Get started

NetApp Ransomware Resilience

NetApp
March 10, 2026

Table of Contents

Get started

Learn about NetApp Ransomware Resilience

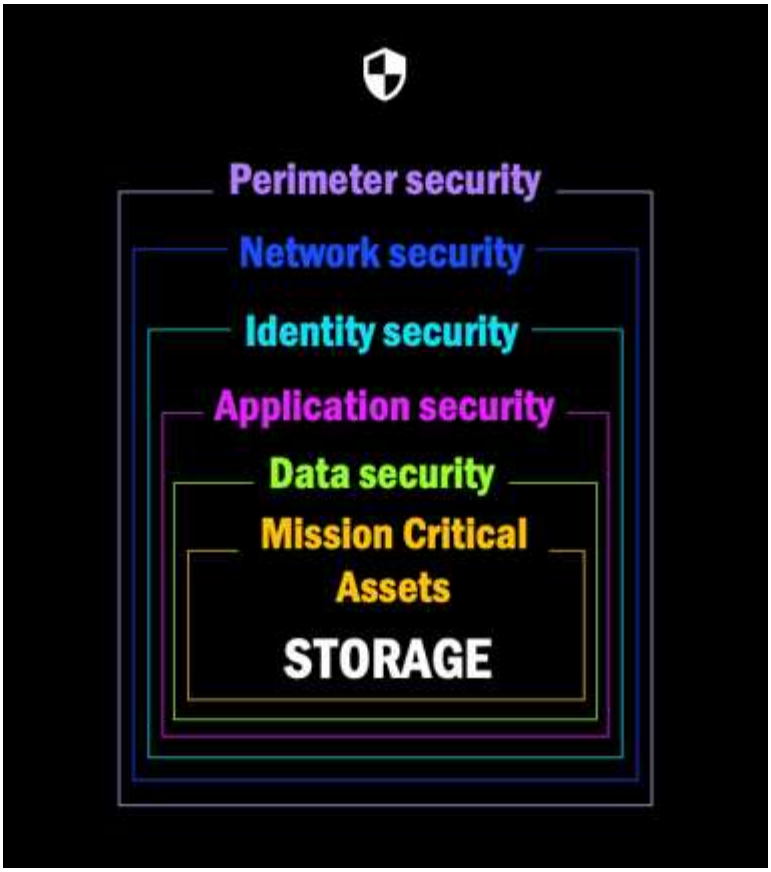
Ransomware attacks can block access to your data and attackers can ask for ransom in exchange for the release of data or decryption. According to the IDC, it is not uncommon for victims of ransomware to experience multiple ransomware attacks. The attack can disrupt access to your data for anywhere from 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, VM datastores, and file shares for NAS storage (NFS and CIFS protocols) and SAN storage (FC, iSCSI, and NVMe protocols). Ransomware Resilience is supported in on-premises storage as well as Cloud Volumes ONTAP for Amazon Web Services, Cloud Volumes ONTAP for Google Cloud, Cloud Volumes ONTAP for Microsoft Azure, Azure NetApp Files, and Amazon FSx for NetApp ONTAP across the NetApp Console. You can back up data to Amazon Web Services, Google Cloud, Microsoft Azure, 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** application-based, file share, or VMware-managed workloads in NetApp on-premises NAS and SAN systems across the NetApp Console, projects, and Console agents. After discovering workloads, Ransomware Resilience identifies opportunities to improve ransomware resiliency.
- **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 point-in-time snapshot that is locked so that the copy can't 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 while providing recommendations to improve protection.
- Applies AI/ML-driven data protection recommendations with one-click access.
- Protects data in application-based workloads such as 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 NetApp Backup and Recovery.
- Uses role-based access control (RBAC) to govern access to features and operations.

Cost

New deployments of Ransomware Resilience offer a 30-day free trial. NetApp doesn't charge you for using the trial version of Ransomware Resilience.

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

When a workload is classified as protected, it counts against purchased capacity or the PAYGO subscription. Ransomware Resilience classifies a workload as protected when a detection policy is enabled with at least one snapshot or backup policy. Workloads discovered with a detection policy but *without* backup or snapshot policies are classified as at risk. At risk workloads do not count against purchased capacity.

Protected workloads count against purchased capacity or the subscription after the free trial period ends. Ransomware Resilience is charged on a per GB basis for the data associated with protected workloads (as reported by ONTAP) 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.

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.

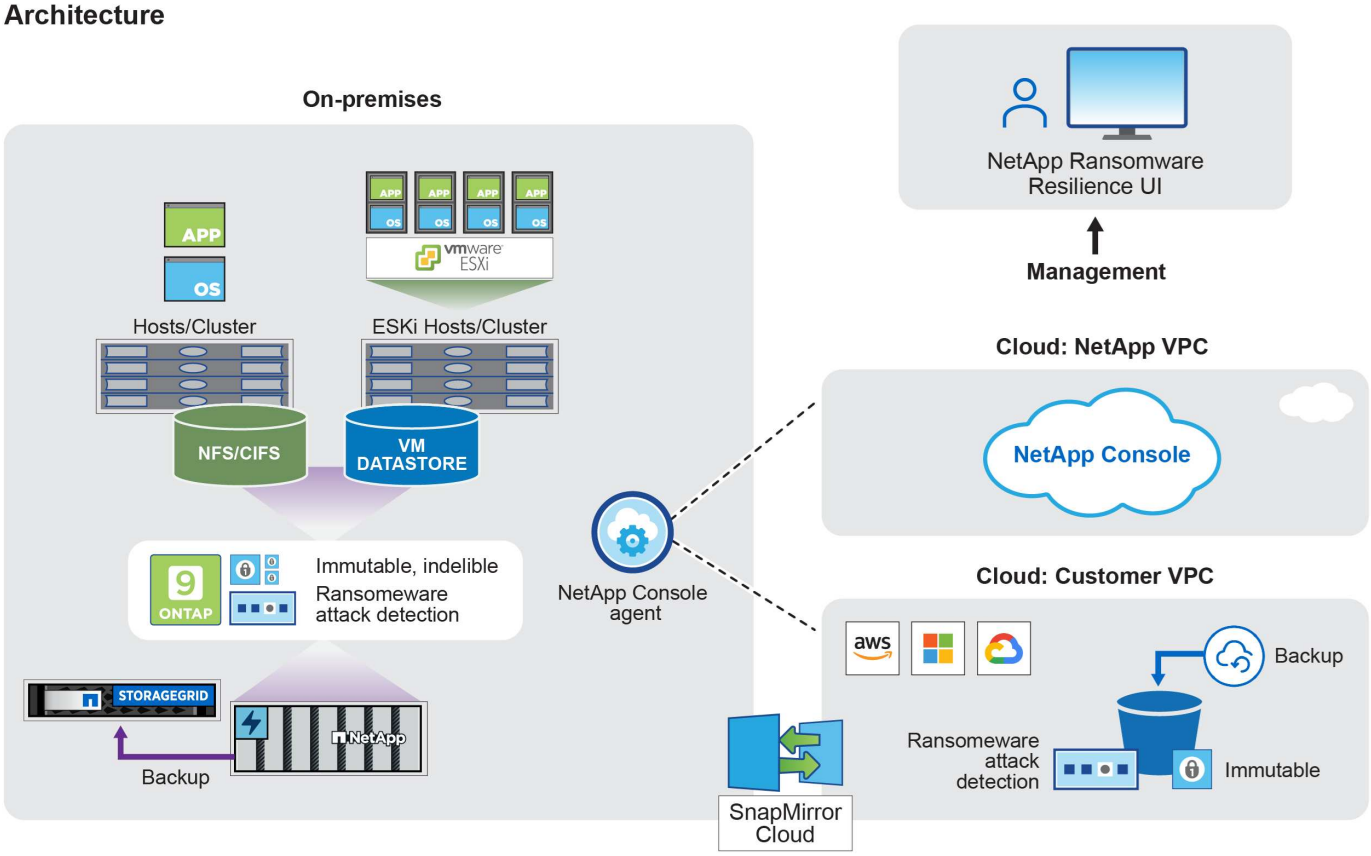
You don’t need a license or subscription to start using NetApp Console and you only incur charges when you deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

