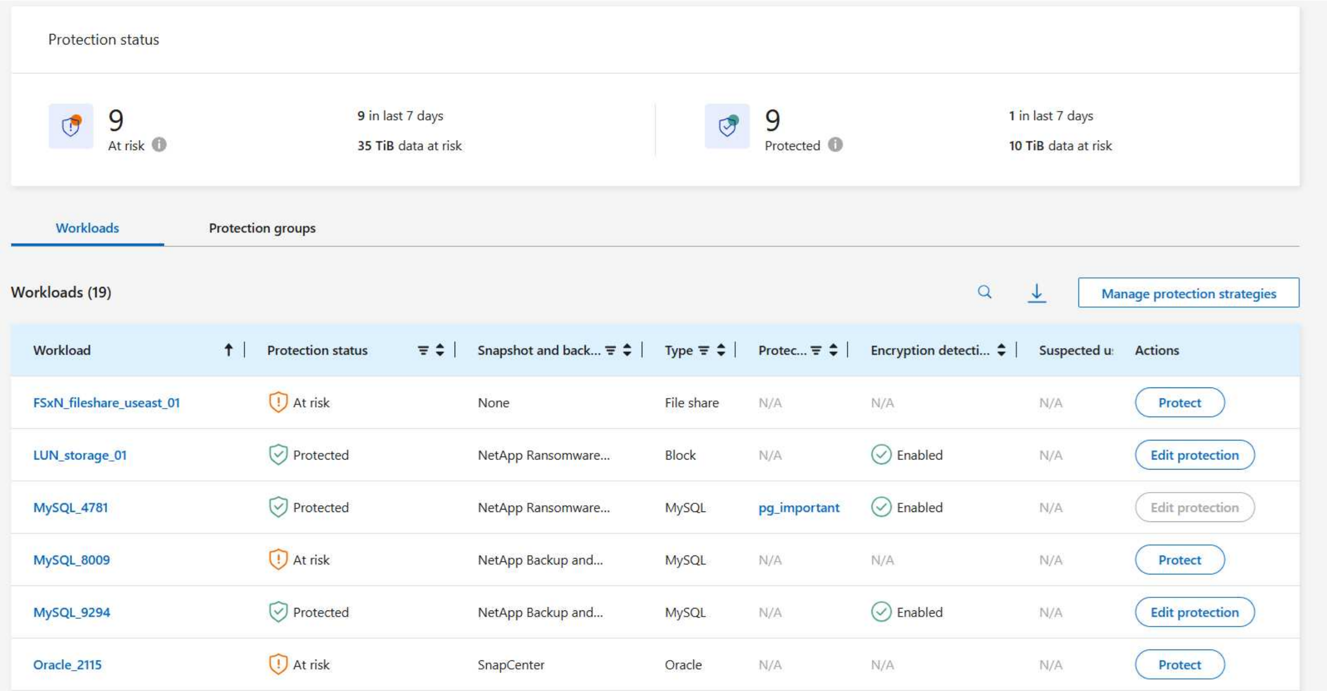
Create a ransomware protection strategy (if you have no snapshot or backup policies)

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**.

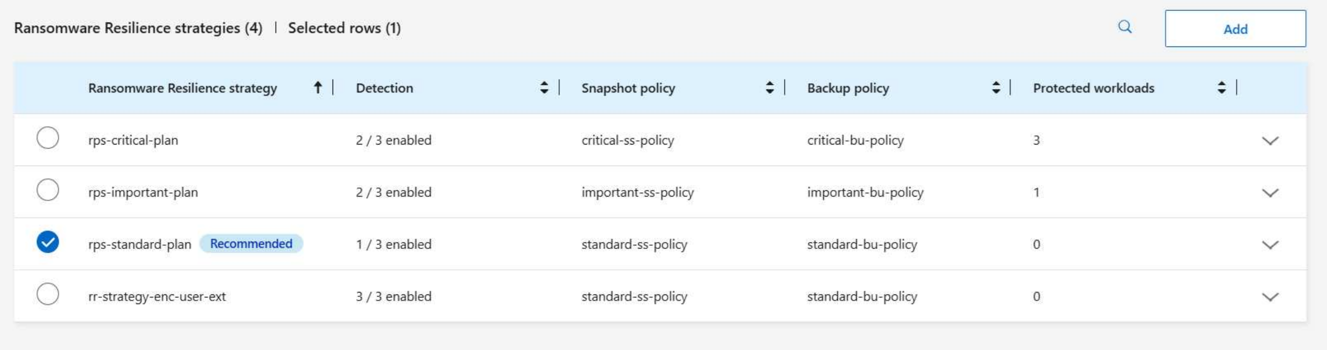

Protection status

9 At risk	9 in last 7 days 35 TiB data at risk	9 Protected	1 in last 7 days 10 TiB data at risk

Workloads (19)

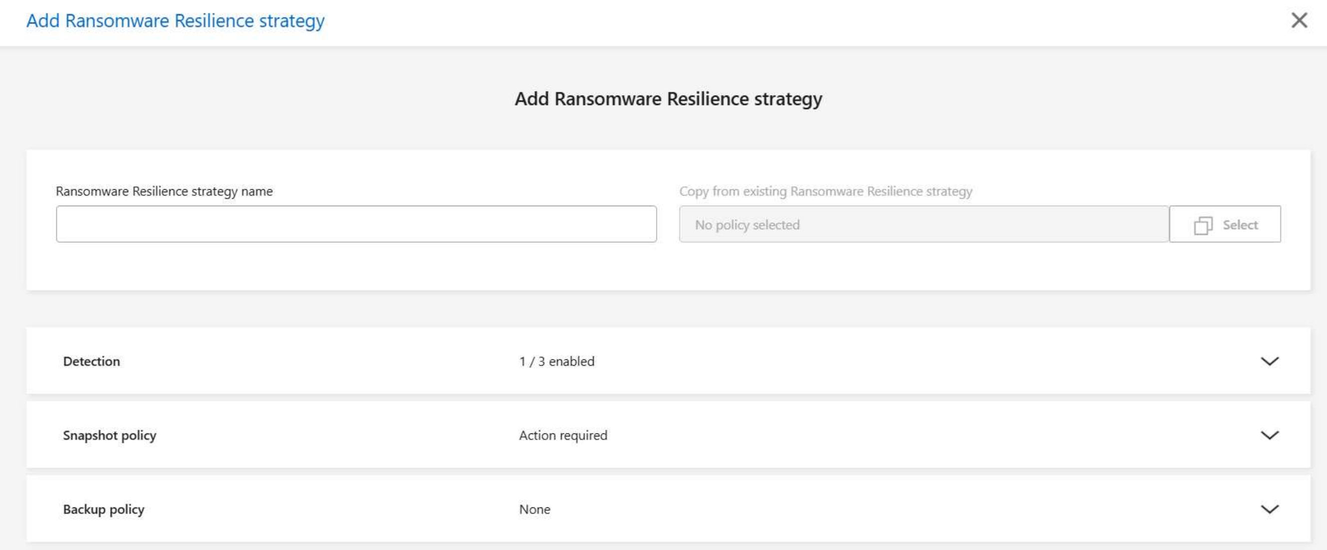
Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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


Ransomware Resilience strategies (4) | Selected rows (1)

	Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
○	rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
○	rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
●	rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0
○	rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0

3. From the Ransomware protection strategies page, select **Add**.


Add Ransomware Resilience strategy

Add Ransomware Resilience strategy

Ransomware Resilience strategy name

Copy from existing Ransomware Resilience strategy: No policy selected

Detection	1 / 3 enabled
Snapshot policy	Action required
Backup policy	None

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

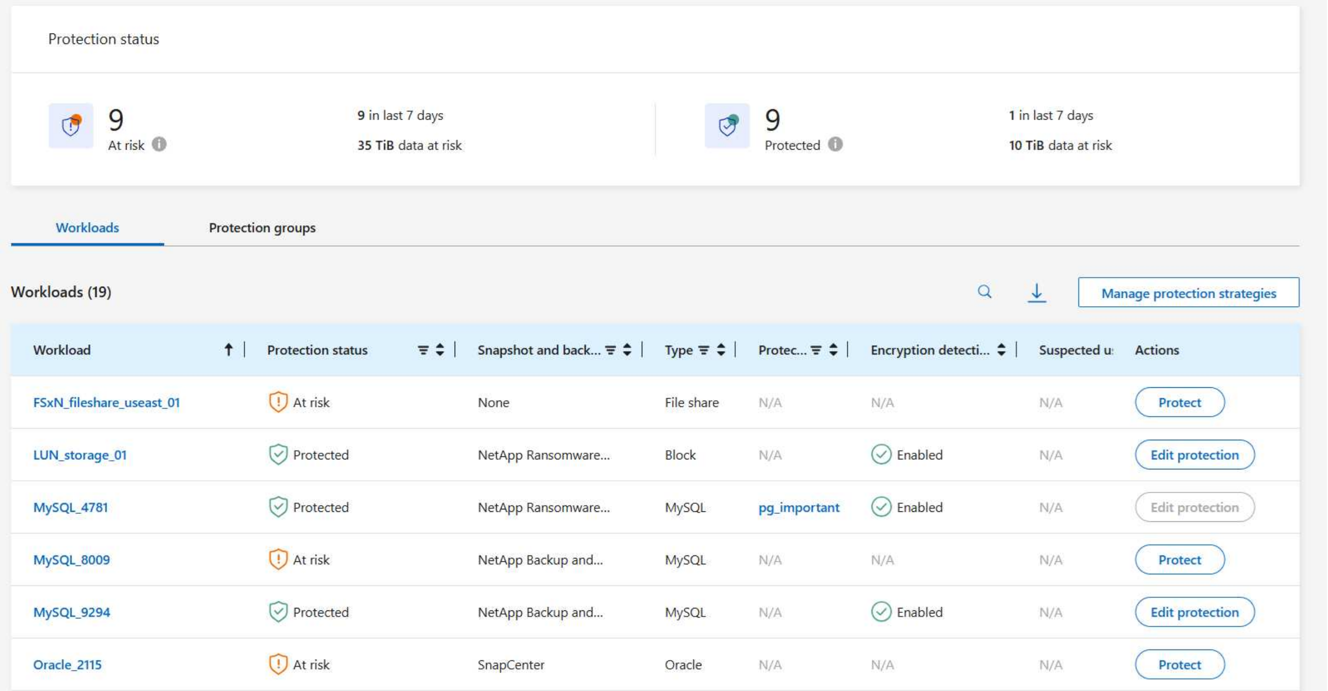
Ransomware Resilience enables you to assign either a detection policy or a protection policy to workloads with existing snapshot and backup protection managed in other NetApp products or services. Other services, such as Backup and Recovery and SnapCenter, use policies that govern snapshots, replication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



Protection status

9 At risk — 9 in last 7 days — 35 TiB data at risk

9 Protected — 1 in last 7 days — 10 TiB data at risk

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	✓ Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	✓ Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	✓ Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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**.

   Select a detection policy then select **Protect**.

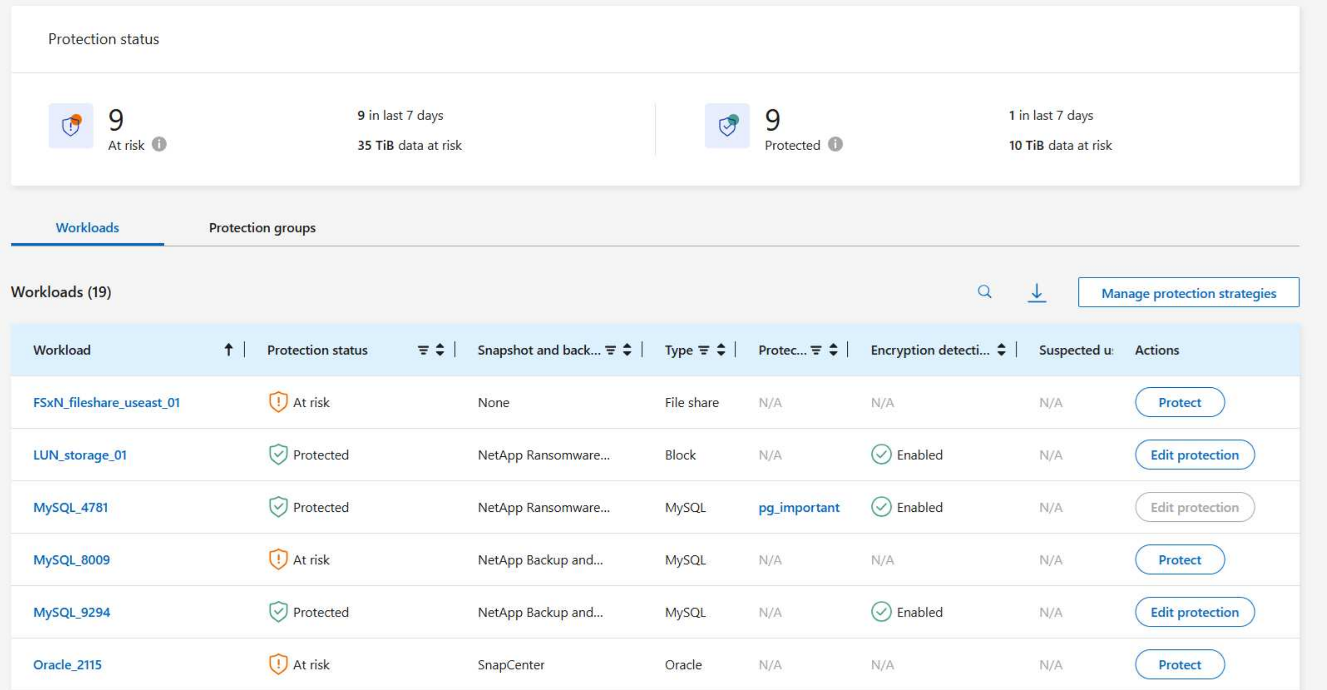
6. On the Protection page, review the **Detection status** to confirm detection is Active.

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**.



Protection status

9 At risk

9 in last 7 days

35 TiB data at risk

9 Protected

1 in last 7 days

10 TiB data at risk

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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**.
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.

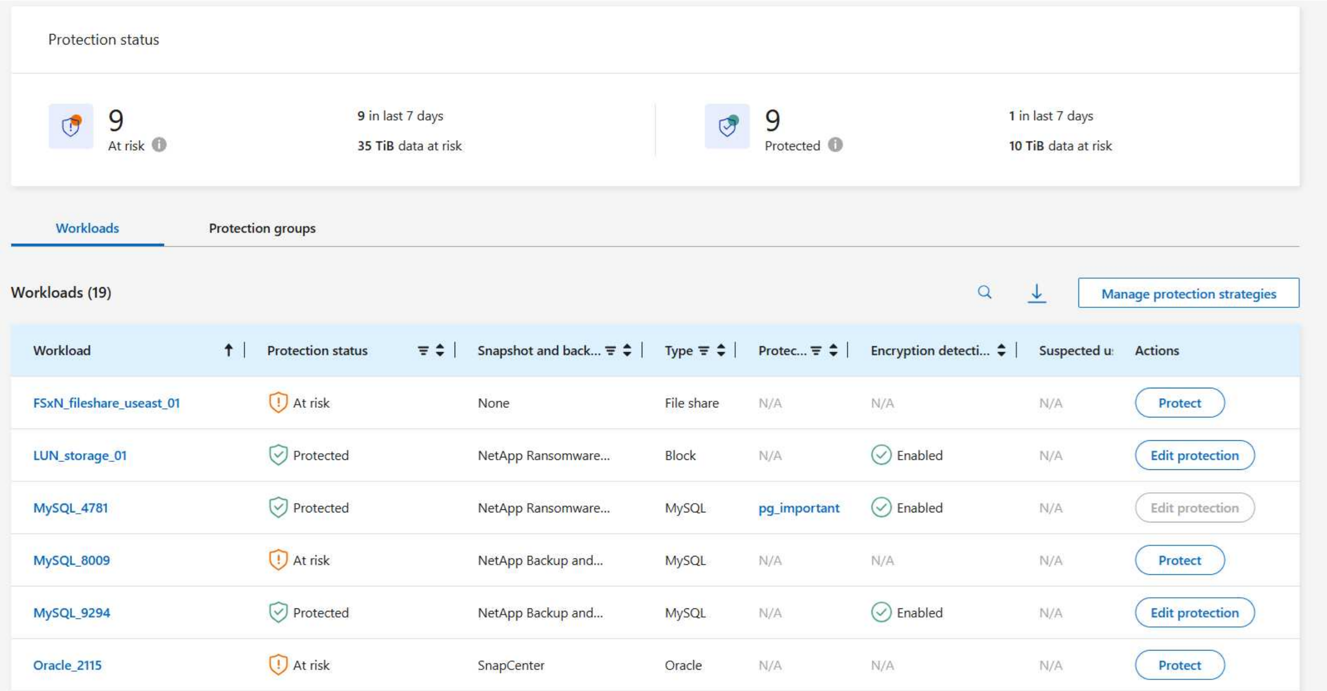
Group file shares for easier protection

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 that are 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**.



