H NetApp

Ransomware Protection documentation

Ransomware Protection

NetApp
May 12, 2022

Table of Contents

Ransomware Protection documentation

What's new with Ransomware Protection

Learn what's new in Ransomware Protection.

11 May 2022

New panel to track the security hardening of your ONTAP environments.

A new panel "Harden your ONTAP environments" provides the status of certain settings in your ONTAP systems that track how secure your deployment is according to the NetApp Security Hardening Guide for ONTAP Systems and to the ONTAP anti-ransomware feature that proactively detects and warns about abnormal activity.

You can review the recommendations and then decide how you want to address the potential issues. You can follow the steps to change the settings on your clusters, defer the changes to another time, or ignore the suggestion. Go here for details.

New panel to show how different categories of data are being protected using Cloud Backup.

This new "Backup Status" panel shows how comprehensively your most important categories of data are backed up in case you need to recover because of a ransomware attack. This data is a visual representation of how many items of a specific category in an environment are backed up by Cloud Backup. Go here for details.

15 March 2022

New panel to track the permissions status of your business critical data

A new panel "Business critical data permissions analysis" shows the permissions status of data that is critical for your business. That way you can quickly assess how well you are protecting your business-critical data. Go here for details.

Open Permissions area now includes OneDrive and SharePoint accounts

The Open Permissions area in the Ransomware Protection Dashboard now includes the permissions that exist for files that are being scanned in OneDrive accounts and SharePoint accounts.

9 February 2022

New Ransomware Protection service

The new Ransomware Protection service enables you to view relevant information about cybersecurity and assess how resilient your data is to a cyber attack. It also provides you with a list of alerts and remediations for making your data more secure.

Learn more about this new service.

Get started

Learn about Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The Ransomware Protection service enables you to view relevant information about cybersecurity and assess how resilient your organization is to a cyber attack. It also provides you with a list of alerts and remediations for making your data more secure.

Learn about the use cases for Ransomware Protection.

💡 | The Ransomware Protection service is currently a Beta offering.

Features

Ransomware Protection currently provides several features that can help you with your cyberstorage protection efforts. Additional features will be added in the future. Current features identify when:

- Volumes in your working environments aren't being protected by making periodic Snapshot copies.
- Volumes in your working environments aren't being protected by creating backups to the cloud using Cloud Backup.
- Data in your working environments and data sources aren't being scanned using Cloud Data Sense to identify compliance and privacy concerns, and find optimization opportunities.

  This capability is also important from a ransomware protection perspective because it allows you to better understand where your important (sensitive, business critical) data is located so you can make sure you're focusing your protections there.

- Your most important categories of data aren't being backed up in case you need to recover because of a ransomware attack.
- An abnormal increase in the percentage of encrypted files in a working environment or data source has occurred.

  This can be an indicator that a ransomware attack has commenced on your network.

- Sensitive data is found in files and the access permissions level is too high in a working environment or data source.
- Users have been added to your Active Directory Domain Administrator Groups.
- The ONTAP software version on your clusters is old and should be updated to provide the best protection and security features.
- On-box anti-ransomware features are not enabled on your ONTAP systems.

  The ONTAP anti-ransomware features proactively detect and warn about abnormal activity that might indicate a ransomware attack.

See how to view these potential issues in the Ransomware Protection dashboard.

When using Cloud Volumes ONTAP systems, there are some additional ransomware protections you can deploy directly from the working environment. See how to add additional protection against ransomware.

Supported working environments and data sources

Cloud Data Sense is a prerequisite to using the Ransomware Protection service. After Data Sense is installed and activated, you can use Ransomware Protection to see how resilient your data is to a cyber attack on the following types of working environments and data sources:

Working environments:

- Cloud Volumes ONTAP (deployed in AWS, Azure, or GCP)
- On-premises ONTAP clusters
- Azure NetApp Files
- Amazon FSx for ONTAP
- Amazon S3

Data sources:

- Non-NetApp file shares
- Object storage (that uses S3 protocol)
- Databases (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL Server)
- OneDrive accounts
- SharePoint accounts
- Google Drive accounts

Ransomware Protection also monitors your global Active Directory configuration if you have configured this in Cloud Data Sense.

How Ransomware Protection works

At a high-level, Ransomware Protection works like this:

1. Ransomware Protection gathers information from your storage systems, Cloud Data Sense, Cloud Backup, and from other Cloud Manager resources, to populate the Ransomware Protection Dashboard.
2. You use the Ransomware Protection dashboard to get an overview of how well protected your systems are.
3. You use the provided reporting tools to help in your cyberstorage protection efforts.