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.

Architecture



Feature	Description
IDENTIFY	• Finds all customer on-premises and cloud NAS (NFS and CIFS protocols) and SAN (FC, iSCSI, and NVMe) data in systems attached to the Console. • Identifies customer data from ONTAP and Backup and Recovery service APIs and associates it with workloads. Learn more about ONTAP. • 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 and Recovery, 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 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) 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.
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

Environment	Protocol	Supported versions
Amazon FSx for NetApp ONTAP*	CIFS, NFS, and SAN	N/A
Azure NetApp Files	CIFS & NFS	N/A
Cloud Volumes ONTAP for AWS	CIFS & NFS	9.11.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Google Cloud Platform	CIFS & NFS	9.11.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Microsoft Azure	CIFS & NFS	9.12.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
ONTAP (on-premises)	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later

* Amazon FSx for NetApp ONTAP uses Autonomous Ransomware Protection (ARP) and not ARP/AI. For more information about the difference, see ARP/AI.

Using ARP/AI in ONTAP requires ONTAP 9.16 or greater.
ONTAP doesn't provide ransomware protection support for FabricPool FlexCache, FlexGroup volumes, consistency groups mount point volumes, mount path volumes, offline volumes, and Data protection (DP) volumes. Ensure you review supported and unsupported configurations in ONTAP.

Supported workload data sources

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

- Block storage
- Databases:
  - Microsoft SQL Server
  - Oracle
  - PostgreSQL

- NetApp file shares
- VMware datastores

Key terms

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 Oracle databases, VMware datastores, or file shares.

NetApp Ransomware Resilience prerequisites

To ensure a successful deployment of NetApp Ransomware Resilience, verify the readiness of your operational environment, network access, and web browser.

Review and ensure you meet the following requirements.

Supported systems

Ensure you're using a supported system:

Environment	Protocol	Supported versions
Amazon FSx for NetApp ONTAP*	CIFS, NFS, and SAN	N/A
Azure NetApp Files	CIFS & NFS	N/A
Cloud Volumes ONTAP for AWS	CIFS & NFS	9.11.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Google Cloud Platform	CIFS & NFS	9.11.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Microsoft Azure	CIFS & NFS	9.12.1 and later
	SAN (iSCSI & NVMe)	9.17.1 and later
ONTAP (on-premises)	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later

* Amazon FSx for NetApp ONTAP uses Autonomous Ransomware Protection (ARP) and not ARP/AI. For more information about the difference, see ARP/AI.

NetApp Console requirements

Your NetApp Console configuration requires:

- A NetApp Console user account with Organization Admin privileges for discovering resources.
- A Console organization and system with at least one active Console agent connecting to a supported system.

- If your on-premises ONTAP clusters or Cloud Volumes ONTAP systems are not set up in the Console, see 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.

- The Console agent must have the `cloudmanager-ransomware-protection` container in an active state.
- For ONTAP or Cloud Volumes ONTAP clusters, Ransomware Resilience requires the ONTAP version be 9.11.1 or greater.

> To use Ransomware Resilience on SAN workloads, you must be running ONTAP 9.17.1 or later.

ONTAP requirements

- You must be running ONTAP 9.11.1 or later with an ONTAP One license enabled on the on-premises ONTAP instance. For more information about ONTAP support, see Autonomous Ransomware Protection overview.
- To apply protection configurations (such as enabling Autonomous Ransomware Protection), Ransomware Resilience needs admin permissions on the ONTAP cluster. The ONTAP cluster should have been onboarded using ONTAP cluster admin user credentials only.

> If you've connected an ONTAP cluster to the Console with non-admin credentials, [you must update the credentials in the ONTAP cluster](#update-non-admin-user-permissions-in-an-ontap-system).

Data backups

- An account in NetApp StorageGRID, AWS S3, Azure Blob, or Google Cloud Platform for backup targets with appropriate access permissions configured.

  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 Add a backup destination.

Suspicious user behavior requirements

For Ransomware Resilience to provide alerts about suspicious user behavior, you must configure a user activity agent. To install a user activity agent, ensure your system meets the requirements.

Update non-admin user permissions in an ONTAP system

If you need to update non-admin user permissions for a particular system, use this procedure steps.

1. Log in to the Console. In the dashboard, identify the system that needs its ONTAP user permissions

updated.