Protection status

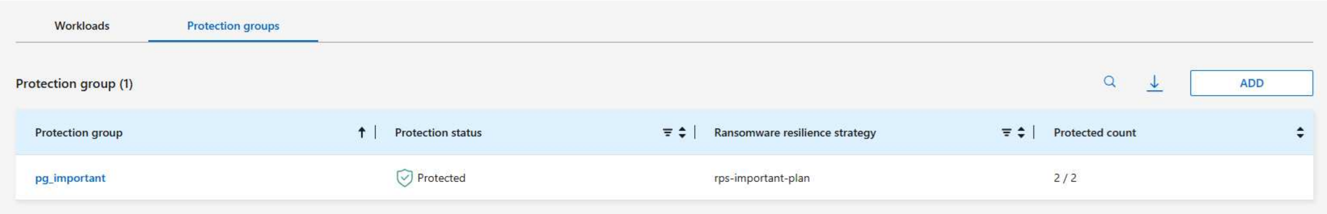
9 At risk — 9 in last 7 days — 35 TiB data at risk

9 Protected — 1 in last 7 days — 10 TiB data at risk

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

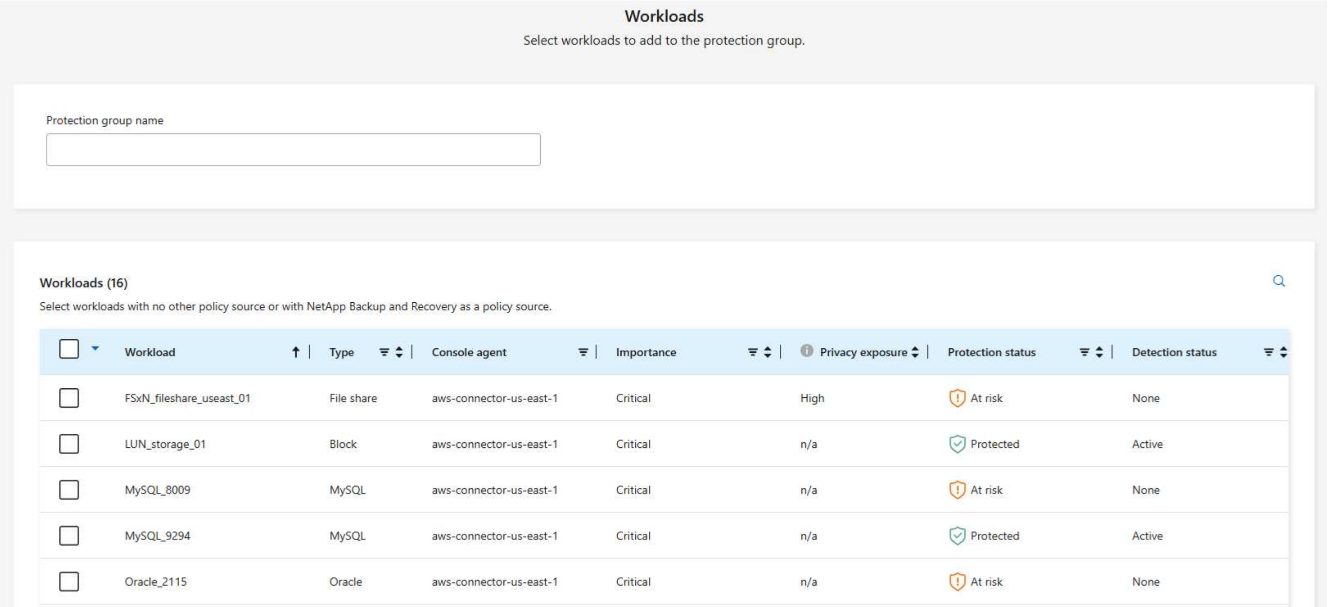
2. From the Protection page, select the **Protection groups** tab.



Protection group (1)

Protection group	Protection status	Ransomware resilience strategy	Protected count
pg_important	Protected	rps-important-plan	2 / 2

3. Select **Add**.



Workloads

Select workloads to add to the protection group.

Protection group name

Workloads (16)

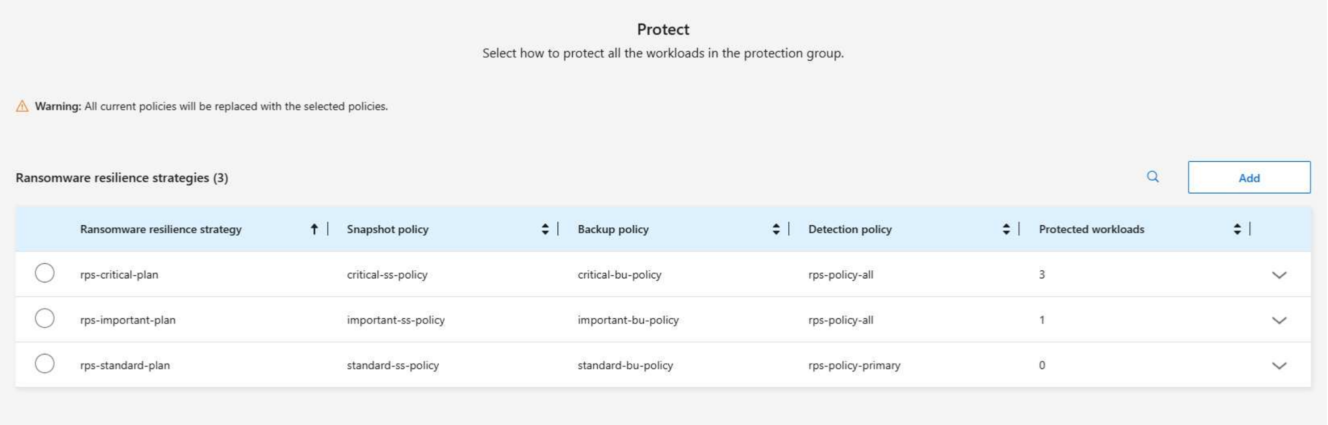
Select workloads with no other policy source or with NetApp Backup and Recovery as a policy source.

□	Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection status
□	FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	None
□	LUN_storage_01	Block	aws-connector-us-east-1	Critical	n/a	Protected	Active
□	MySQL_8009	MySQL	aws-connector-us-east-1	Critical	n/a	At risk	None
□	MySQL_9294	MySQL	aws-connector-us-east-1	Critical	n/a	Protected	Active
□	Oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	At risk	None

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**.



Protect

Select how to protect all the workloads in the protection group.

Warning: All current policies will be replaced with the selected policies.

Ransomware resilience strategies (3)

	Ransomware resilience strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads
○	rps-critical-plan	critical-ss-policy	critical-bu-policy	rps-policy-all	3
○	rps-important-plan	important-ss-policy	important-bu-policy	rps-policy-all	1
○	rps-standard-plan	standard-ss-policy	standard-bu-policy	rps-policy-primary	0

7. Select the policy to govern the protection for this group.
8. Select **Next**.
9. Review the selections for the protection group.
10. 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.

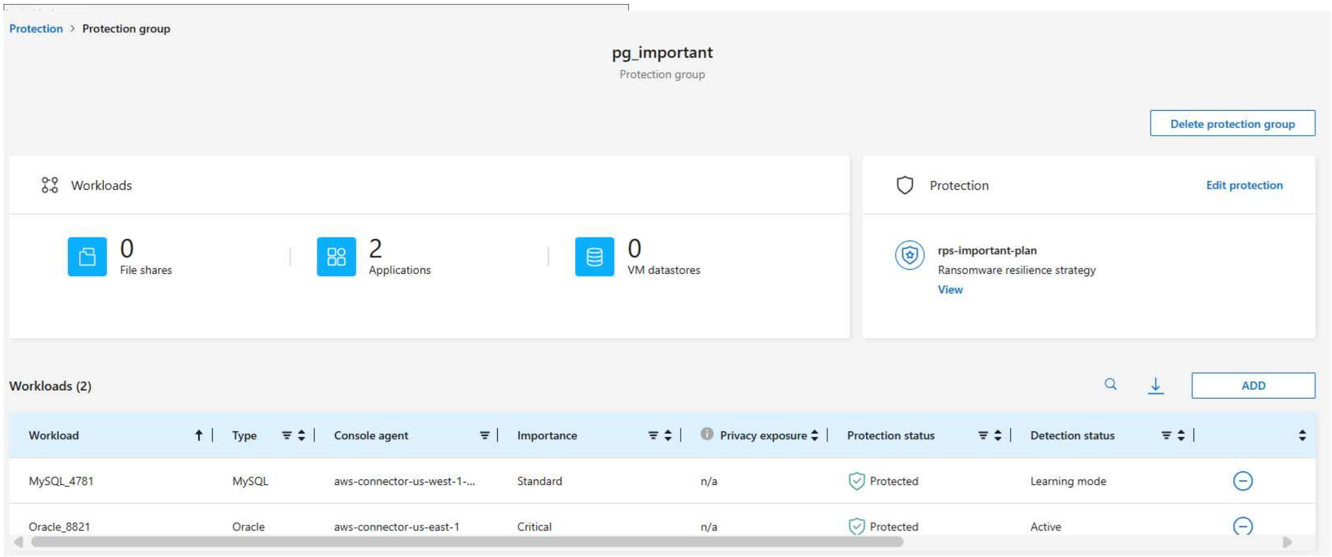
3. From protection group’s overview page, select **Edit protection**.
4. Select an existing protection policy to apply or select **Add** to create a new protection policy. For more information about adding a protection policy see, Create a protection policy. Then select **Save**.
5. In the backup destination 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.



Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection status	
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	n/a	Protected	Learning mode	⊖
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	Active	⊖

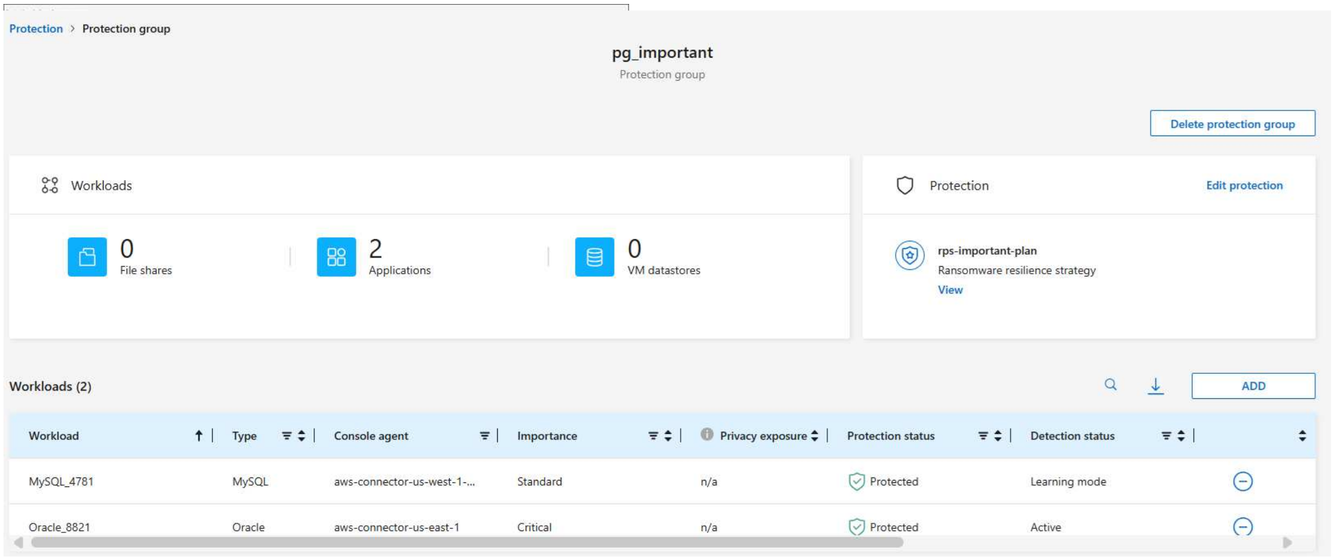
4. From the selected protection group page, select the workload you want to remove from the group and select the **Actions** ••• option.
5. From the Actions menu, select **Remove workload**.
6. Confirm that you want to remove the workload and select **Remove**.

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.



pg_important

Protection group

Workloads

0 File shares

2 Applications

0 VM datastores

Protection

rps-important-plan

Ransomware resilience strategy

Workloads (2)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection status	
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	n/a	Protected	Learning mode	⊖
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	Active	⊖

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

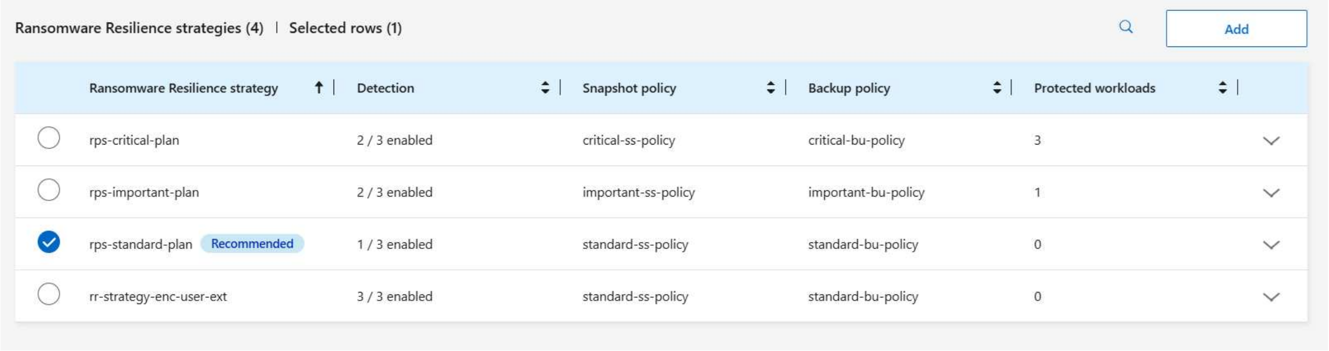
Before you delete a ransomware protection strategy, you might want to view which workloads are protected by that strategy.

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

   The Ransomware protection strategies page displays a list of strategies.



Ransomware Resilience strategies (4) | Selected rows (1)

	Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads	
○	rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3	⌄
○	rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1	⌄
●	rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0	⌄
○	rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0	⌄

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 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.