Cost

There is no separate cost for the Ransomware Protection service during the Beta.

Use Ransomware Protection

Managing cyber security recommendations for your data sources

Use the Ransomware Protection dashboard to view an overview of the cyber resilience of all your working environments and data sources. You can drill down in each area to find more details and possible remediations.
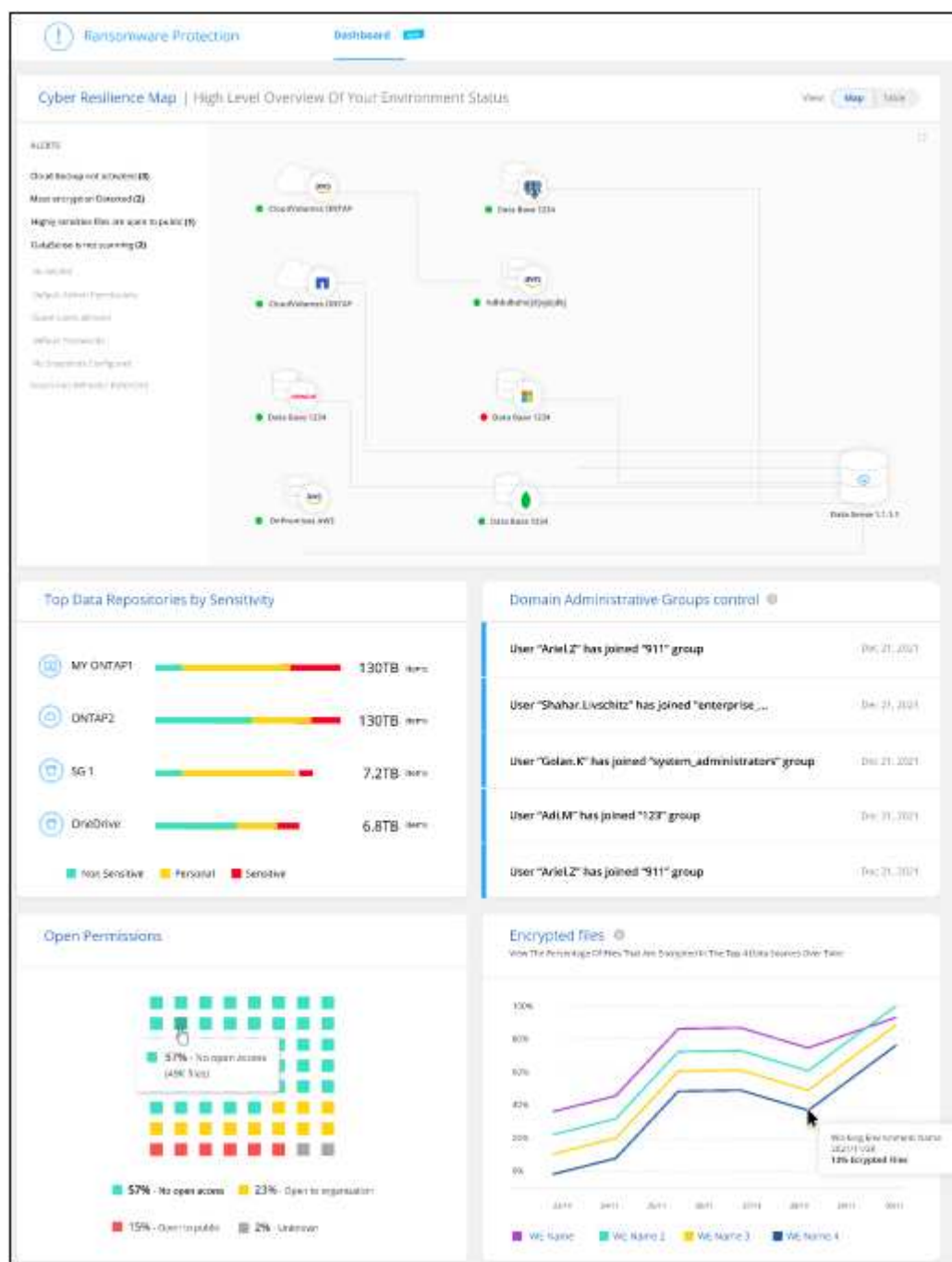
Cyber Resilience Map