2. Select the system to view its details.
3. Select **View additional information** to display the username.
4. Log in to the ONTAP cluster CLI as an admin user.
5. Display the existing roles for that user:

```
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 NetApp Console to use Ransomware Resilience.

Quick start for NetApp Ransomware Resilience

Understand the high-level steps you need to follow to set up Ransomware Resilience and protect your workloads.

Follow the links in each step for detailed information.

1 Review prerequisites

These tasks require the *Console admin* role.

- Ensure you've installed a Console agent
- Ensure your system meets the requirements
- Review Ransomware Resilience user roles and assign permissions to users accessing Ransomware Resilience
- Set up licensing

2 Get started with Ransomware Resilience

These tasks require the *Ransomware Resilience admin* role.

- Discover workloads in the Console
- View workload protection health on the Dashboard
- Optionally, conduct a ransomware attack readiness drill

3 Configure protection and detection in Ransomware Resilience

These tasks require the *Ransomware Resilience admin* role. Configuring suspicious user behavior activity requires the additional *Ransomware Resilience user behavior admin* role.

- Protect workloads
  - Optionally, enhance protection by configuring suspicious user activity detection
- Optionally, configure backup destinations:
  - Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform, or Microsoft Azure as a backup destination.
  - Configure backup destinations
- Respond to detection of potential ransomware attacks
- Recover from an attack (after incidents are neutralized)

What's next?

After you configure protection in Ransomware Resilience, here's what you might do next.

- Enable Data Classification to identify governance and security risks
- Send alerts to SIEM
- Download alert, protection, readiness drill, recovery, or summary reports

