Release notes

NetApp Ransomware Resilience

NetApp
February 11, 2026

Table of Contents

Release notes

What's new in NetApp Ransomware Resilience

Learn what's new in NetApp Ransomware Resilience.

19 January 2026

Unsupported volumes

Ransomware Resilience reports now capturing information about supported and unsupported volumes in the **Summary** report. Use this information to diagnose why volumes in a system might be ineligible for ransomware protection.

For more information, see Download reports in Ransomware Resilience.

12 January 2026

Replicate snapshots to ONTAP

Ransomware Resilience now supports adding replication of snapshots to a secondary ONTAP site. With protection groups that use a replication policy, you can replicate to the same destination or different destinations for every workload. You can create a ransomware protection strategy that includes replication or use the predefined strategy.

For more information, see Protect workloads in Ransomware Resilience.

Exclude workloads from Ransomware Resilience

Ransomware Resilience now supports excluding specific workloads in a system from protection and the Ransomware Resilience dashboard. You can exclude workloads after discovery, and re-include them if you want to add ransomware protection. You aren't billed for excluded workloads.

For more information, see Exclude workloads.

Mark alerts as in review

Ransomware Resilience now allows you to mark alerts as "In review." Use the "In review" label to improve clarity across your team when triaging and managing active ransomware threats.

For more information, see Manage alerts in Ransomware Resilience.

08 December 2025

Extension blocking is enabled at the workload level

When you enable extension blocking, it's now enabled at the workload level rather than the storage VM level.

Edit user behavior alert status

Ransomware Resilience now enables you to edit the status of user behavior alerts. You can manually dismiss and resolve alerts.

For more information, see [Manage alerts in Ransomware Resilience](#).

Support for multiple Console agents

Ransomware Resilience now supports using multiple Console agents to manage the same systems.

For more information about Console agents, see [Create a Console agent](#).

10 November 2025

This release includes general enhancements and improvements.

06 October 2025

BlueXP ransomware protection is now NetApp Ransomware Resilience

BlueXP ransomware protection service has been renamed to NetApp Ransomware Resilience.

BlueXP is now NetApp Console

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](#).

Data breach detection

Ransomware Resilience includes a new detection mechanism that can be activated in a few steps to detect anomalous user reads as an early indicator of data breach. Ransomware resilience collects and analyzes user read events by creating a historic baseline, which is a profile of expected, normal behavior from the past data. When new user activity significantly deviates from this established norm (such as an unexpected read surge combined with suspicious read patterns), an alert is generated. Ransomware Resilience includes an AI model to detect suspicious read patterns.

Unlike encryption detection by ARP at the storage layer, detection of the user behavior anomaly is done in the Ransomware Resilience SaaS service by collecting FPolicy events.

> ⓘ   You must use the new [Ransomware Resilience user behavior admin and Ransomware Resilience user behavior viewer](#) roles to access suspicious user behavior detection settings.

For more information, see [Enable suspicious user activity detection](#) and [View anomalous user behavior](#).

Additional suspicious user activity detections

In addition to data breach detection, Ransomware Resilience also detects the following alert types based on observed suspicious user activity:

- **Data destruction - potential attack** - An alert with the severity of potential attack is created when the number of file deletions exceed the historic norm.
- **Suspicious user behavior - potential attack** - An alert with the severity of potential attack is created when read, rename, and delete operations in a sequence similar to a ransomware attack are observed

- **Suspicious user behavior - Warning** - An alert with the severity of warning is created when the total number of file activities (read, delete, rename etc.) exceeds the historic norm

New user roles for data breach detection

To manage suspicious user activity alerts, Ransomware Resilience has introduced two new roles for Console organization admins to grant access to supsicious user activity detection: Ransomware Resilience user behavior admin and Ransomware Resilience user behavior viewer.

You must be a user behavior admin to configure suspicious user behavior settings. The Ransomware Resilience admin role is not supported for configuring suspicious user behavior settings.

For more information, see NetApp Ransomware Resilience role-based access.

12 August 2025

This release includes general enhancements and improvements.

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, 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 Amazon FSx for ONTAP:

- Backup policies are not supported for Amazon 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.