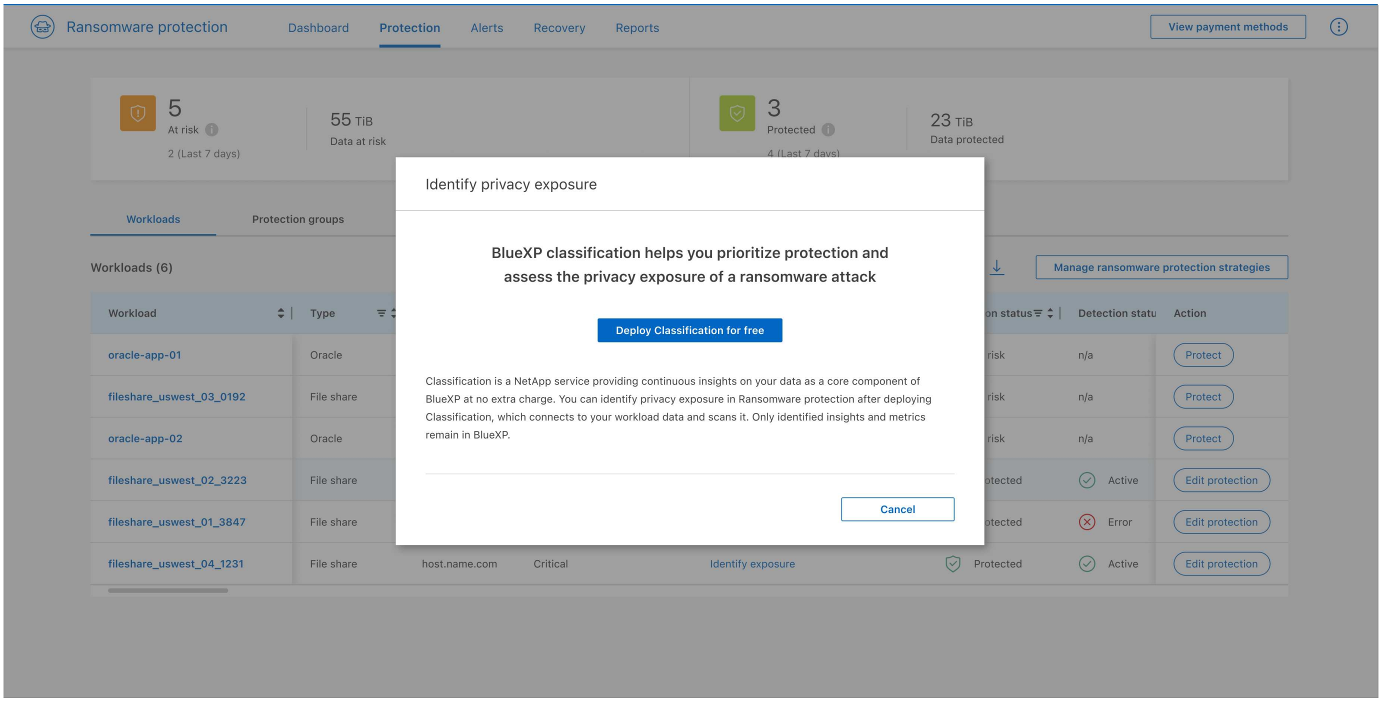
> This process can impact workload importance to help ensure you have the appropriate protection.

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

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.



BlueXP classification helps you prioritize protection and assess the privacy exposure of a ransomware attack

Classification is a NetApp service providing continuous insights on your data as a core component of BlueXP at no extra charge. You can identify privacy exposure in Ransomware protection after deploying Classification, which connects to your workload data and scans it. Only identified insights and metrics remain in BlueXP.

For more information about Data Classification, see:

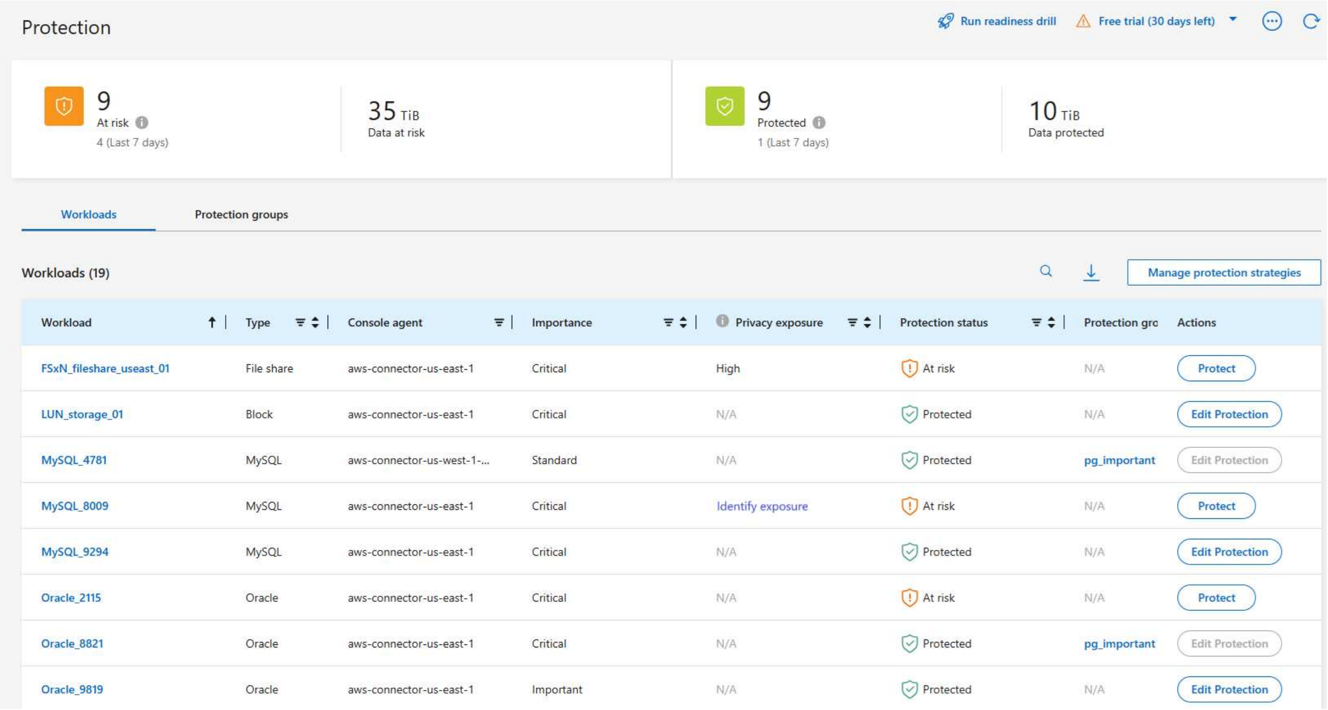
- Learn about Data Classification
- Categories of private data
- Investigate the data stored in your organization

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.



Workloads (19)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Protection gro	Actions
FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	Protect
LUN_storage_01	Block	aws-connector-us-east-1	Critical	N/A	Protected	N/A	Edit Protection
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	N/A	Protected	pg_important	Edit Protection
MySQL_8009	MySQL	aws-connector-us-east-1	Critical	Identify exposure	At risk	N/A	Protect
MySQL_9294	MySQL	aws-connector-us-east-1	Critical	N/A	Protected	N/A	Edit Protection
Oracle_2115	Oracle	aws-connector-us-east-1	Critical	N/A	At risk	N/A	Protect
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	N/A	Protected	pg_important	Edit Protection
Oracle_9819	Oracle	aws-connector-us-east-1	Important	N/A	Protected	N/A	Edit Protection

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

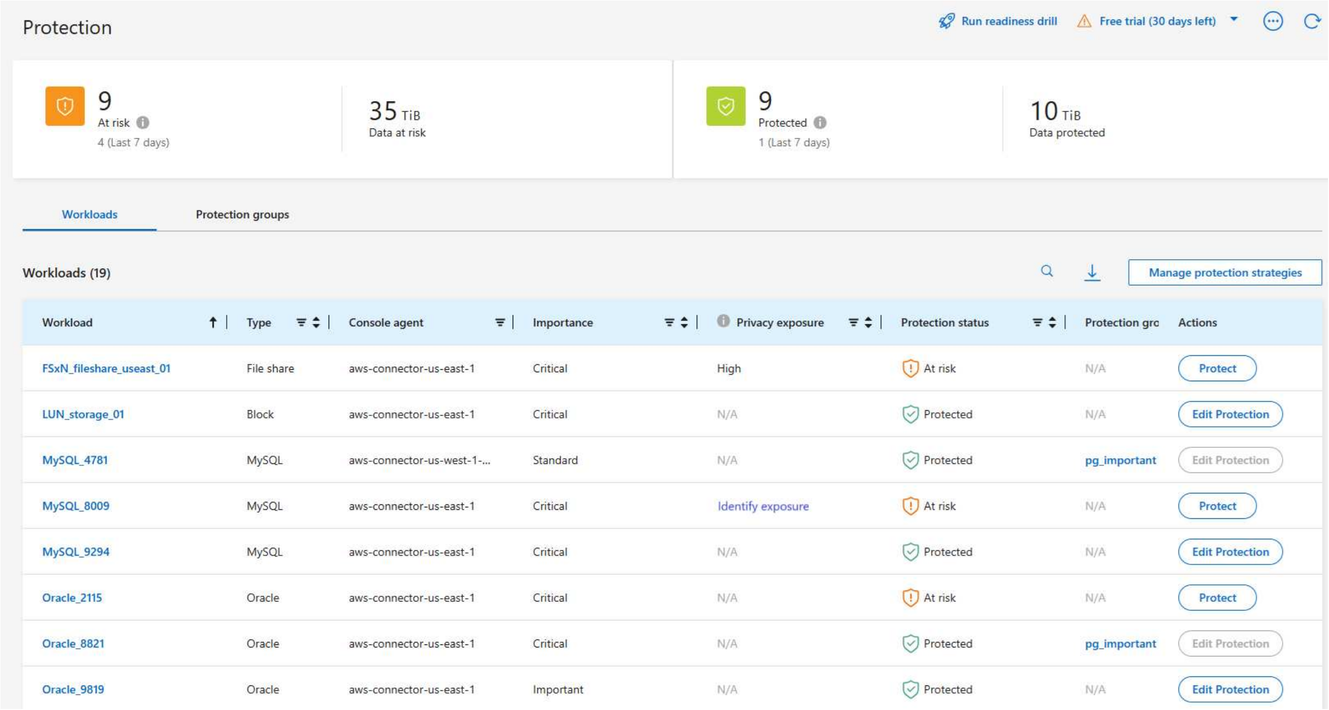
After Data Classification scans for PII, assess the risk.

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.



9 At risk, 4 (Last 7 days)

35 TiB Data at risk

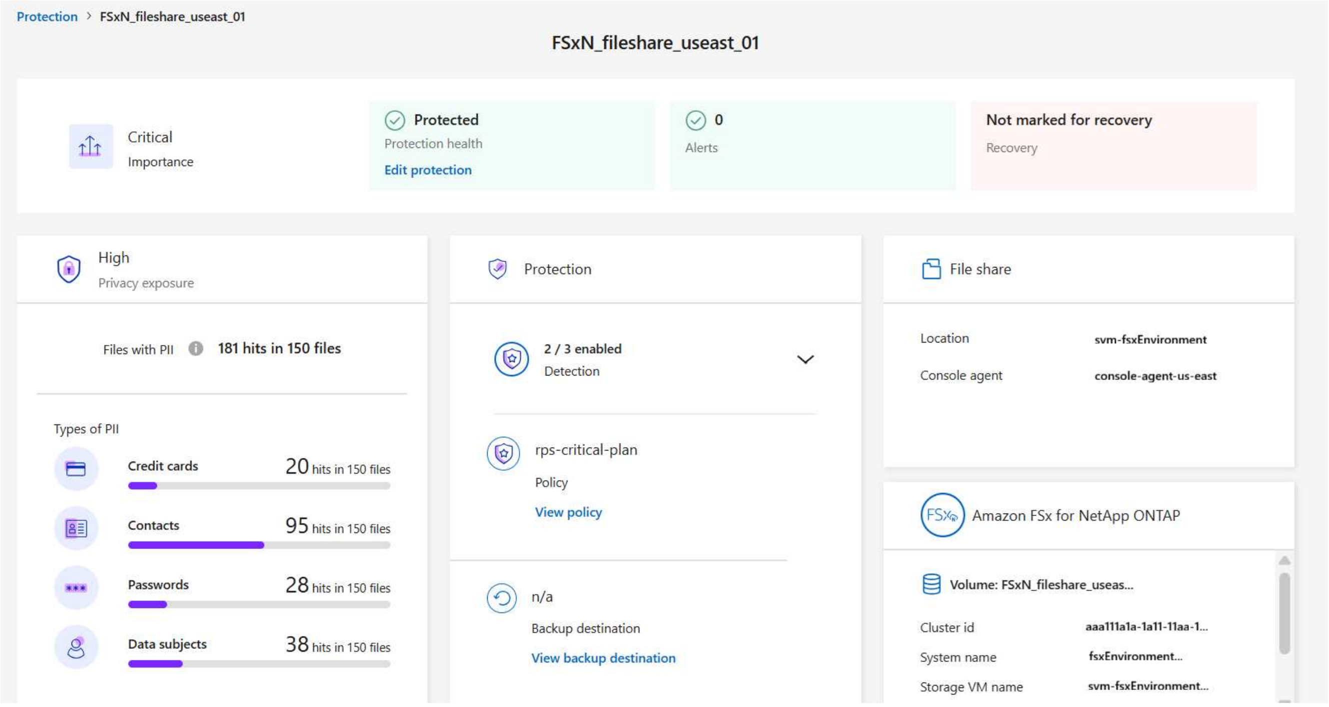
9 Protected, 1 (Last 7 days)

10 TiB Data protected

Workloads (19)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Protection gro	Actions
FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	Protect
LUN_storage_01	Block	aws-connector-us-east-1	Critical	N/A	Protected	N/A	Edit Protection
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	N/A	Protected	pg_important	Edit Protection
MySQL_8009	MySQL	aws-connector-us-east-1	Critical	Identify exposure	At risk	N/A	Protect
MySQL_9294	MySQL	aws-connector-us-east-1	Critical	N/A	Protected	N/A	Edit Protection
Oracle_2115	Oracle	aws-connector-us-east-1	Critical	N/A	At risk	N/A	Protect
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	N/A	Protected	pg_important	Edit Protection
Oracle_9819	Oracle	aws-connector-us-east-1	Important	N/A	Protected	N/A	Edit Protection

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



Critical — Importance

Protected — Protection health

0 — Alerts

Not marked for recovery — Recovery

High — Privacy exposure

Files with PII: 181 hits in 150 files

Types of PII

Credit cards	20 hits in 150 files
Contacts	95 hits in 150 files
Passwords	28 hits in 150 files
Data subjects	38 hits in 150 files

Protection

2 / 3 enabled — Detection

rps-critical-plan — Policy

n/a — Backup destination

File share

Location	svm-fsxEnvironment
Console agent	console-agent-us-east

Amazon FSx for NetApp ONTAP

Volume: FSxN_fileshare_useas...

Cluster id	aaa111a1a-1a11-11aa-1...
System name	fsxEnvironment...
Storage VM name	svm-fsxEnvironment...

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

Handle detected ransomware alerts with NetApp Ransomware Resilience

When NetApp Ransomware Resilience detects a possible attack, it shows 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 address. 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 only based on high entropy.

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 one of the following states:

- **New**: All incidents are marked "new" when they are first identified.
- **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 cannot change this back. 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

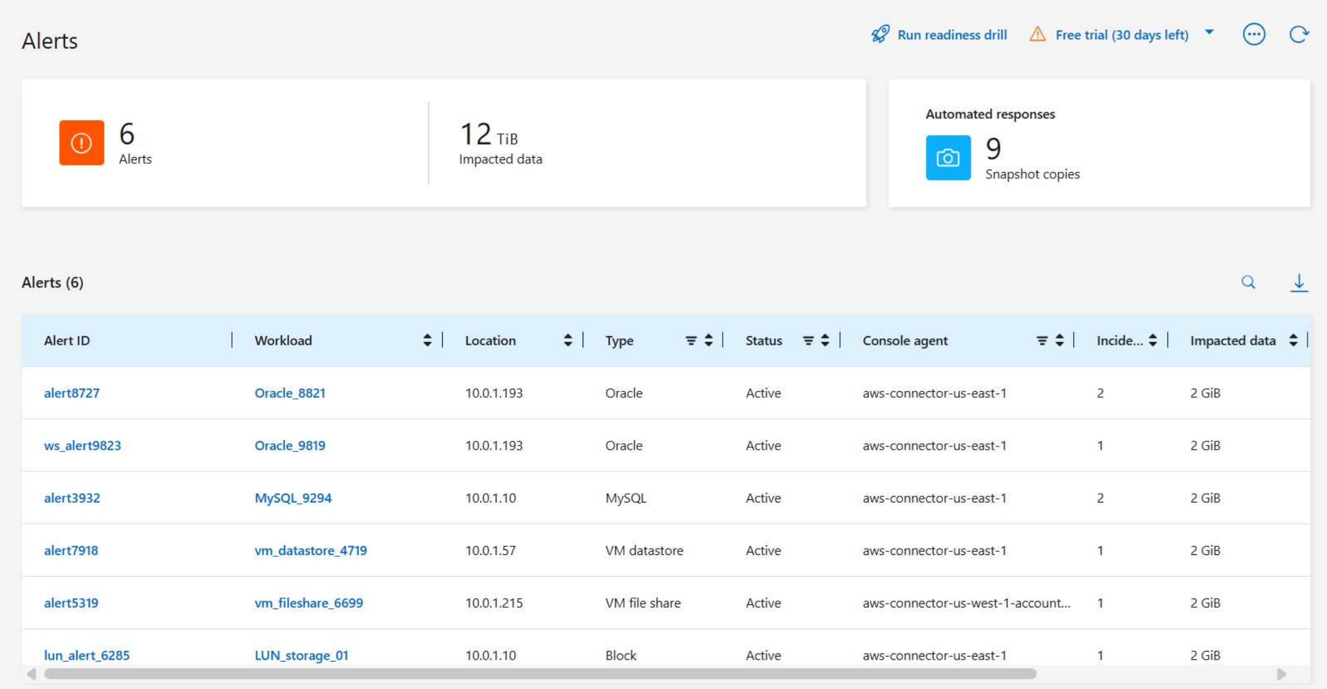
You can access alerts from the Ransomware Resilience Dashboard or from the **Alerts** tab.