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.

Set up licensing for NetApp Ransomware Resilience

NetApp Ransomware Resilience offers different license plans, enabling you to subscribe to the service where it makes sense for your organization.

To set up licensing, you need the Organization admin, Folder or project admin role. Learn about Console access roles.

License types

Ransomware Resilience is available with the following license types:

- 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): 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:

- View workloads and workload health
- Delete resources such as policies
- Run all scheduled operations created during the trial period or under the license

Other licenses

The Ransomware Resilience license does not include additional NetApp products. However, Ransomware Resilience can integrate with NetApp Backup and Recovery, even if you do not have a separate license for Backup and Recovery.

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

Cost

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

When a workload is classified as protected, it counts against purchased capacity or the PAYGO subscription. Ransomware Resilience classifies a workload as protected when a detection policy is enabled with at least one snapshot or backup policy. Workloads discovered with a detection policy but *without* backup or snapshot policies are classified as at risk. At risk workloads do not count against purchased capacity.

Protected workloads count against purchased capacity or the subscription after the free trial period ends. Ransomware Resilience is charged on a per GB basis for the data associated with protected workloads (as reported by ONTAP) before efficiencies.

Monitor the size of protected data in the Ransomware Resilience protection dashboard. To add capacity, see Update a license.

Try Ransomware Resilience with a 30-day free trial

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

Storage capacity limits are not enforced during the trial.

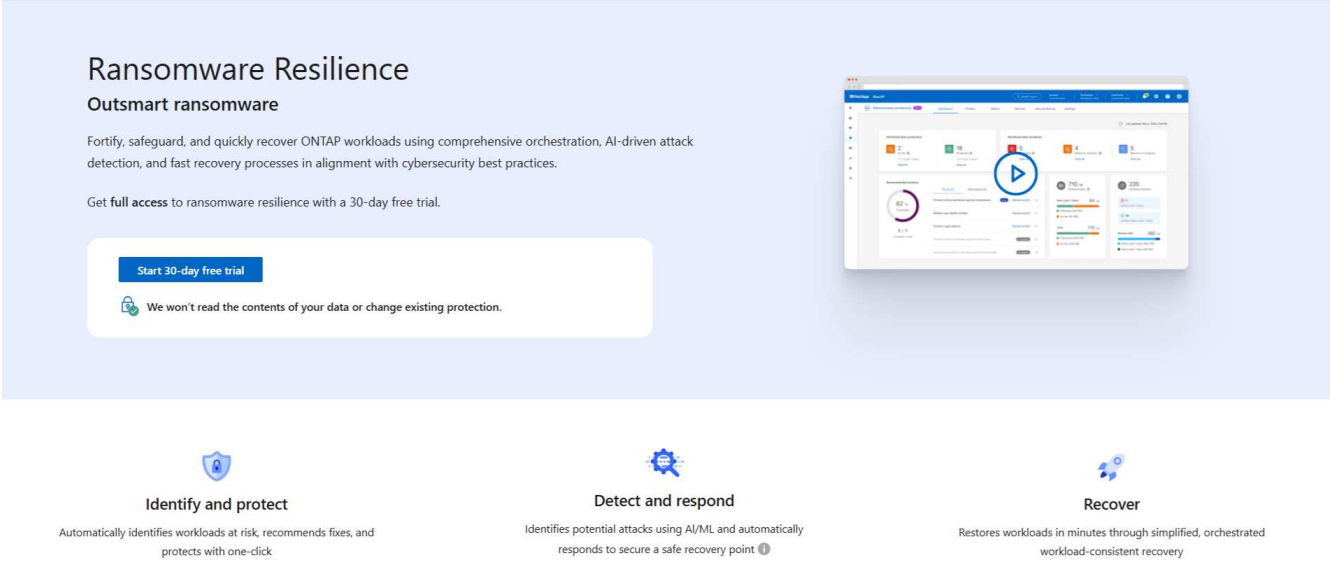
You can get a license or subscribe at any time and you will not be charged until the 30-day trial ends. To continue after the 30-day trial, you'll need to purchase a BYOL license or PAYGO subscription.

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.



4. If you haven't already added a Console agent for other services, add one.
5. In the Ransomware Resilience landing page, select **Start by discovering workloads** to discover your workloads.

   This option is only available if you've successfully installed a Console agent.

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.

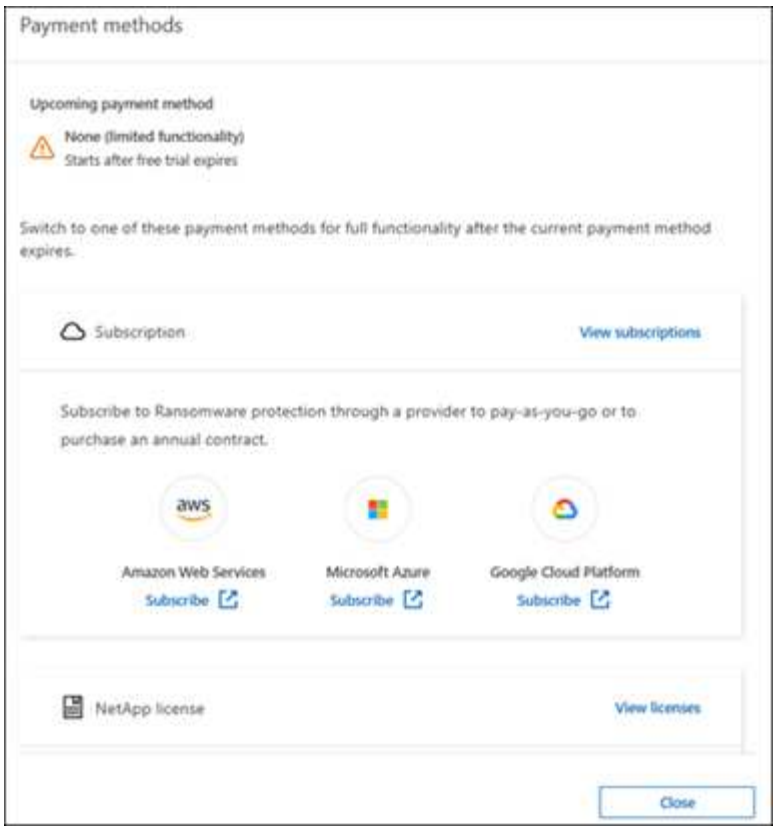
Subscribe through AWS Marketplace
Subscribe through Microsoft Azure Marketplace
Subscribe through Google Cloud Platform Marketplace
Bring your own license (BYOL)

Subscribe through AWS Marketplace

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

Steps

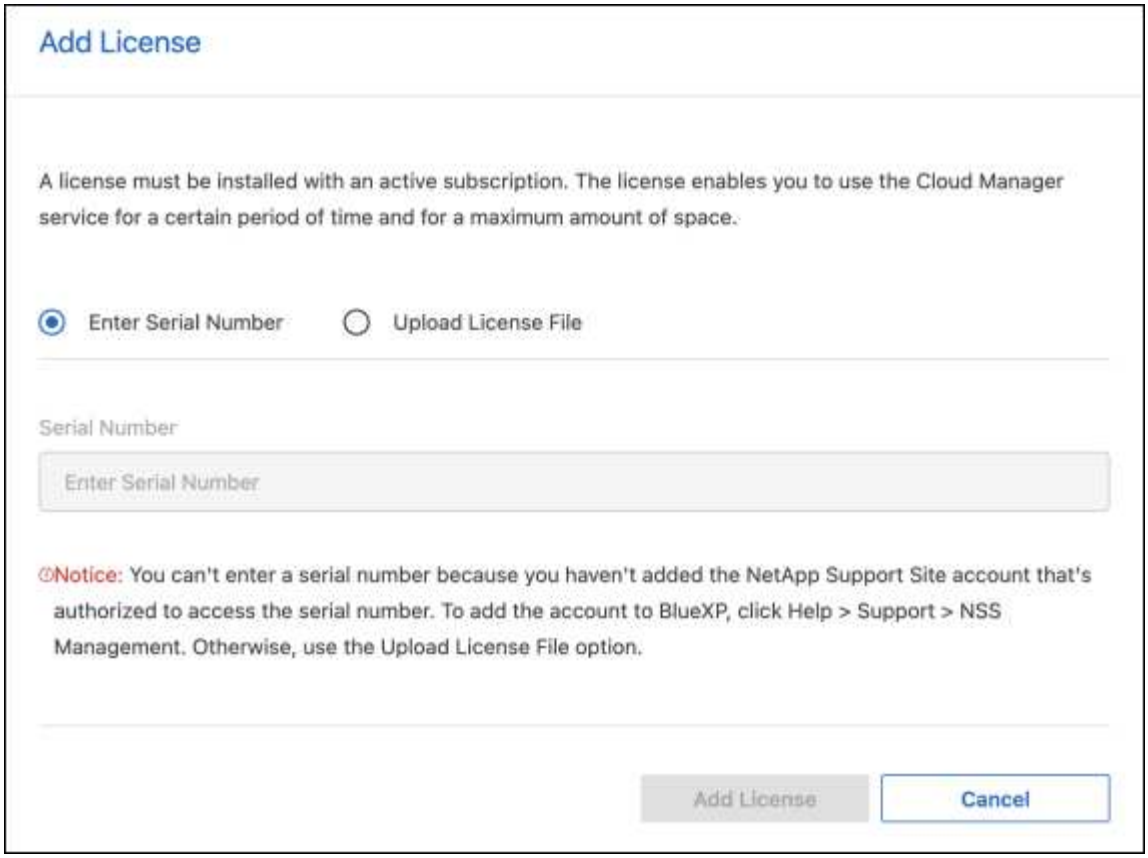
1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven't started the trial, select the **Free trial** notice at the top right then **View payment methods**.



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**.



8. In the Add License page, select **Enter Serial Number**, enter the serial number that was included in the email sent to you, then 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**.
10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

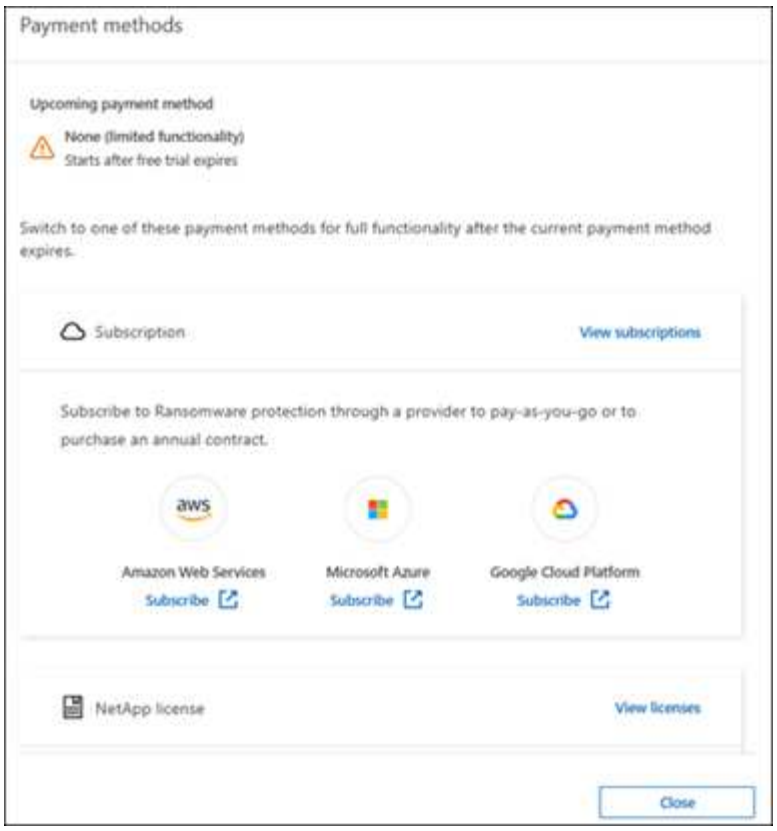
    A message confirms a license has been added.

Subscribe through Microsoft Azure Marketplace

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

Steps

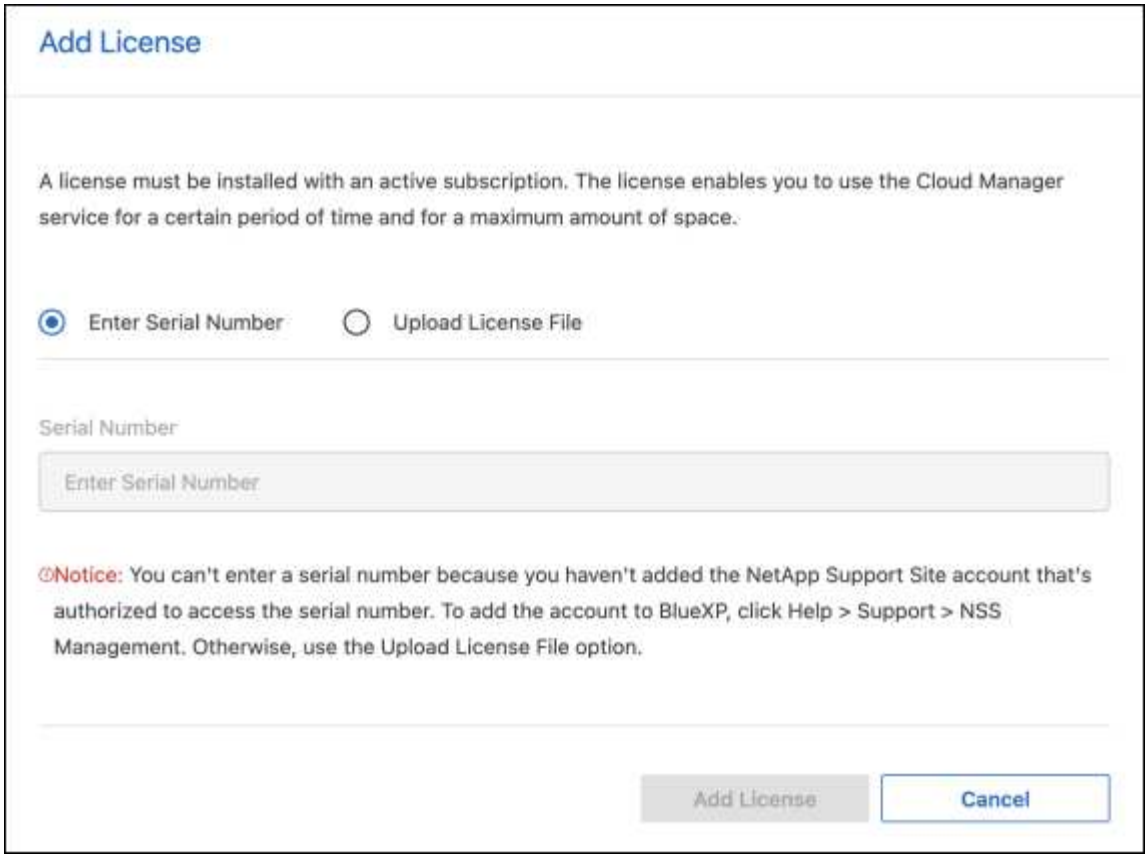
1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven’t started the trial, select the **Free trial** notice at the top right then **View payment methods**.



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**.