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 BlueXP access roles for all services.

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 Alerts

12 TiB Impacted data

Automated responses

9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

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. The email contains information about the alert, including the severity and resources impacted.

You can receive email notifications for Ransomware Resilience alerts. This feature helps you to stay informed about alerts, their severity, and resources impacted.

To subscribe to email notifications, refer to Set email notification settings.

1. In Ransomware Resilience , go to the **Settings** page.
2. Under **Notifications**, locate the email notification settings.
3. Enter the email address where you want to receive alerts.

4. Save your changes.

You will now receive email notifications when new alerts are generated.

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 BlueXP access roles for all services.

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.

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

What details appear?
The details that appear depend on how the alert was triggered:

- Triggered by the Autonomous Ransomware Protection feature in ONTAP. This detects malicious activity based on the behavior of the files in the volume.
- Triggered by Data Infrastructure Insights Workload security. This requires a license for Data Infrastructure Insights Workload security and that you enable it in Ransomware Resilience . This feature detects anomalous user behavior in your storage workloads and enables you to block that user from further access.

  To enable Workload security in Ransomware Resilience , go to the **Settings** page and select the **Workload security connection** option.

  For an overview of Data Infrastructure Insights Workload security, review About Workload security.

> If you don’t have a license for Data Infrastructure Workload security and don’t enable it in Ransomware Resilience , you won’t see the anomalous user behavior information.

When malicious activity occurs, an alert is generated and an automated snapshot is taken.

View malicious activity from Autonomous Ransomware Protection only

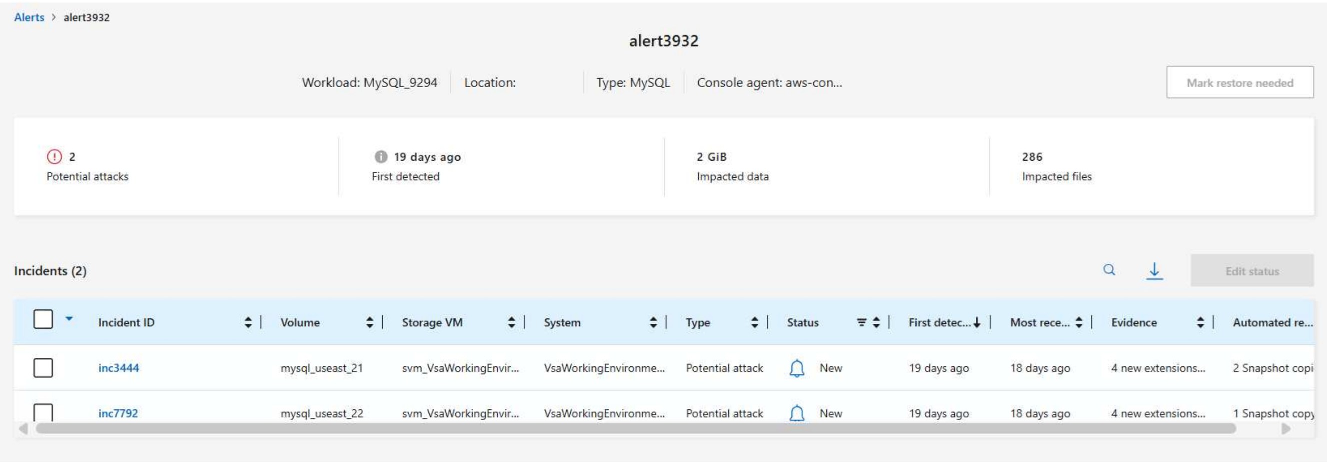
When Autonomous Ransomware Protection triggers an alert in Ransomware Resilience , you can view the following details:

- 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.



alert3932

Workload: MySQL_9294 | Location: | Type: MySQL | Console agent: aws-con...

2 Potential attacks	19 days ago First detected	2 GiB Impacted data	286 Impacted files

Incidents (2)

□	Incident ID	Volume	Storage VM	System	Type	Status	First detec...	Most rece...	Evidence	Automated re...
□	inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
□	inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copy

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

View anomalous user behavior in Data Infrastructure Insights Workload security

When Data Infrastructure Insights Workload security triggers an alert in Ransomware Resilience , you can view the suspicious user, block the user, and investigate the user activity directly in Data Infrastructure Insights Workload security.

These features are in addition to the details available from just Autonomous Ransomware Protection.

Before you begin

This option requires a license for Data Infrastructure Insights Workload security and that you enable it in Ransomware Resilience .

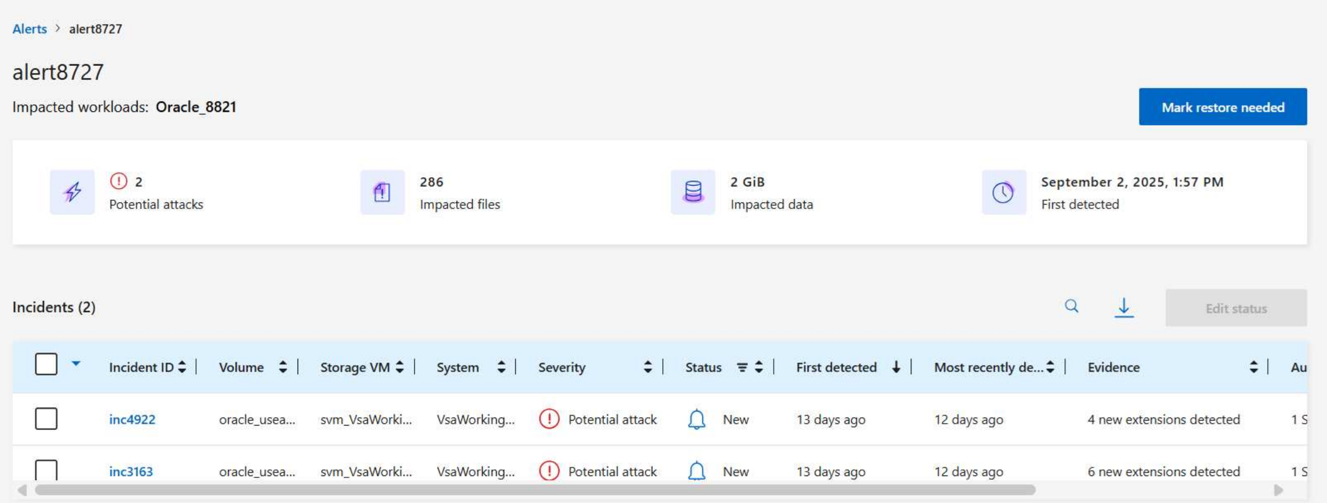
To enable Workload security in Ransomware Resilience , do the following:

1. Go to the **Settings** page.
2. Select the **Workload Security connection** option.

   For details, 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.



Alerts > alert8727

alert8727

Impacted workloads: **Oracle_8821**

2 Potential attacks

286 Impacted files

2 GiB Impacted data

September 2, 2025, 1:57 PM First detected

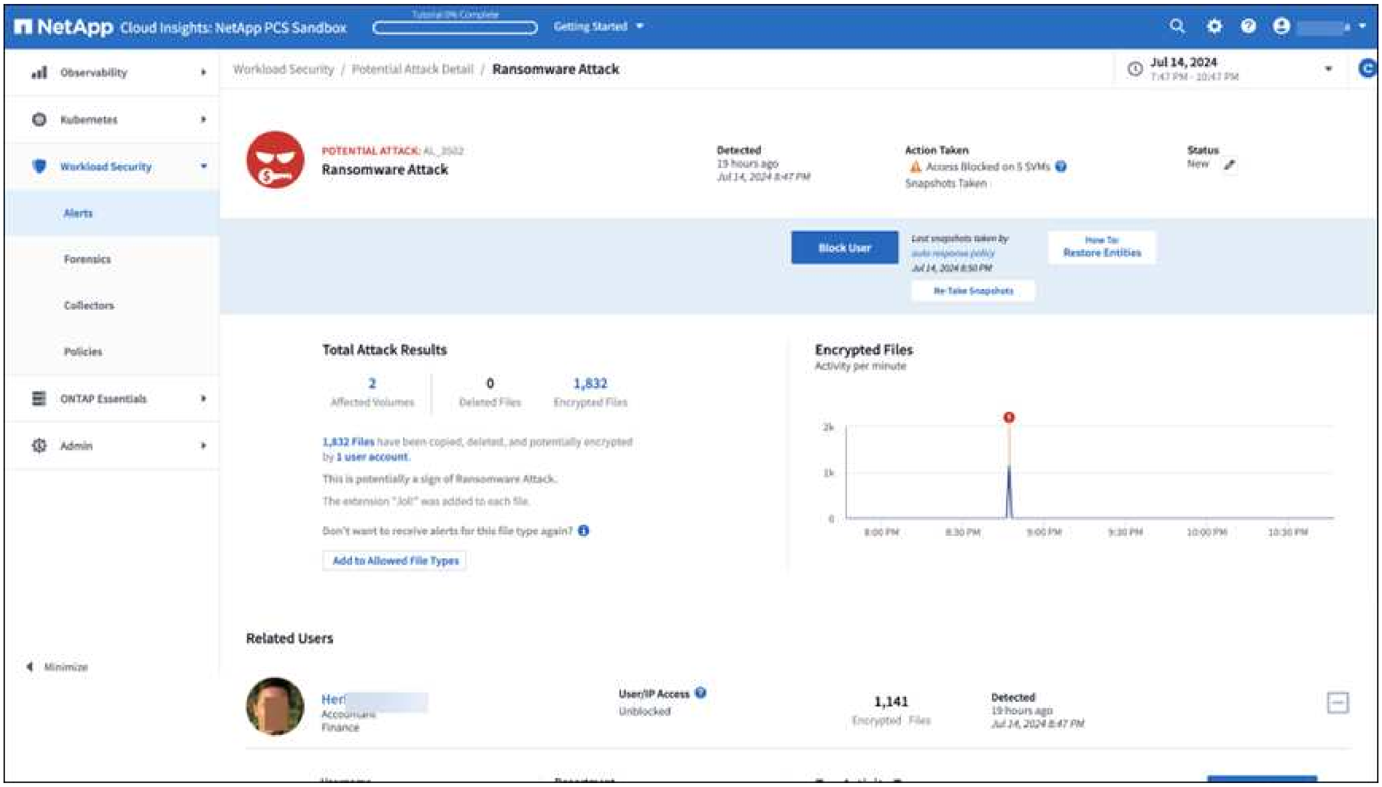
Incidents (2)

□	Incident ID	Volume	Storage VM	System	Severity	Status	First detected	Most recently de...	Evidence	Au
□	inc4922	oracle_usea...	svm_VsaWorki...	VsaWorking...	Potential attack	New	13 days ago	12 days ago	4 new extensions detected	1 S
□	inc3163	oracle_usea...	svm_VsaWorki...	VsaWorking...	Potential attack	New	13 days ago	12 days ago	6 new extensions detected	1 S

4. To block a suspected user from further access in your environment that is monitored by the Console, select the **Block user** link.
5. Research the alert or an incident in the alert:
   a. To research the alert further in Data Infrastructure Insights Workload security, select the **Investigate in Workload security** link.
   b. Select an incident to review the details of the incident.

Data Infrastructure Insights Workload Security opens in a new tab.

+



[redacted]

Workload Security / Potential Attack Detail / Ransomware Attack

Jul 14, 2024
7:47 PM - 10:47 PM

POTENTIAL ATTACK: AL_3502
Ransomware Attack

Detected
19 hours ago
Jul 14, 2024 8:47 PM

Action Taken
Access Blocked on 5 SVMs
Snapshots Taken

Status
New

Last snapshots taken by
auto response policy
Jul 14, 2024 8:50 PM

Total Attack Results

2 Affected Volumes | 0 Deleted Files | 1,832 Encrypted Files

1,832 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of Ransomware Attack.

The extension ".lol" was added to each file.

Don't want to receive alerts for this file type again?

Related Users

[redacted]
Finance

User/IP Access
Unblocked

1,141
Encrypted Files

Detected
19 hours ago
Jul 14, 2024 8:47 PM

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

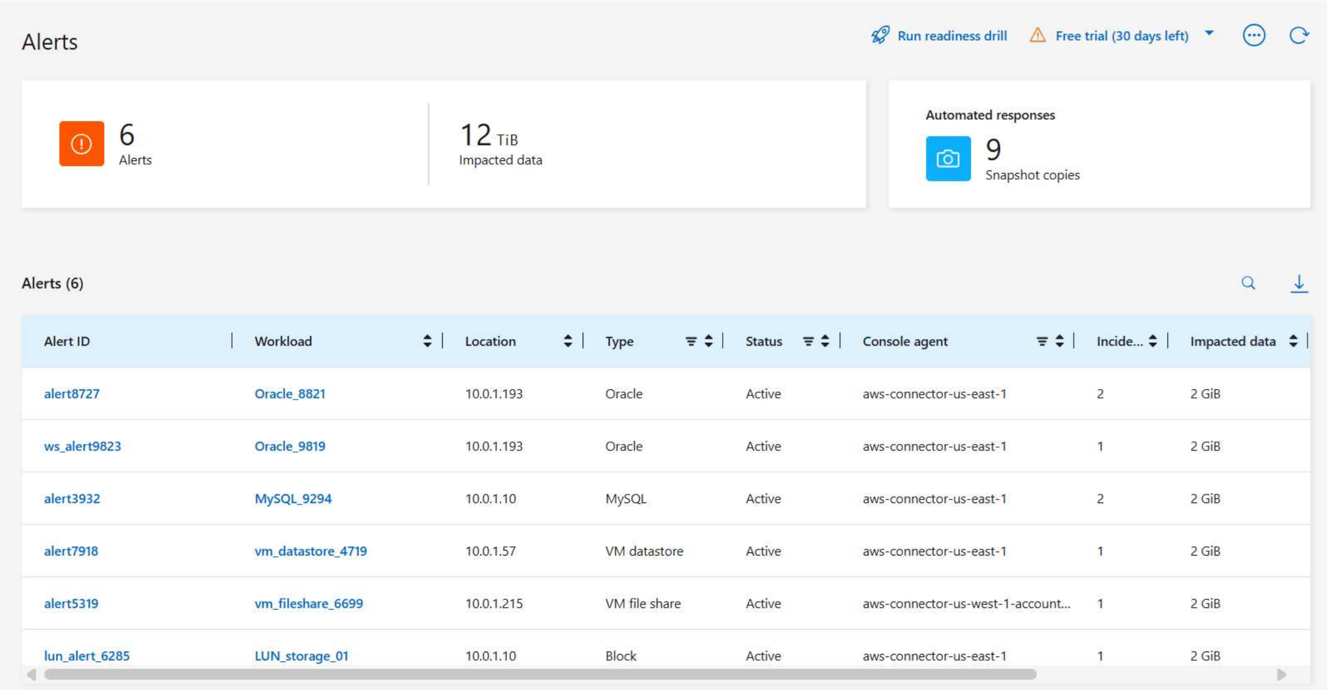
After stopping the attack, notify your storage administrator that the data is ready so they can start recovery.