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

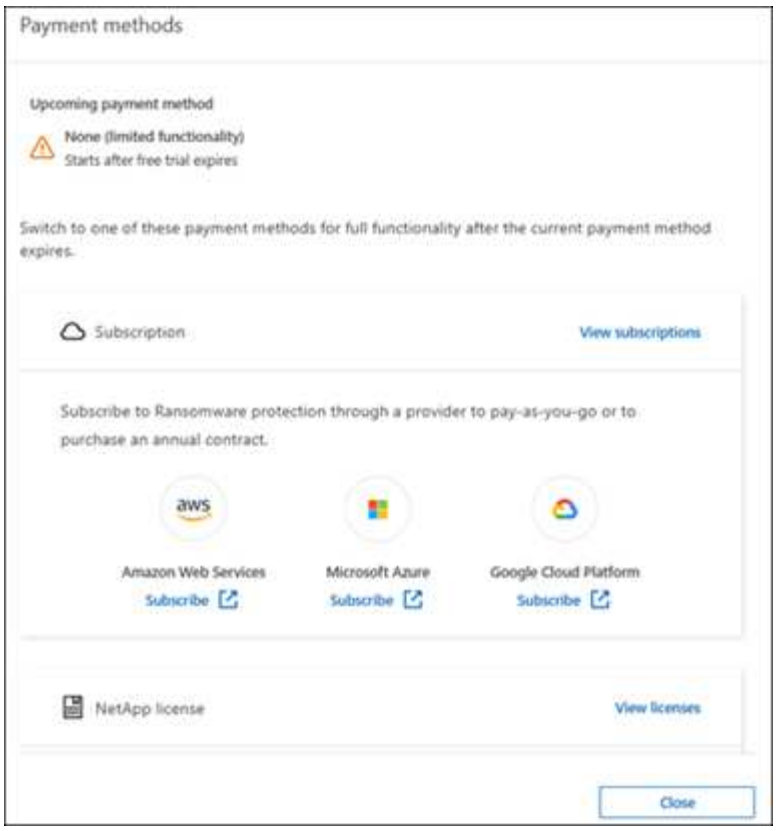
    A message appears indicating that a license has been added.

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

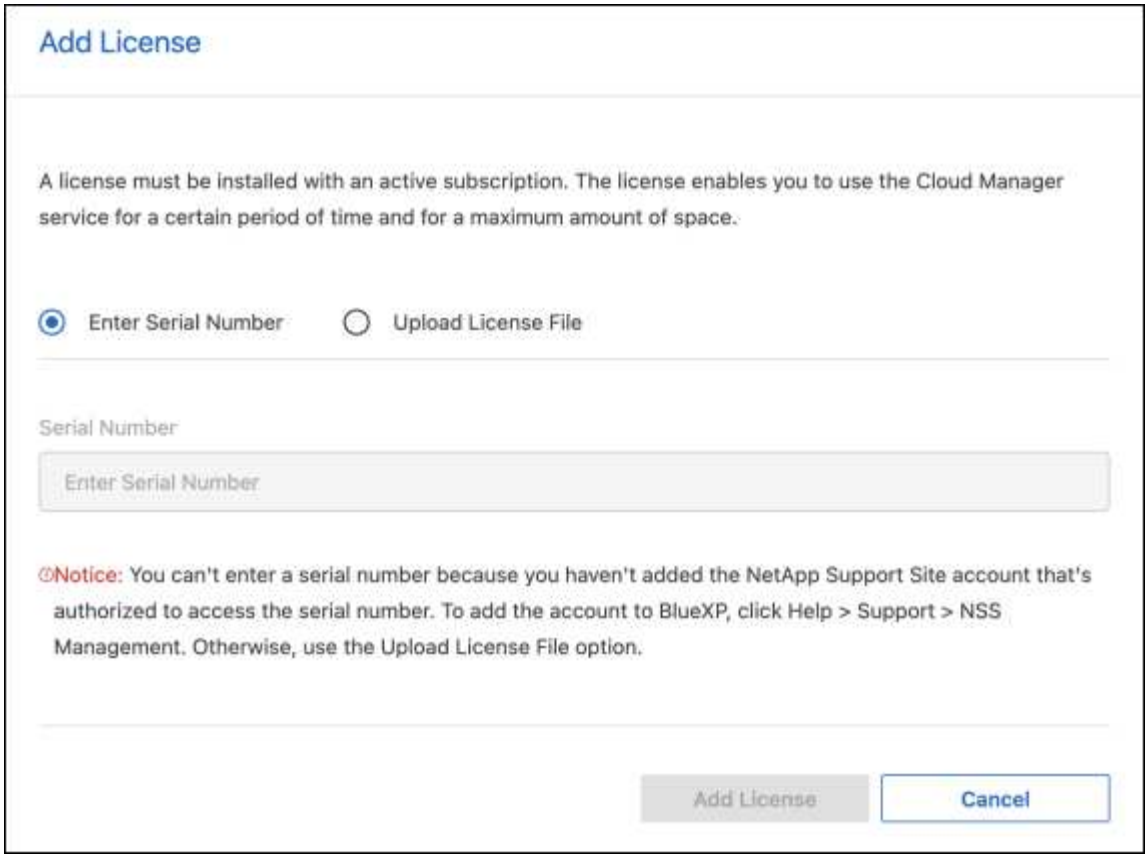
1. In the Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven’t started the trial, select the **Free trial** notice at the top right then **View payment methods**.



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**.
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**.



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**.
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

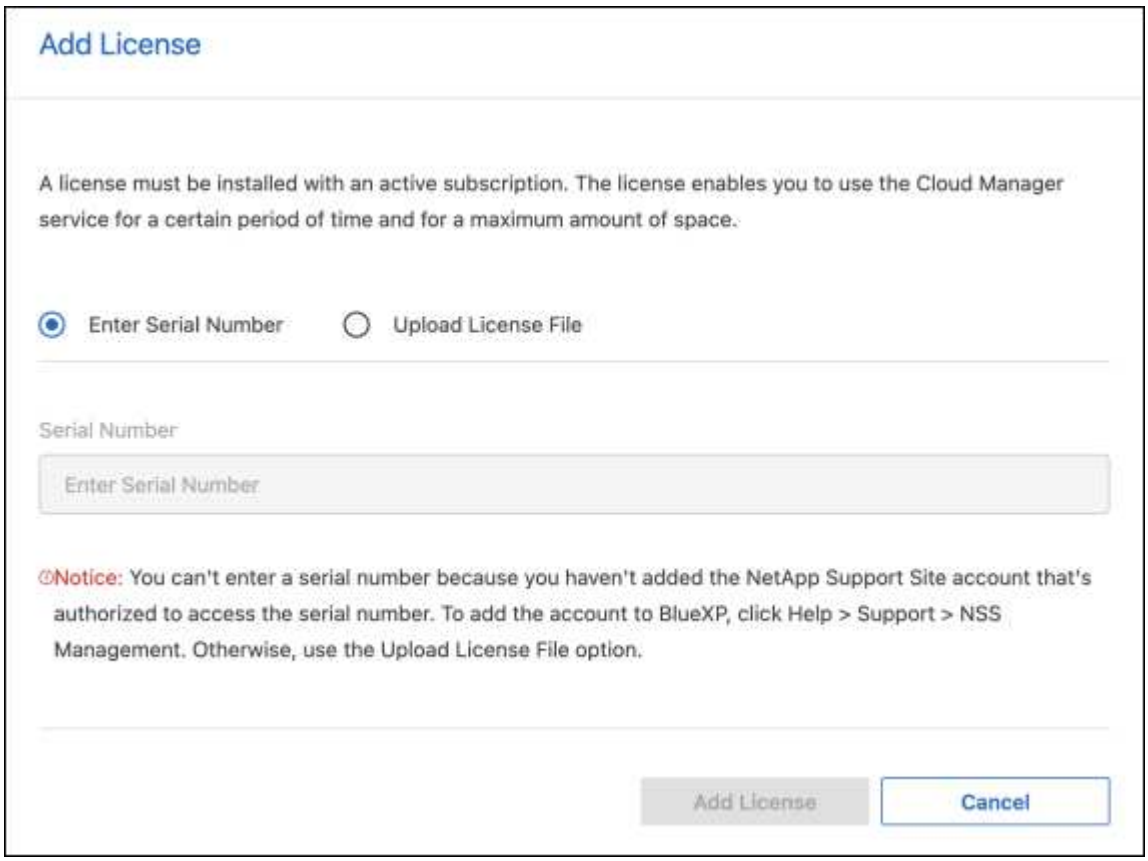
After you've purchased your Ransomware Resilience license from your NetApp sales rep, you activate the license by entering the Ransomware Resilience serial number and NetApp Support Site (NSS) account information.

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**.



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 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**.

More information

- NetApp Console licenses and subscriptions documentation

Discover and manage workloads in NetApp Ransomware Resilience

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

In the Discovery dashboard, Ransomware Resilience displays supported and unsupported system configurations. Ransomware Resilience assesses Oracle applications, VMware datastores, file shares, and block storage.

Ransomware Resilience does not discover workloads with volumes using FlexGroup.

Ransomware Resilience checks your current backup protection, snapshot copies, and NetApp Autonomous Ransomware Protection options. Ransomware Resilience also detects protection information from NetApp Backup and Recovery for file shares and VM file shares. It then recommends ways to improve your ransomware protection.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience

admin role. Learn about Ransomware Resilience roles for NetApp Console.