Required Console role

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

Steps

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



Alerts

6 Alerts

12 TiB Impacted data

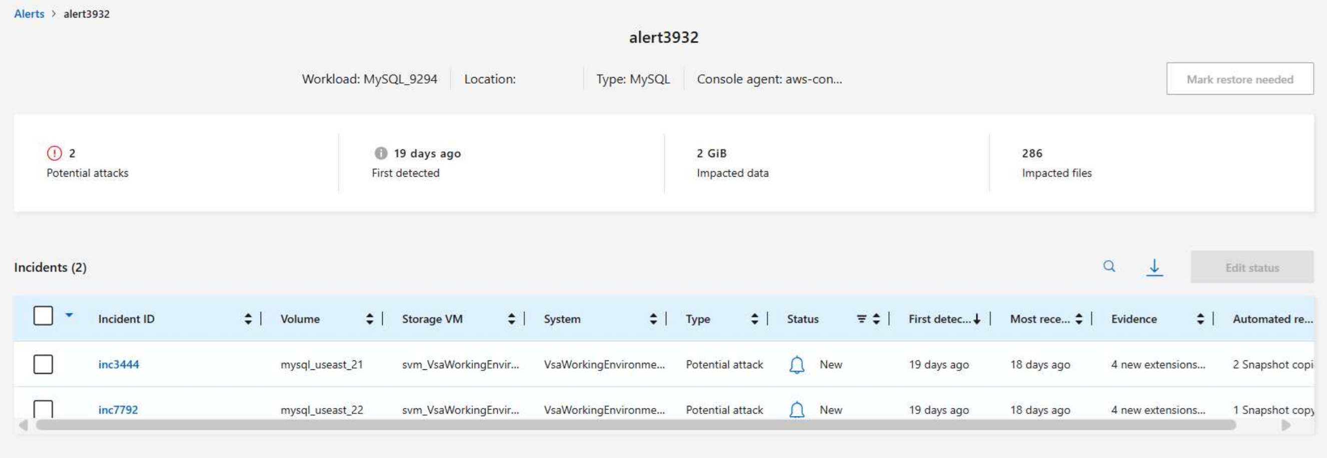
Automated responses

9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

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



alert3932

Workload: MySQL_9294 | Location: | Type: MySQL | Console agent: aws-con...

2 Potential attacks

19 days ago First detected

2 GiB Impacted data

286 Impacted files

Incidents (2)

□	Incident ID	Volume	Storage VM	System	Type	Status	First detec...	Most rece...	Evidence	Automated re...
□	inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
□	inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copy

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 the previous condition is not met, 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, associates it with normal operations, and doesn't initiate an alert on such a behavior again.

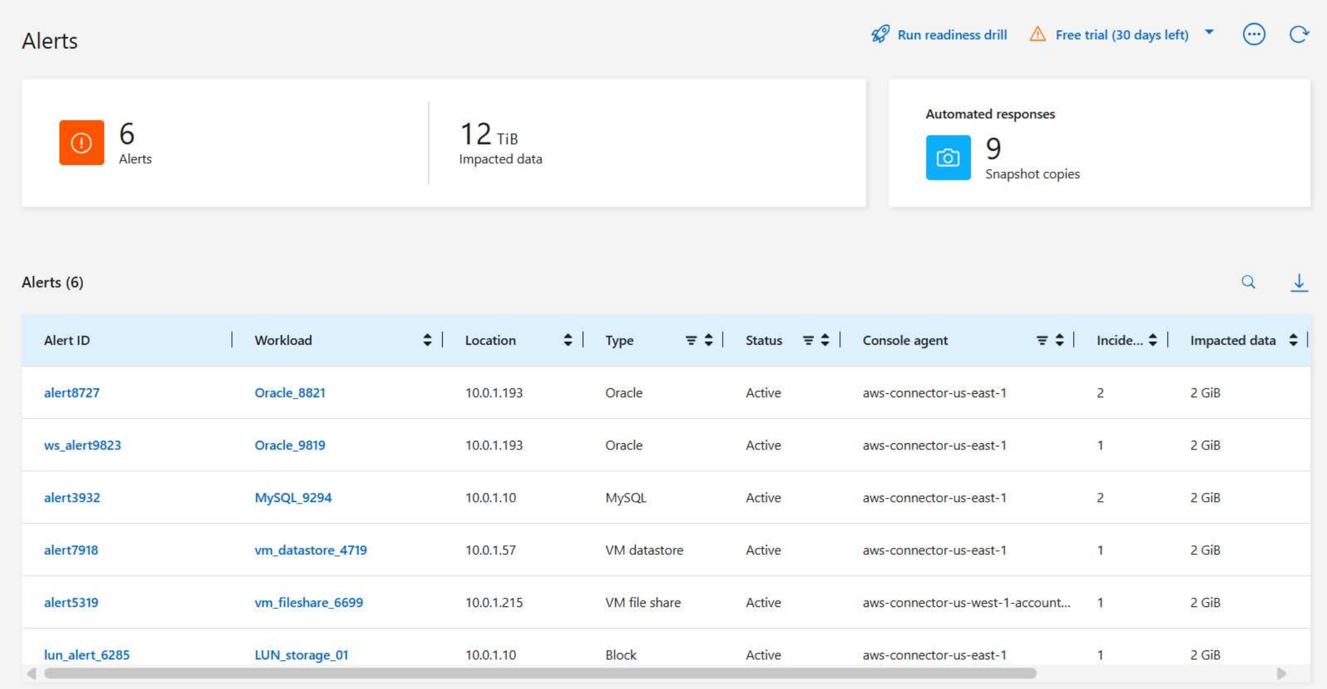
If you dismiss a workload, all snapshot copies taken automatically in response to a potential ransomware attack are permanently deleted.

> If you dismiss an alert, you cannot change that status back to any other status and you cannot 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 Console access roles for all services.

Steps

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



6 Alerts

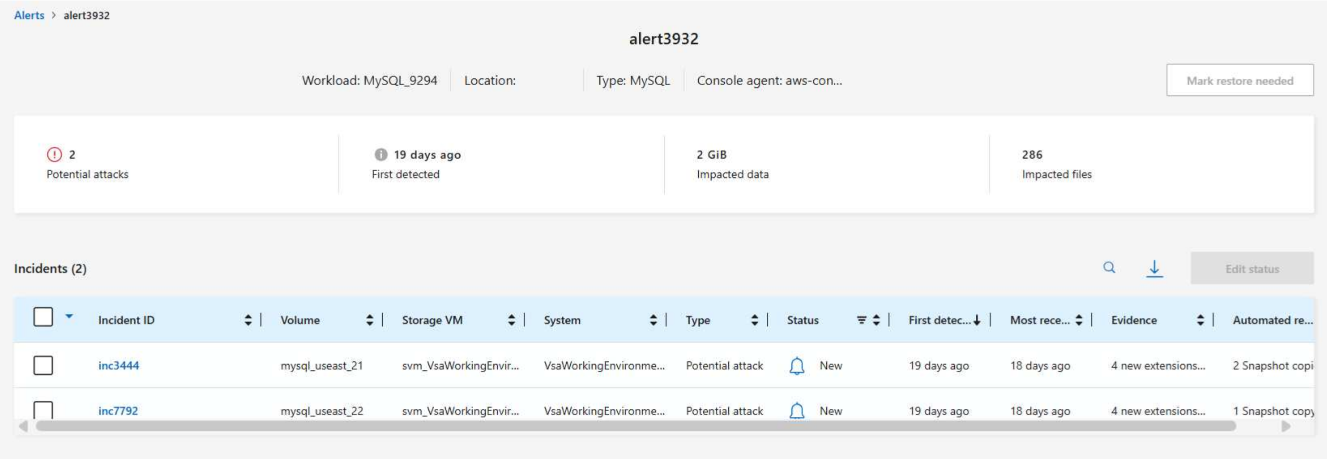
12 TiB Impacted data

Automated responses
9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

2. In the Alerts page, select the alert.



alert3932

Workload: MySQL_9294 | Location: | Type: MySQL | Console agent: aws-con...

2 Potential attacks

19 days ago First detected

2 GiB Impacted data

286 Impacted files

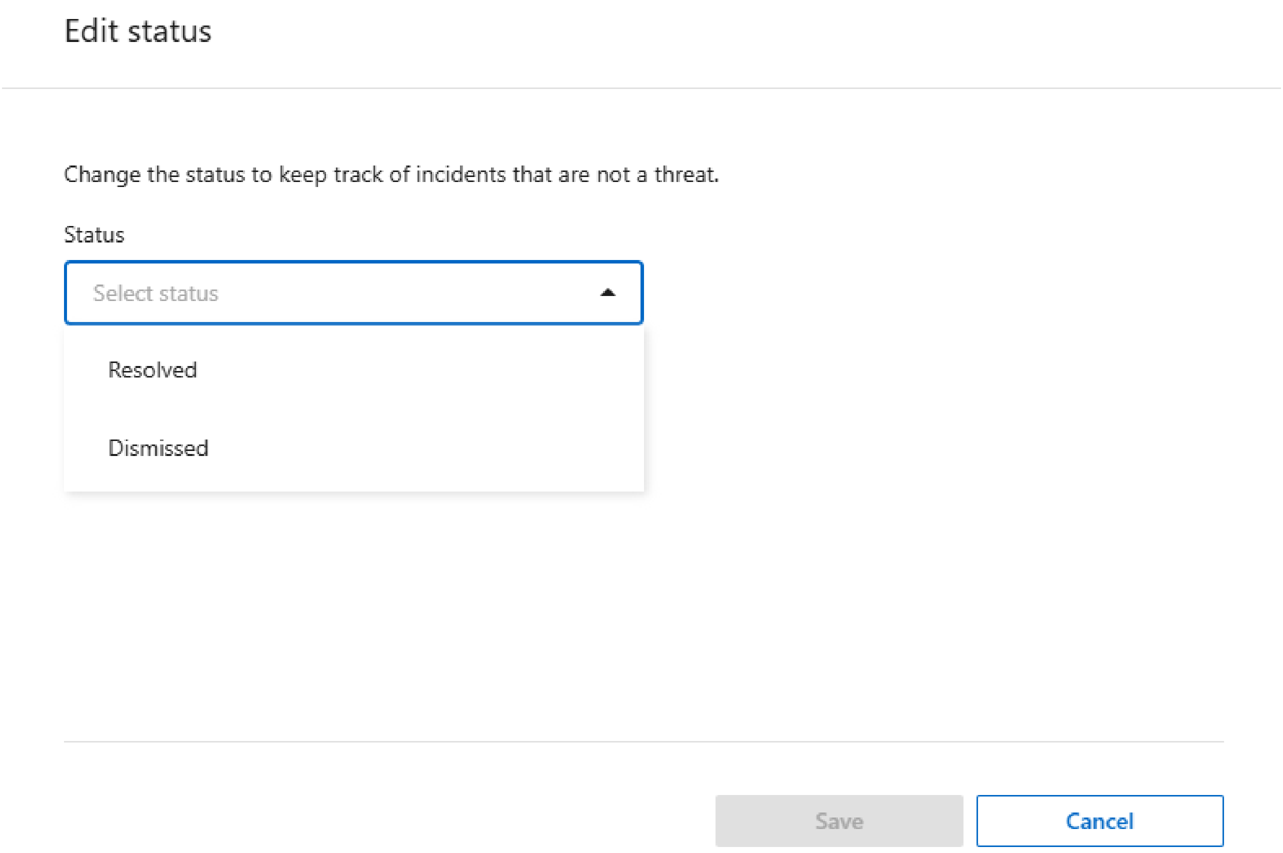
Incidents (2)

□	Incident ID	Volume	Storage VM	System	Type	Status	First detec...	Most rece...	Evidence	Automated re...
□	inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
□	inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copy

3. Select one or more incidents. Or, 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.



Edit status

Change the status to keep track of incidents that are not a threat.

Status

5. From the Edit status box, select the **“Dismissed”** status.

   Additional information about the workload and that 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.

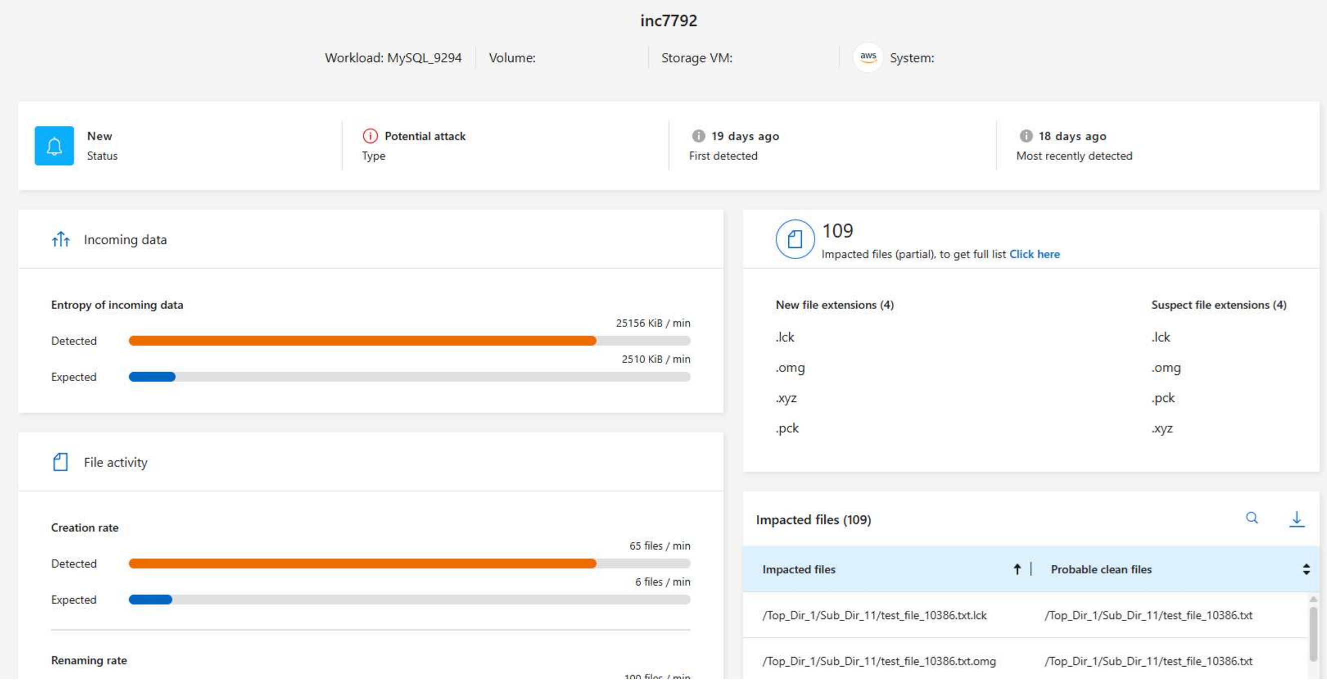
Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Console access roles for all services.

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.



inc7792

Workload: MySQL_9294 | Volume: | Storage VM: | aws System:

New	Potential attack	19 days ago	18 days ago
Status	Type	First detected	Most recently detected

Incoming data

Entropy of incoming data

Detected: 25156 KiB / min

Expected: 2510 KiB / min

File activity

Creation rate

Detected: 65 files / min

Expected: 6 files / min

Renaming rate

100 files / min

109

Impacted files (partial), to get full list Click here

New file extensions (4)	Suspect file extensions (4)
.lck	.lck
.omg	.omg
.xyz	.pck
.pck	.xyz

Impacted files (109)

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.lck	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.omg	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt

5. For that incident, select the download icon and 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.

   [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 Console access roles for all services.

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 Console access roles for all services.

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.

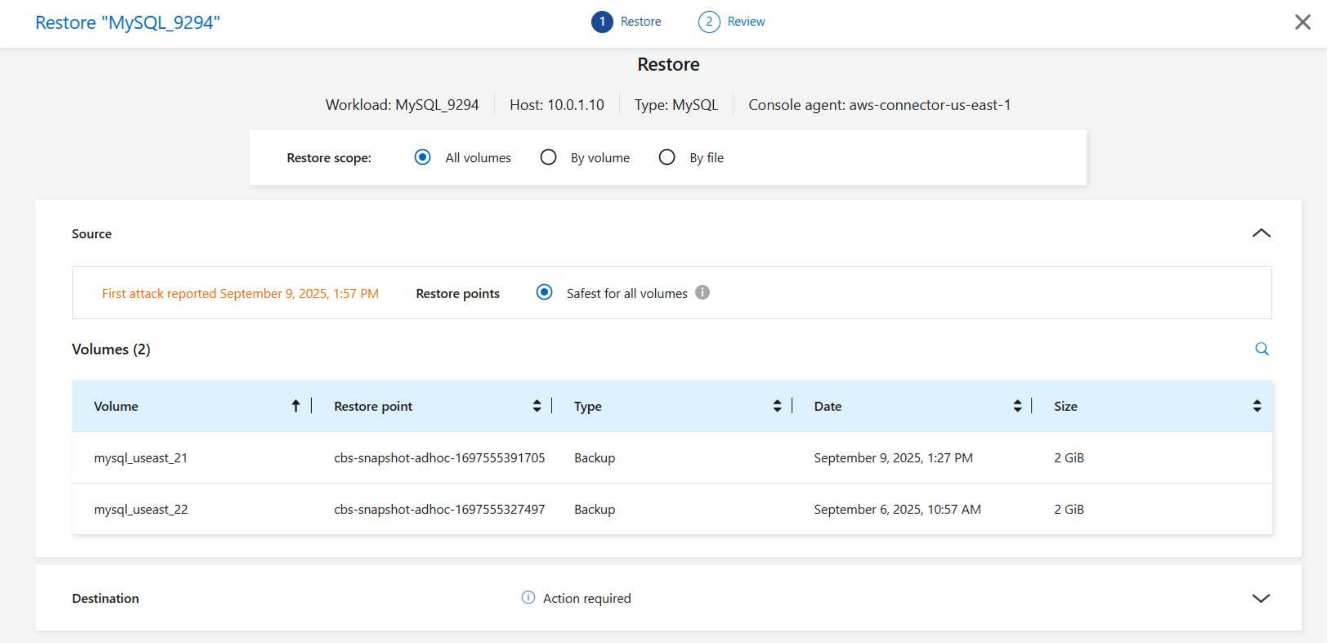
        > ⓘ For SAN workloads, you can only restore by workload.

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**.



Restore

Workload: MySQL_9294 | Host: 10.0.1.10 | Type: MySQL | Console agent: aws-connector-us-east-1

Restore scope: ● All volumes ○ By volume ○ By file

Source

First attack reported September 9, 2025, 1:57 PM

Restore points ● Safest for all volumes

Volumes (2)

Volume	Restore point	Type	Date	Size
mysql_useast_21	cbs-snapshot-adhoc-1697555391705	Backup	September 9, 2025, 1:27 PM	2 GiB
mysql_useast_22	cbs-snapshot-adhoc-1697555327497	Backup	September 6, 2025, 10:57 AM	2 GiB

Destination

Action required

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.

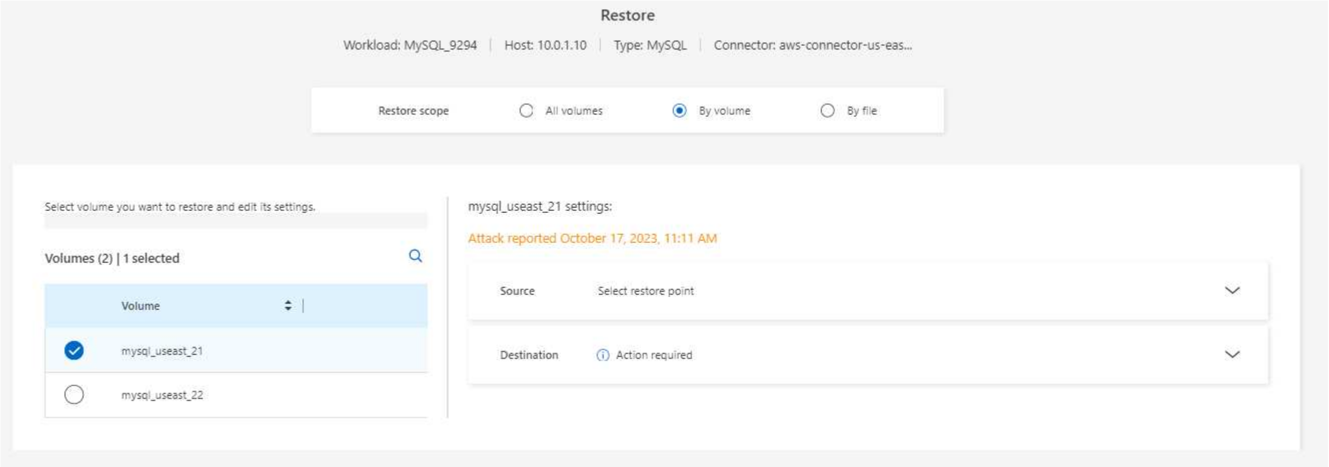
   The new volume name appears as prefix + original volume name + backup name + backup date.

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**.



Restore

Workload: MySQL_9294 | Host: 10.0.1.10 | Type: MySQL | Connector: aws-connector-us-eas...

Restore scope ○ All volumes ● By volume ○ By file

Select volume you want to restore and edit its settings.

Volumes (2) | 1 selected

	Volume
☑	mysql_useast_21
○	mysql_useast_22

mysql_useast_21 settings:

Attack reported October 17, 2023, 11:11 AM

Source: Select restore point

Destination: Action required

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.

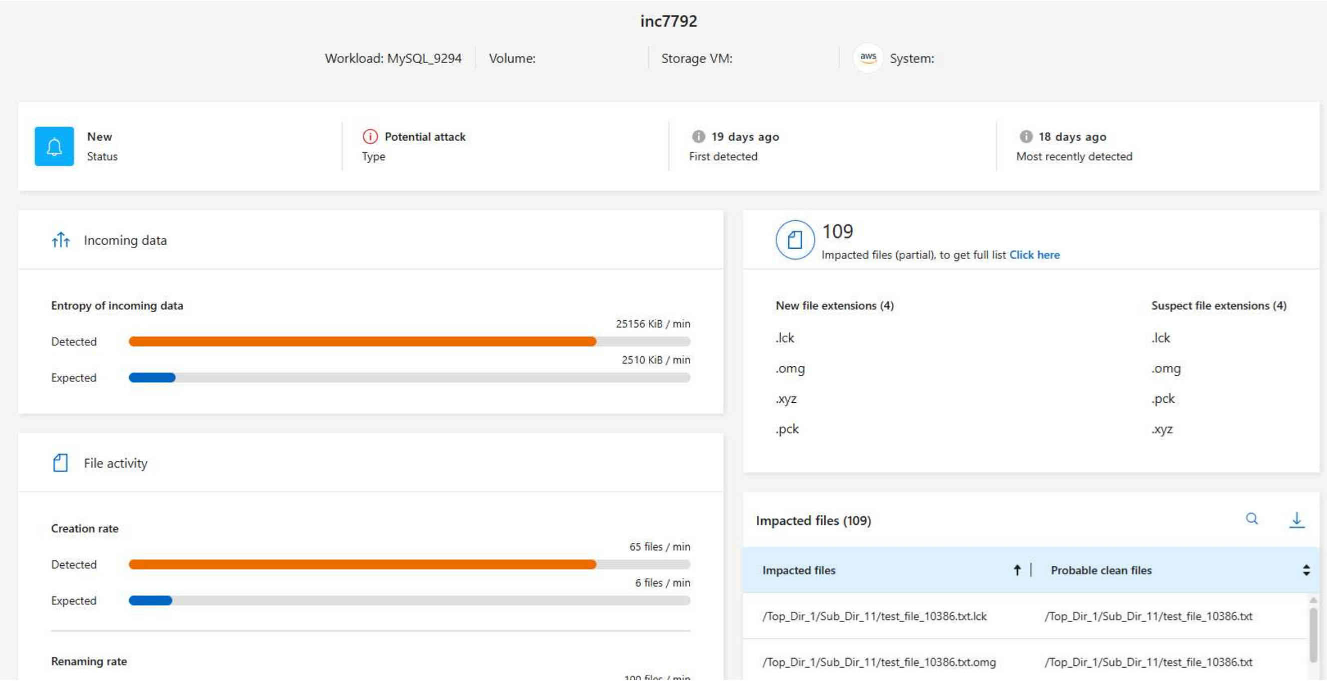
You can restore an application workload at the file level to the same or different system.

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.



inc7792

Workload: MySQL_9294 | Volume: | Storage VM: | System:

New
Status

Potential attack
Type

19 days ago
First detected

18 days ago
Most recently detected

Entropy of incoming data

Detected 25156 KiB / min

Expected 2510 KiB / min

109
Impacted files (partial), to get full list Click here

New file extensions (4)	Suspect file extensions (4)
.lck	.lck
.omg	.omg
.xyz	.pck
.pck	.xyz

Creation rate

Detected 65 files / min

Expected 6 files / min

Renaming rate

100 files / min

Impacted files (109)

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.lck	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.omg	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt

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.

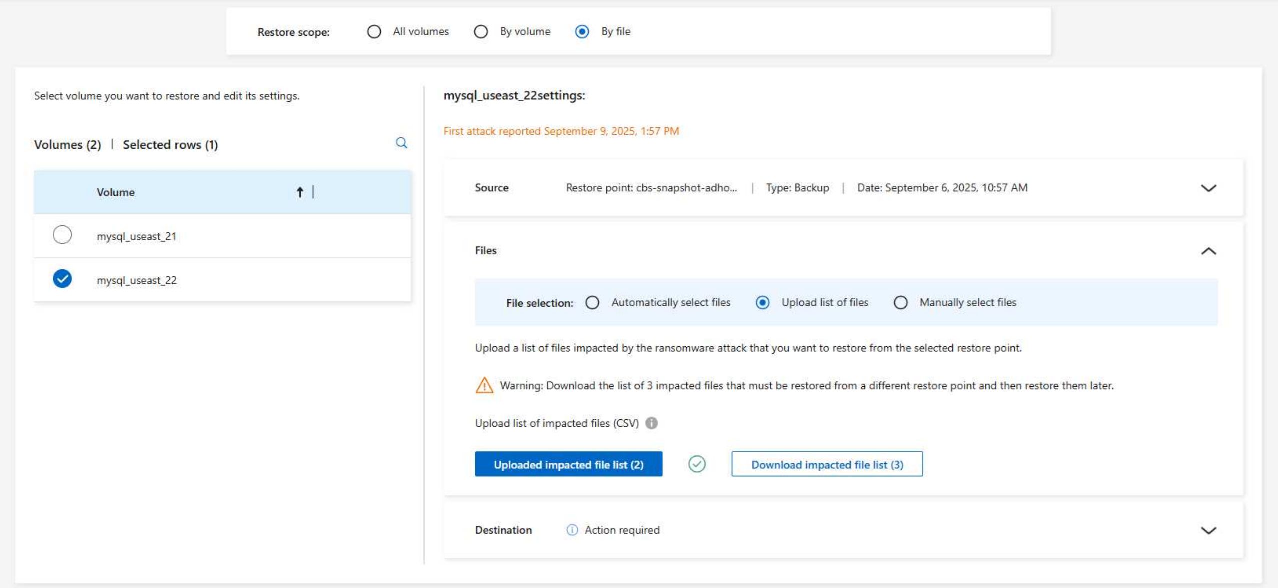
Steps to restore those files

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.



Restore scope: ○ All volumes ○ By volume ● By file

Select volume you want to restore and edit its settings.

Volumes (2) | Selected rows (1)

	Volume
○	mysql_useast_21
●	mysql_useast_22

mysql_useast_22settings:

First attack reported September 9, 2025, 1:57 PM

Source: Restore point: cbs-snapshot-adho... | Type: Backup | Date: September 6, 2025, 10:57 AM

Files

File selection: ○ Automatically select files ● Upload list of files ○ Manually select files

Upload a list of files impacted by the ransomware attack that you want to restore from the selected restore point.

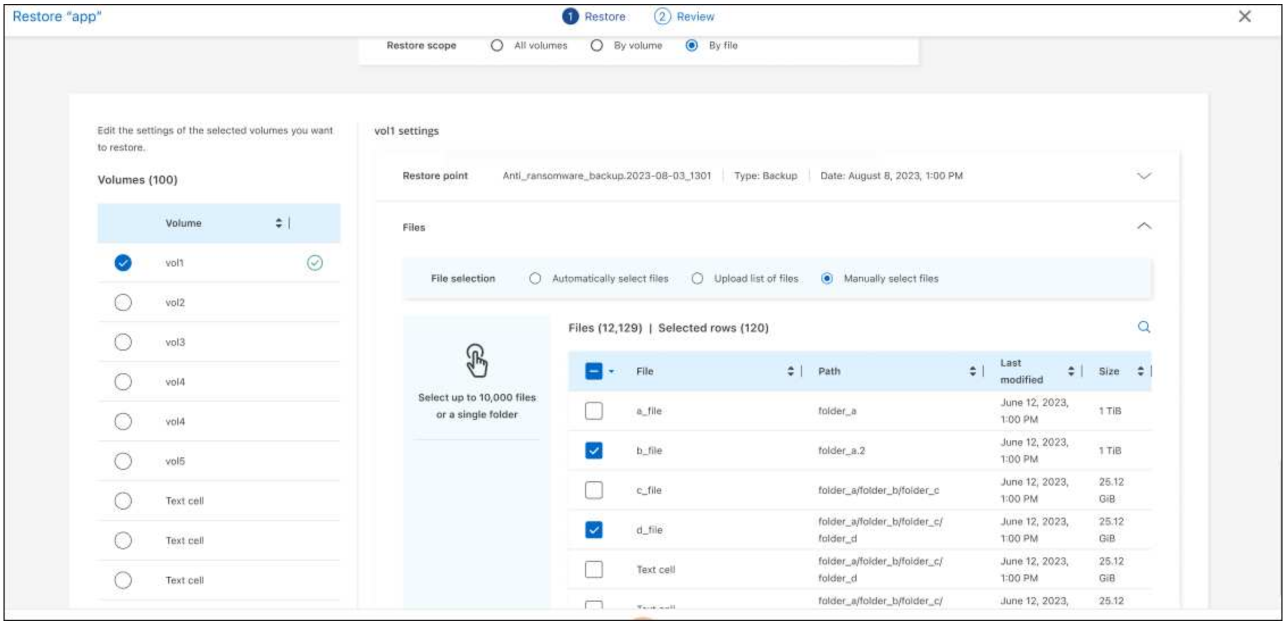
Warning: Download the list of 3 impacted files that must be restored from a different restore point and then restore them later.

Upload list of impacted files (CSV)

Uploaded impacted file list (2)
Download impacted file list (3)

Destination: Action required

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



Restore "app"

Restore scope ○ All volumes ○ By volume ● By file

Edit the settings of the selected volumes you want to restore.

Volumes (100)

	Volume
●	vol1
○	vol2
○	vol3
○	vol4
○	vol4
○	vol5
○	Text cell
○	Text cell
○	Text cell

vol1 settings

Restore point: Anti_ransomware_backup.2023-08-03_1301 | Type: Backup | Date: August 8, 2023, 1:00 PM

Files

File selection ○ Automatically select files ○ Upload list of files ● Manually select files

Select up to 10,000 files or a single folder

Files (12,129) | Selected rows (120)

	File	Path	Last modified	Size
□	a_file	folder_a	June 12, 2023, 1:00 PM	1 TiB
☑	b_file	folder_a.2	June 12, 2023, 1:00 PM	1 TiB
□	c_file	folder_a/folder_b/folder_c	June 12, 2023, 1:00 PM	25.12 GiB
☑	d_file	folder_a/folder_b/folder_c/folder_d	June 12, 2023, 1:00 PM	25.12 GiB
□	Text cell	folder_a/folder_b/folder_c/folder_d	June 12, 2023, 1:00 PM	25.12 GiB
□		folder_a/folder_b/folder_c/	June 12, 2023,	25.12

> 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.