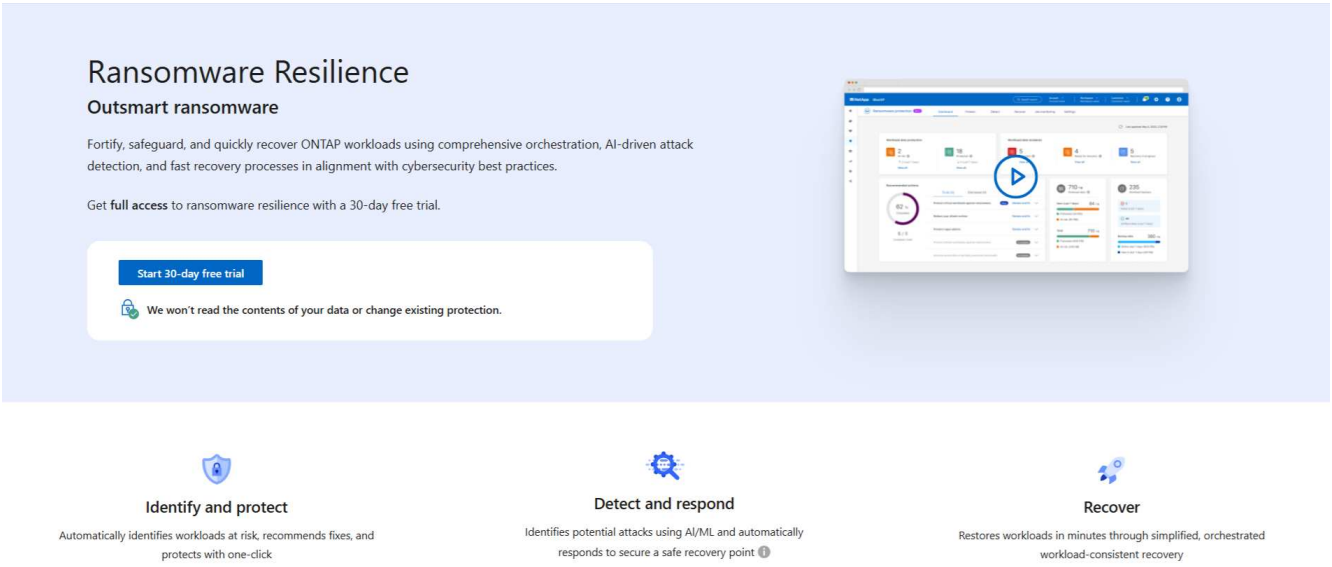
Select workloads to discover and protect

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

Steps

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

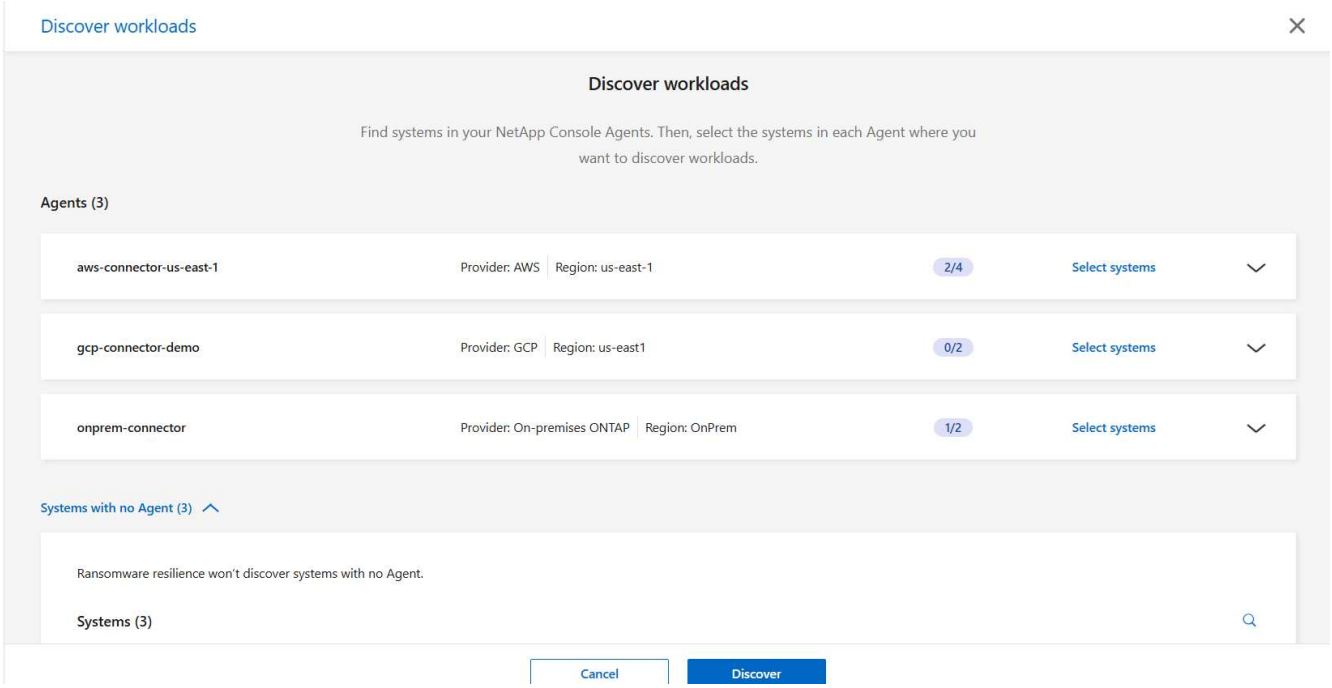
   If this is your first login, the landing page appears.



   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.

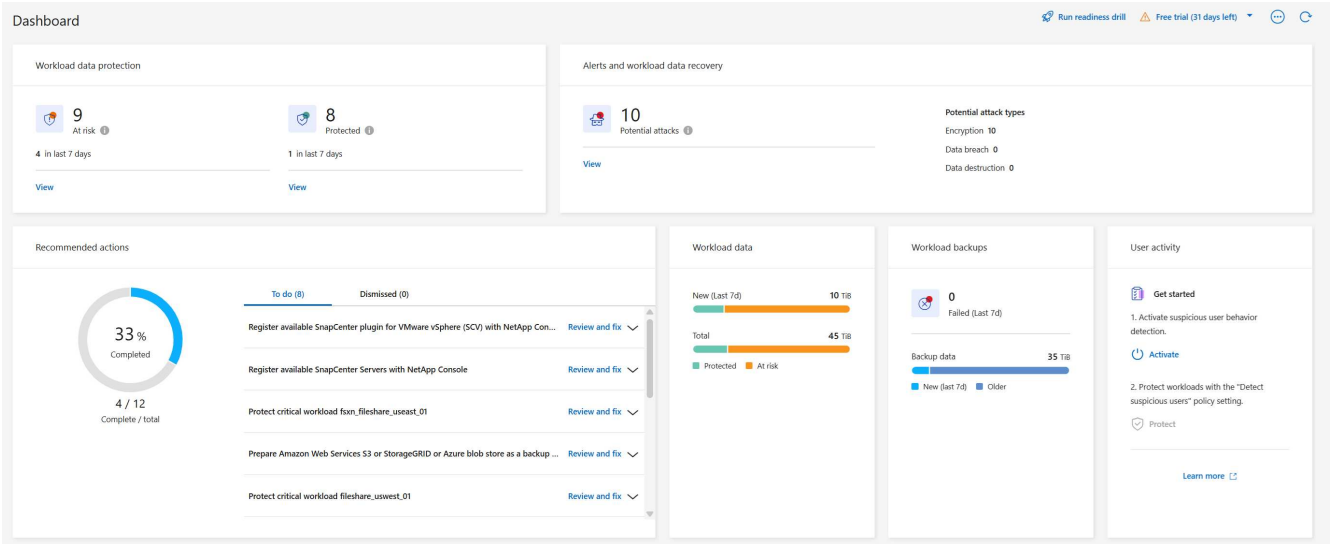


3. To discover workloads for a specific Console agent, select **Select systems** next to the Console agent where you want to discover workloads.
4. Select the systems where you want to discover workloads.
5. Select **Discover**.

   Ransomware Resilience only discovers workload data when you select system. The discovery process can take several 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.



Learn what the dashboard shows you.

Discover newly created workloads for previously selected systems

If you've added workloads to a previously discovered system, you need to reinitiate discovery to protect the new workloads.

Steps

1. To identify the time 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.

If you find there are volumes not displaying for the system you've discovered, the volumes might be unsupported. To find a list of unsupported volumes, go to the **Settings** menu then select the action menu in the Workload discovery card to download a JSON report of supported and unsupported volumes.

Discover new systems

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

Steps

1. From Ransomware Resilience, select **Settings**.
2. In the Workload discovery card, select **Discover workloads**. Discovery can take a few minutes. A loading icon displays the progress.
3. Ransomware Resilience discovers both supported and unsupported systems. It 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**.

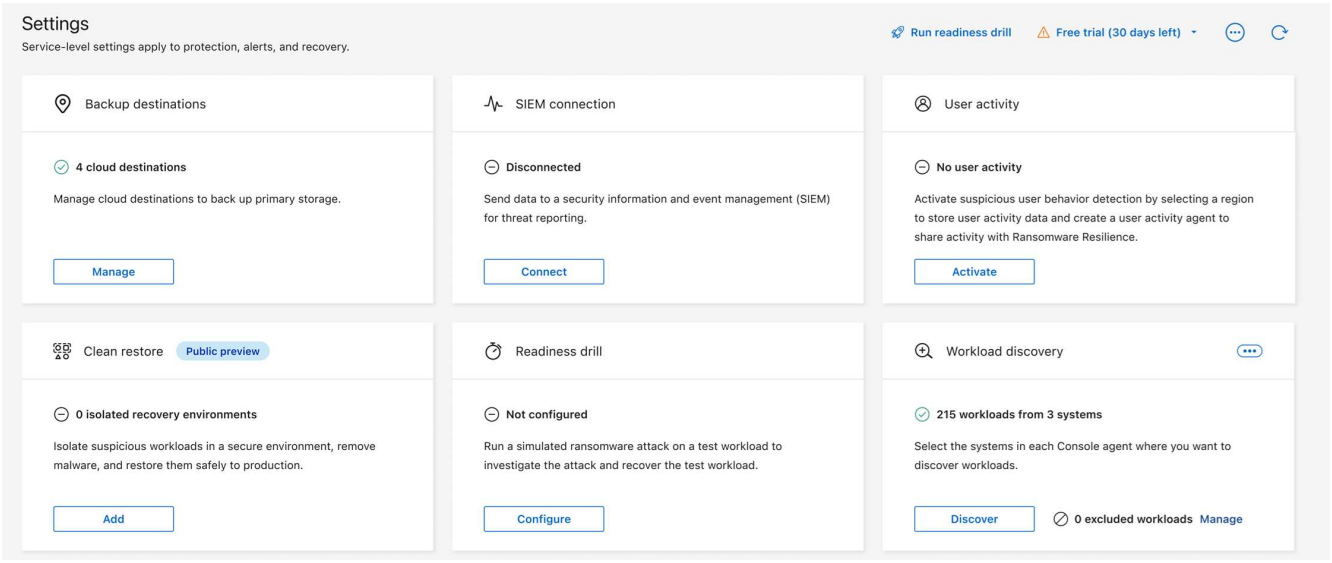
Exclude workloads

Ransomware Resilience allows your to exclude specific workloads in a system from ransomware protection and detection.

You can only exclude workloads that are supported and have been discovered successfully. You can modify the list of excluded workloads at any time. You aren't billed for workloads excluded from Ransomware Resilience.

Add workloads to the excluded workloads list

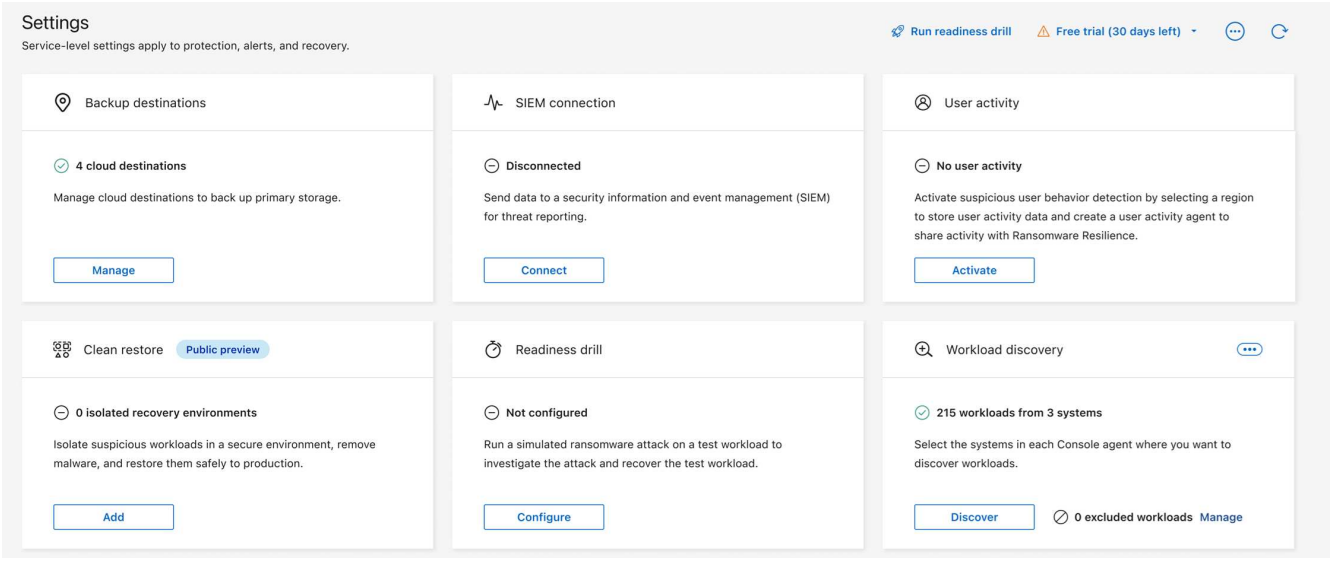
1. In Ransomware Resilience, select **Settings**.
2. In the Settings dashboard, locate the Workload discovery dashboard. The card identifies the number of excluded workloads. To add workloads, next to the excluded workloads, select **Manage**.



3. In the Excluded workloads page, select **Add**.
4. Select the workloads you want to exclude then **Add**.
5. Review the excluded workloads in the Excluded workloads page. While the workload is being added, a progress indicator displays next to its name. If a workload was not excluded successfully, it doesn't display on the page.

Remove workloads from the excluded workload list

1. In Ransomware Resilience, select **Settings**.
2. In the Settings dashboard, locate the Workload discovery dashboard. The card identifies the number of excluded workloads. Next to the excluded workloads, select **Manage**.

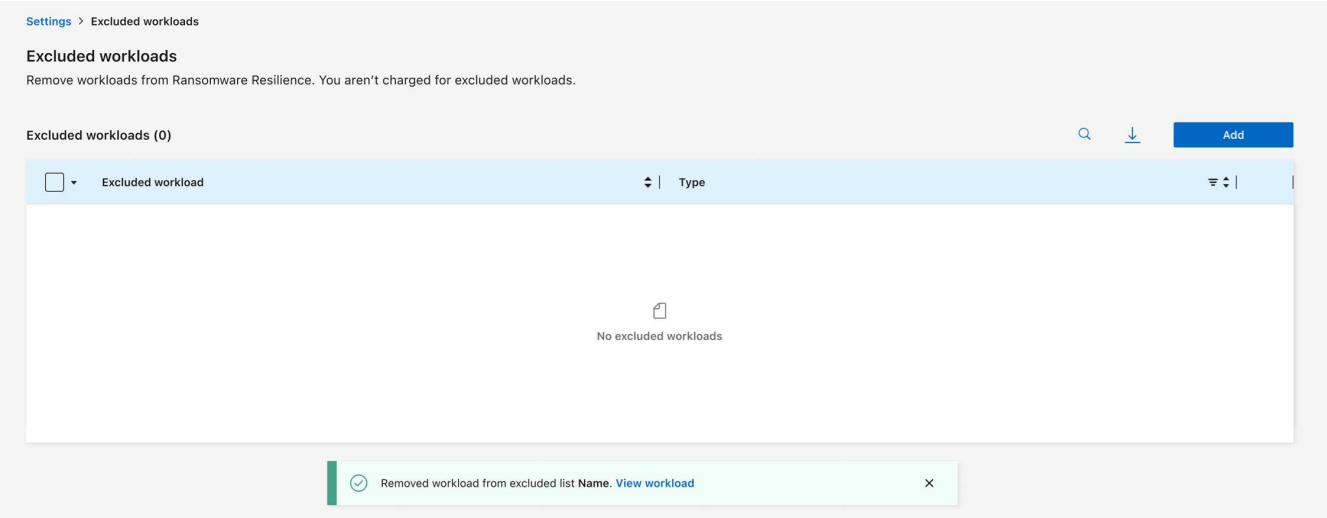


3. To remove an individual workload, select the action menu for the workload you want to remove from the excluded list.

   To remove multiple workloads, select the checkbox next to the workloads you want to remove then **Remove from excluded**.

4. In the dialog, select **Remove** to confirm that you want to remove the workloads from the exclude list.

5. If the workload is removed from the exluded workload list successfully, a success message appears on the Excluded workload page and the workload no longer appears in the list of excluded workloads. If the action fails, an error message appears; attempt the operation again.



Copyright information

Trademark information

[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.