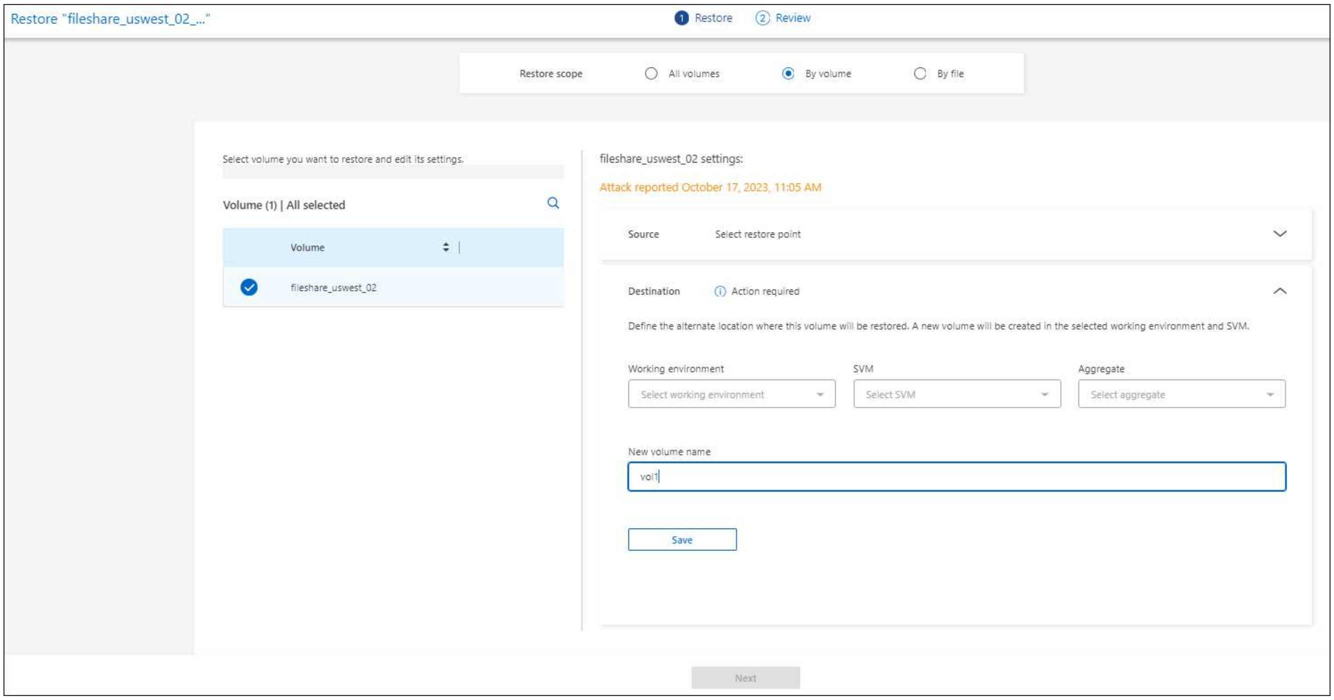
   b. Select the system.
   c. Select the Storage VM.
   d. Optionally, enter the path.

   > 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**.



Restore scope ○ All volumes ● By volume ○ By file

Select volume you want to restore and edit its settings.

Volume (1) | All selected

Volume
✓ fileshare_uswest_02

fileshare_uswest_02 settings:

Attack reported October 17, 2023, 11:05 AM

Source: Select restore point

Destination: ⓘ Action required

Define the alternate location where this volume will be restored. A new volume will be created in the selected working environment and SVM.

Working environment: Select working environment

SVM: Select SVM

Aggregate: Select aggregate

New volume name: vol1

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.

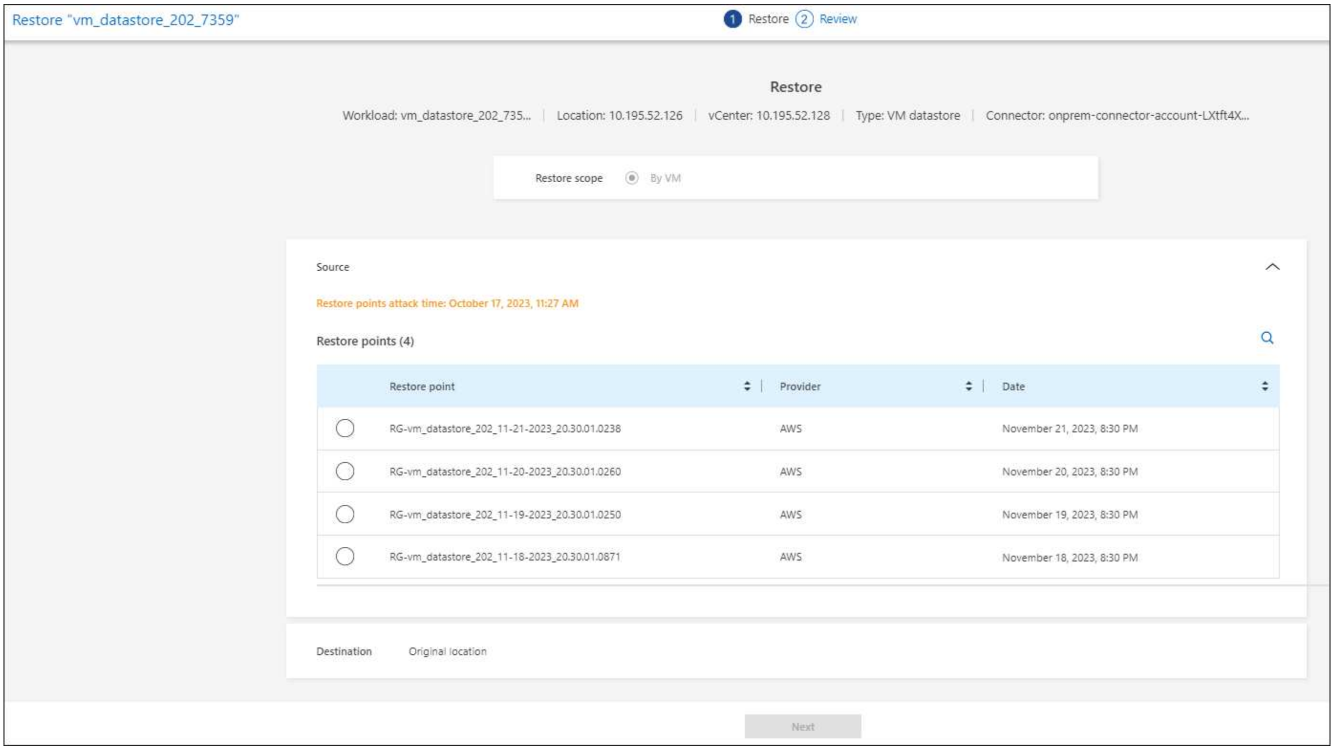
> If you don’t specify a path for the restore, the files will be restored to a new volume at the top-level directory.

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.



Restore "vm_datastore_202_7359"

Restore

Workload: vm_datastore_202_735... | Location: 10.195.52.126 | vCenter: 10.195.52.128 | Type: VM datastore | Connector: onprem-connector-account-LXtft4X...

Restore scope ● By VM

Source

Restore points attack time: October 17, 2023, 11:27 AM

Restore points (4)

	Restore point	Provider	Date
○	RG-vm_datastore_202_11-21-2023_20.30.01.0238	AWS	November 21, 2023, 8:30 PM
○	RG-vm_datastore_202_11-20-2023_20.30.01.0260	AWS	November 20, 2023, 8:30 PM
○	RG-vm_datastore_202_11-19-2023_20.30.01.0250	AWS	November 19, 2023, 8:30 PM
○	RG-vm_datastore_202_11-18-2023_20.30.01.0871	AWS	November 18, 2023, 8:30 PM

Destination Original location

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, you should refresh the data, which also refreshes data that will appear in the files.

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 BlueXP access roles for all services.

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

- **Protection**: Contains 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.

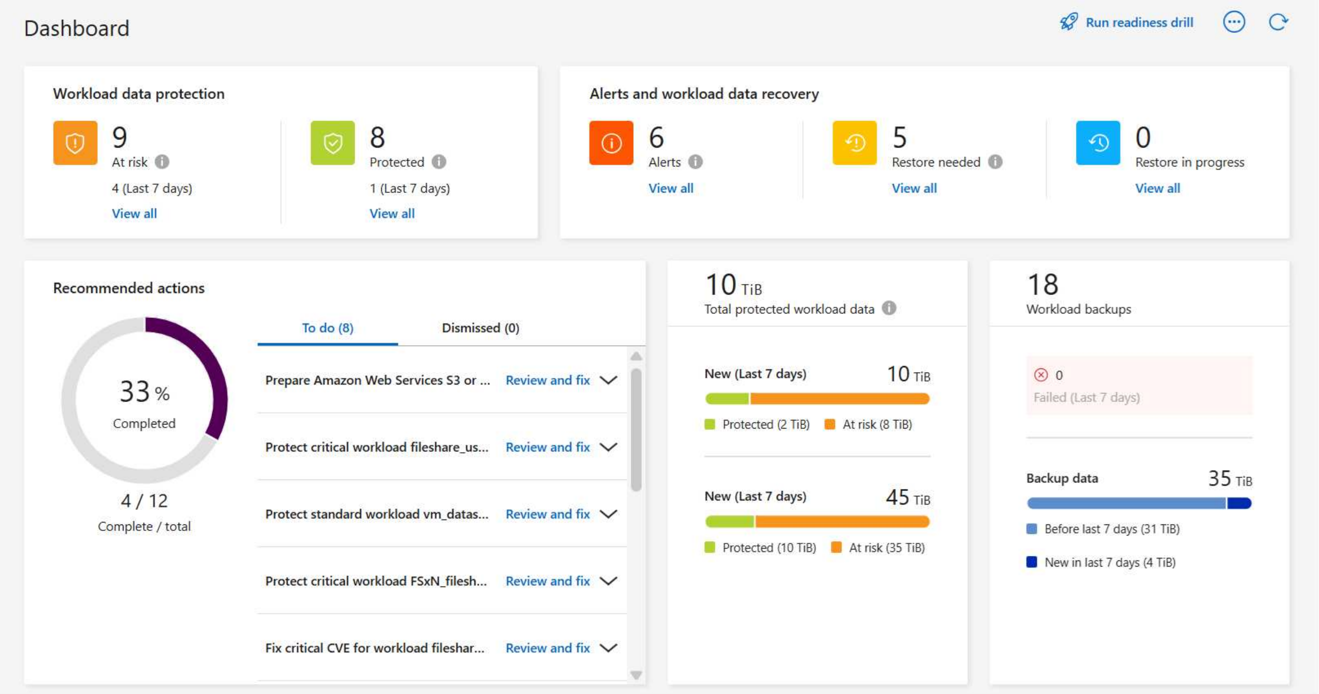
> You can download readiness drill reports only from the **Reports** page.

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

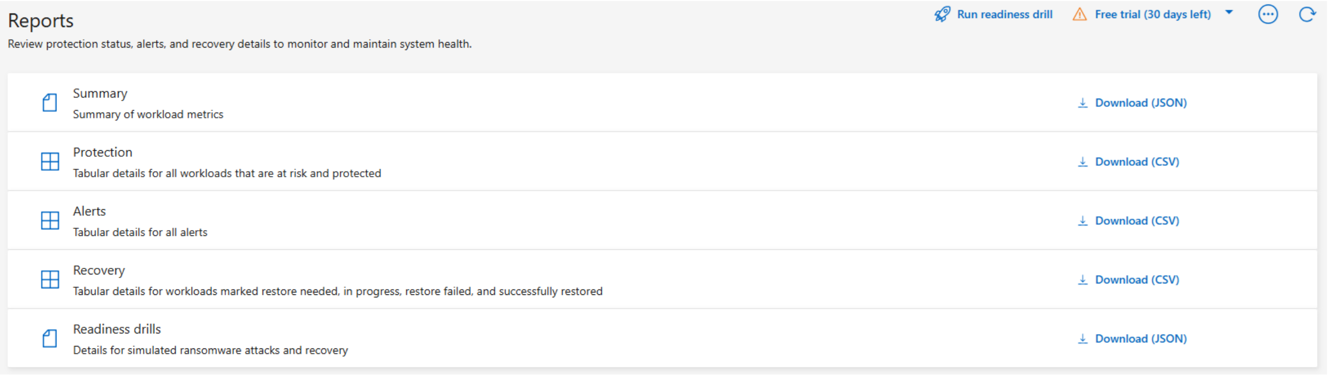
The CSV or JSON files include data for all workloads on all Console systems.

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**.



Reports

Review protection status, alerts, and recovery details to monitor and maintain system health.

Summary Summary of workload metrics	Download (JSON)
Protection Tabular details for all workloads that are at risk and protected	Download (CSV)
Alerts Tabular details for all alerts	Download (CSV)
Recovery Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored	Download (CSV)
Readiness drills Details for simulated ransomware attacks and recovery	Download (JSON)

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account serial number (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in BlueXP).

  This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register BlueXP for NetApp support

To register for support and activate support entitlement, one user in your BlueXP organization (or account) must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your BlueXP organization is registered for support.

   Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP organization is not registered for support. As long as one user in the organization has followed these steps, then your organization has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

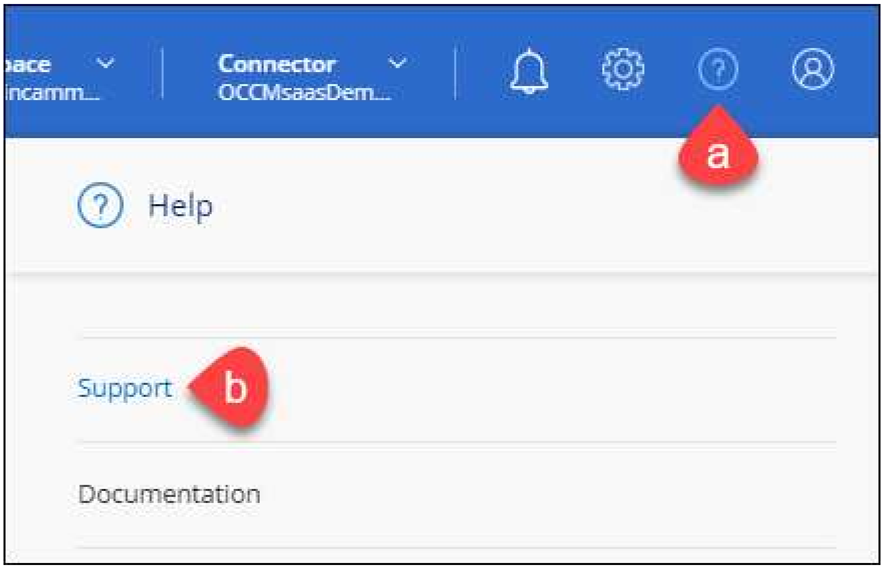
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Brand new to NetApp

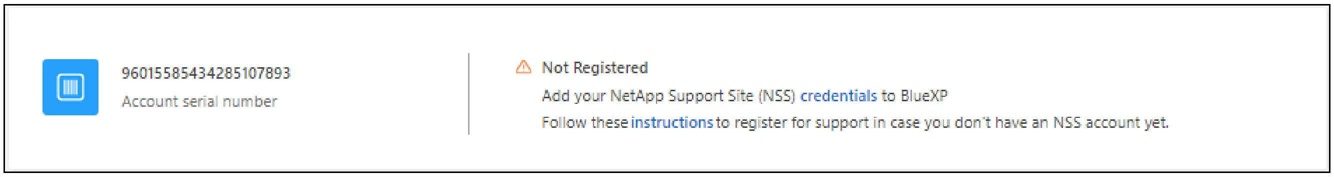
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



96015585434285107893
Account serial number

⚠ Not Registered
Add your NetApp Support Site (NSS) credentials to BlueXP
Follow these instructions to register for support in case you don't have an NSS account yet.

3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP organization is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

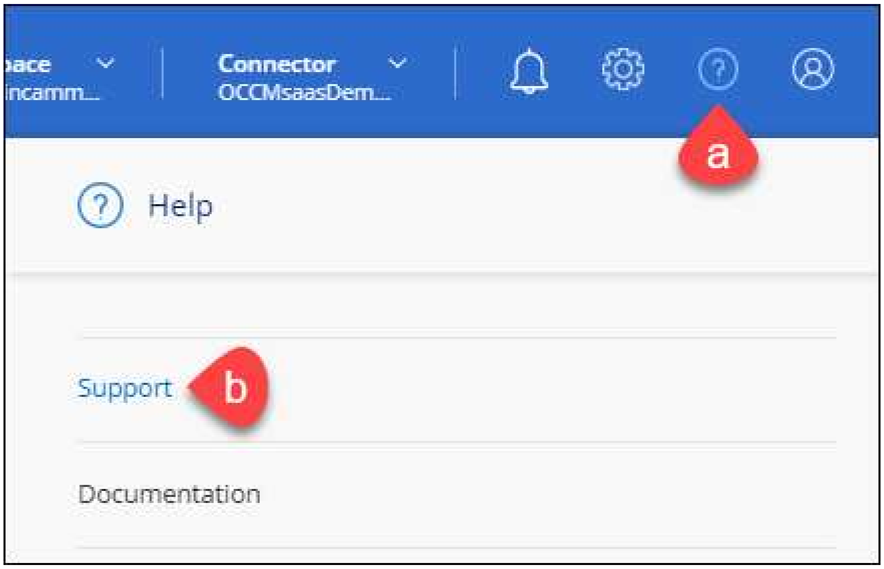
Associating NSS credentials with your BlueXP organization is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP organization ID. Users who belong to the BlueXP organization can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   - The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
   - There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

     "The NSS customer type is not allowed for this account as there are already NSS Users of different type."

     The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

   - Upon successful login, NetApp will store the NSS user name.

     This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

- ◦ If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

  Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- Documentation

  The BlueXP documentation that you're currently viewing.

- Knowledge base

  Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the BlueXP community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. Learn how to manage credentials associated with your BlueXP login.
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be

associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:

    a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

    b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

    - **Service**: Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
    - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

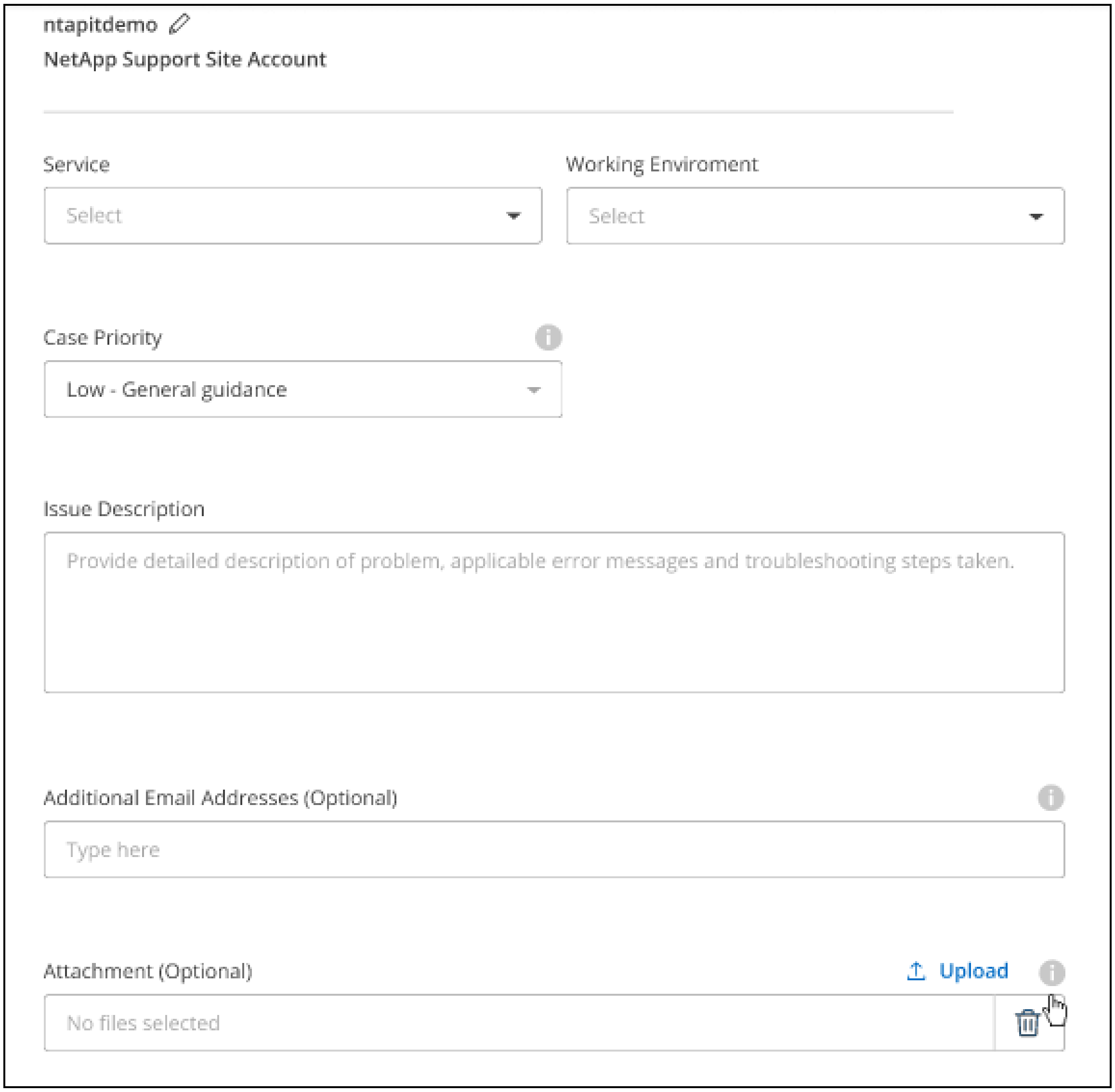
        The list of working environments are within scope of the BlueXP organization (or account), project (or workspace), and Connector you have selected in the top banner of the service.

    - **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

        To learn more details about these priorities, hover your mouse over the information icon next to the field name.

    - **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
    - **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.
    - **Attachment (Optional)**: Upload up to five attachments, one at a time.

        Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



ntapitdemo

NetApp Support Site Account

Service: Select

Working Enviroment: Select

Case Priority: Low - General guidance

Issue Description: Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional): Type here

Attachment (Optional): No files selected

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It’s possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it’s associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

  The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  View the steps below for more details.

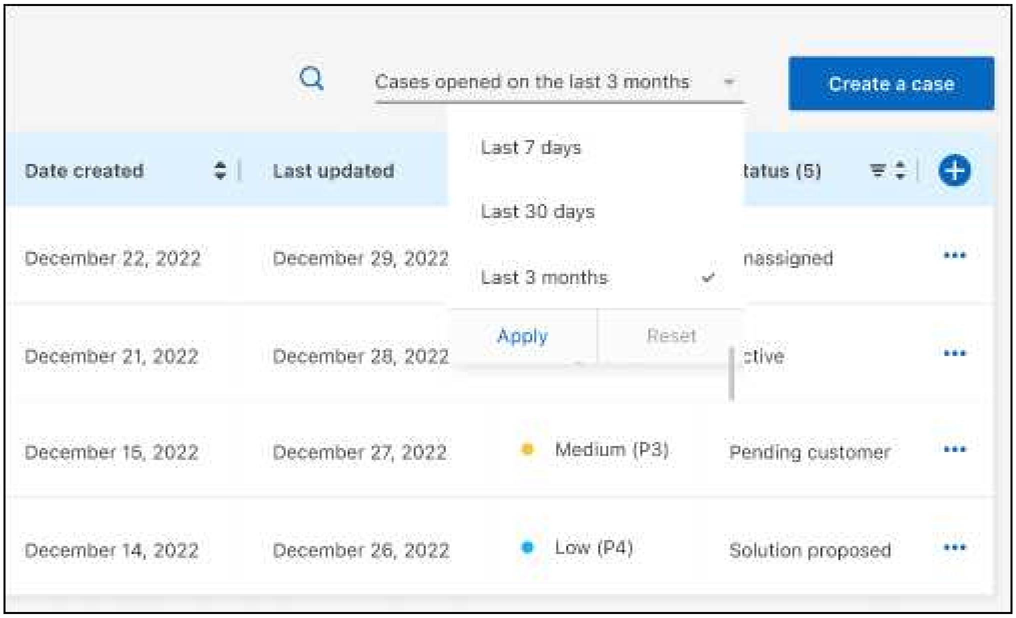
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
   - Under **Organization's cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.



Cases opened on the last 3 months ▾

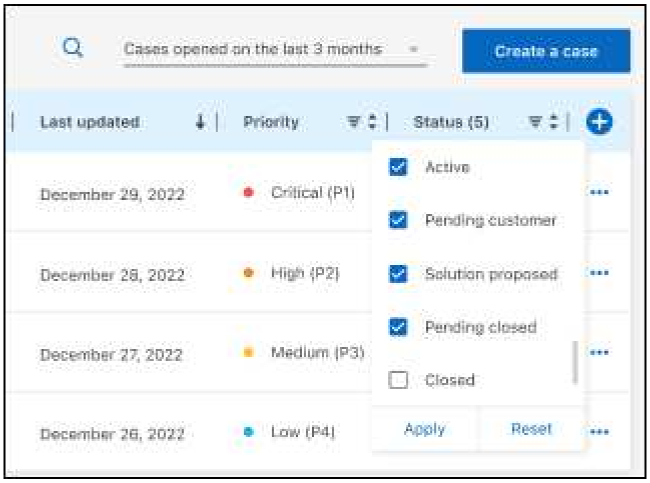
Create a case

- Last 7 days
- Last 30 days
- Last 3 months ✓

Apply | Reset

Date created	Last updated		tatus (5)
December 22, 2022	December 29, 2022		nassigned
December 21, 2022	December 28, 2022		ctive
December 15, 2022	December 27, 2022	● Medium (P3)	Pending customer
December 14, 2022	December 26, 2022	● Low (P4)	Solution proposed

- Filter the contents of the columns.



Cases opened on the last 3 months ▾

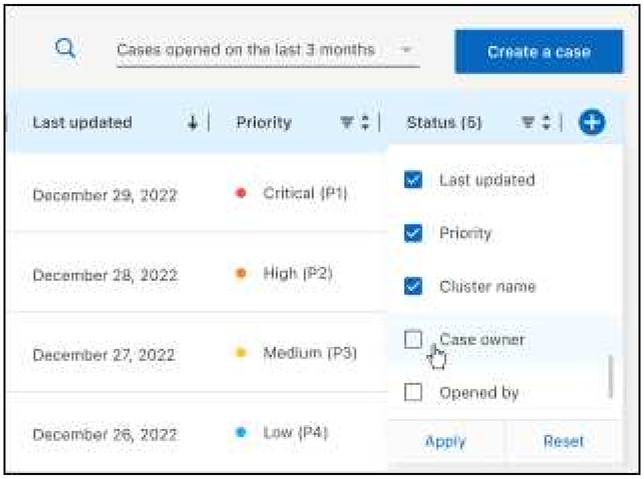
Create a case

Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

- ☑ Active
- ☑ Pending customer
- ☑ Solution proposed
- ☑ Pending closed
- ☐ Closed

Apply | Reset

- Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.



Cases opened on the last 3 months ▾

Create a case

Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

- ☑ Last updated
- ☑ Priority
- ☑ Cluster name
- ☐ Case owner
- ☐ Opened by

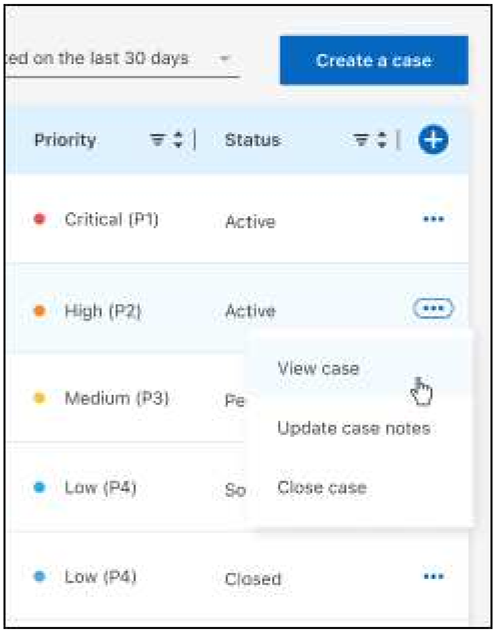
Apply | Reset

4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

   - **Close case**: Provide details about why you’re closing the case and select **Close case**.



Priority	Status
● Critical (P1)	Active
● High (P2)	Active
● Medium (P3)	Pe
● Low (P4)	So
● Low (P4)	Closed

Frequently asked questions about NetApp Ransomware Resilience

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

Deployment

Do you need a license to use Ransomware Resilience?

You can use the following license types:

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription to NetApp Intelligent Services and Ransomware Resilience with Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace, and Microsoft Azure Marketplace.
- Bring your own license (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in the Console's Licesnses and subscriptions section.

How do you enable Ransomware Resilience?
Ransomware Resilience does not require any enablement. You can access Ransomware Resilience from the NetApp Console.

To get going, you need to sign up or reach out to your NetApp Sales rep to try out this service. Then, when you use the Console agent, it will include the appropriate capabilities for Ransomware Resilience.

To get started with Ransomware Resilience, select "Start discovering workloads" from its initial landing page.

Is Ransomware Resilience available in standard, restricted, and private modes?
At this time, Ransomware Resilience is available only in standard mode. Stay tuned for more.

For an explanation about these modes across all NetApp data services, refer to NetApp Console deployment modes.

Access

What's the Ransomware Resilience URL?
In a browser, enter https://console.netapp.com/ransomware-resilience to access the Console.

How are access permissions handled?
Learn about Console access roles for all services.

What device resolution is best?
The recommended device resolution for Ransomware Resilience is 1920x1080 or better.

Which browser should I use?
Any modern browser.

Interaction with other services

Is Ransomware Resilience aware of protection settings made in NetApp ONTAP?
Yes, Ransomware Resilience discovers snapshot schedules set in ONTAP.

If you set a policy using Ransomware Resilience, do you have to make future changes only in this service?
We recommend that you make policy changes from Ransomware Resilience.

How does Ransomware Resilience interact with NetApp Backup and Recovery and SnapCenter?

Ransomware Resilience uses the following products and services:

- Backup and Recovery to discover and set snapshot and backup policies for file share workloads
- SnapCenter or SnapCenter for VMware to discover and set snapshot and backup policies for application and VM workloads.

In addition, Ransomware Resilience uses Backup and Recovery and SnapCenter / SnapCenter for VMware to perform file- and workload-consistent recovery.

Workloads

What makes up a workload?
A workload is an application, a VM, or a file share. 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 Ransomware Resilience prioritize workload data?
Data priority is determined by the snapshot copies made and backups that are scheduled.

The workload priority (critical, standard, important) is determined by snapshot frequencies already applied to each volume associated with the workload.

Learn about workload priority or importance.

What workloads does Ransomware Resilience support?

Ransomware Resilience can identify the following workloads: Oracle, MySQL, file shares, block storage, VMs, and VM datastores.

In addition, if you’re using SnapCenter or SnapCenter for VMware, all workloads supported by those products are also identified in Ransomware Resilience, and Ransomware Resilience can protect and recover these in a workload-consistent manner.

How do you associate data with a workload?

Ransomware Resilience associates data with a workload in the following ways:

- Ransomware Resilience discovers the volumes and the file extensions and associates them to the appropriate workload.
- In addition, if you have SnapCenter or SnapCenter for VMware and have configured workloads in Backup and Recovery, then Ransomware Resilience discovers the workloads managed by SnapCenter and

SnapCenter for VMware and their associated volumes.

What is a "protected" workload?
In Ransomware Resilience, a workload shows a "protected" status when it has a primary detection policy enabled. For now, this means ARP is enabled on all volumes related to the workload.

What is an "at risk" workload?
If a workload does not have a primary detection policy enabled, it is "at risk" even if it has a backup and snapshot policy enabled.

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.

Protection policies

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

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

What 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 Ransomware Resilience strategy.

Is Ransomware Resilience aware of protection settings made in NetApp ONTAP?

Yes, Ransomware Resilience discovers snapshot schedules set in ONTAP and whether ARP and FPolicy are enabled across all volumes in a discovered workload. The info you see initially in the Dashboard is aggregated from other NetApp solutions and products.

Is Ransomware Resilience aware of policies already made in Backup and Recovery and SnapCenter?

Yes, if you have workloads managed in Backup and Recovery or SnapCenter, the policies managed by those products are brought into Ransomware Resilience.

Can you modify policies carried over from NetApp Backup and Recovery and/or SnapCenter?

No, you cannot modify policies managed by Backup and Recovery or SnapCenter from Ransomware Resilience. You manage any changes to those policies in Backup and Recovery or SnapCenter.

If policies exist from ONTAP (already enabled in System Manager such as ARP, FPolicy, and snapshots) are those changed in Ransomware Resilience?

No. Ransomware Resilience does not modify any existing detection policies (ARP, FPolicy settings) from ONTAP.

What happens if you add new policies in Backup and Recovery or SnapCenter after signing up for

Ransomware Resilience?

Ransomware Resilience recognizes any new polices created in Backup and Recovery or SnapCenter.

Can you change policies from ONTAP?

Yes, you can change policies from ONTAP in Ransomware Resilience. You can also create new policies in Ransomware Resilience and apply them to workloads. This action replaces existing ONTAP policies with the policies created in Ransomware Resilience.

Can you disable policies?

You can disable ARP in detection policies using the System Manager UI, APIs, or CLI.

You can disable FPolicy and backup policies by applying a different policy that does not include them.

Copyright information

Trademark information