The Cyber Resilience Map is the main area in the dashboard. It enables you to see all your working environments and data sources in a visual manner and be able to view relevant cyber-resilience information.
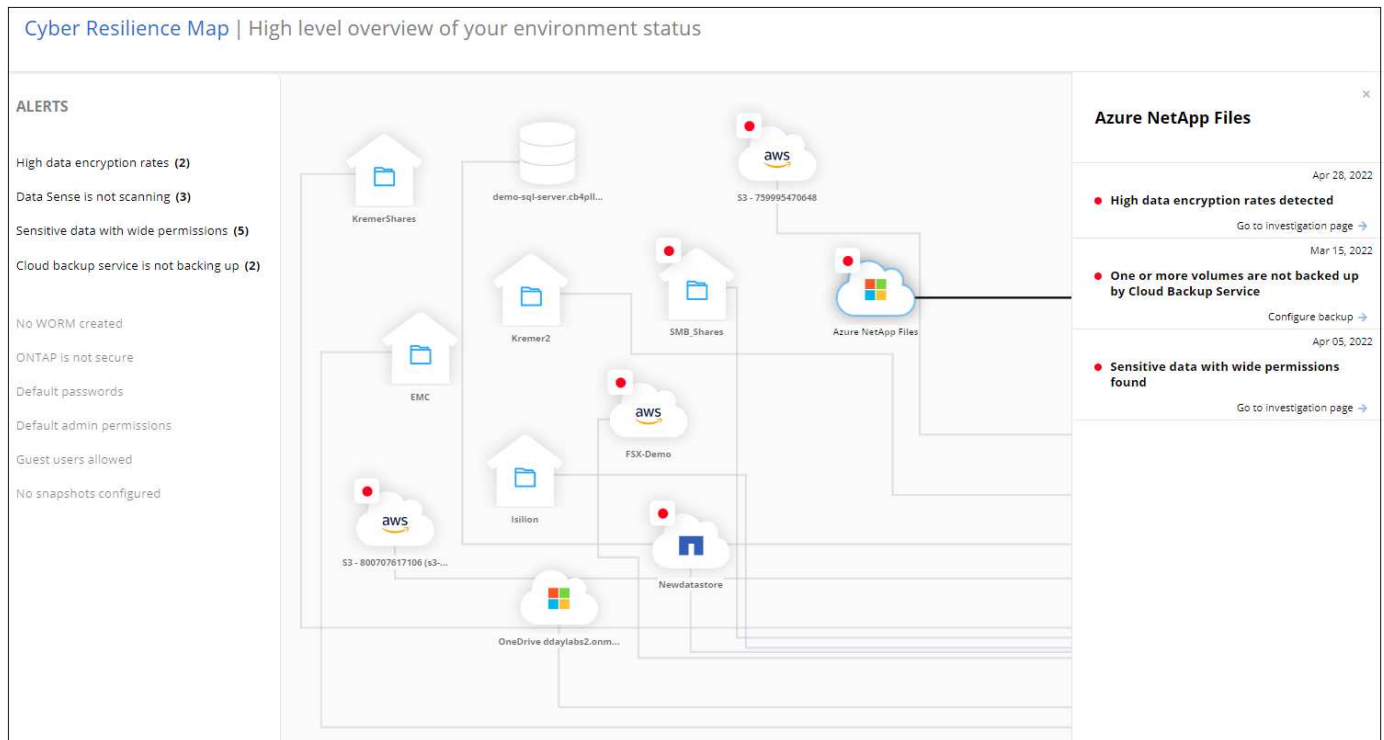
The map consists of three parts:

Left panel

Shows a list of alerts for which the service is monitoring across all of your data sources. It also indicates the number of each particular alert that is active in your environment. Having a large number of one type of alert may be a good reason to try to resolve those alerts first.

Center panel

Shows all of your data sources, services, and Active Directory in a graphical format. Healthy environments have a green indicator and environments that have alerts have a red indicator.

Right panel

After you click on a data source that has a red indicator, this panel shows the alerts for that data source and provides recommendations to resolve the alert. Alerts are sorted so that the most recent alerts are listed first. Many recommendations lead you to another Cloud Manager service where you can resolve the issue.

These are the currently tracked alerts and suggested remediations.

Alert	Description	Remediation
High data encryption rates detected	An abnormal increase in the percentage of encrypted files, or corrupted files, in the data source has occurred. This means that there was a greater than 20% increase in the percentage of encrypted files in the past 7 days. For example, if 50% of your files are encrypted, then a day later this number increases to 60%, you would see this alert.	Click the link to launch the Data Sense Investigation page. There you can select the filters for the specific *Working Environment* and *Category (Encrypted and Corrupted)* to view the list of all encrypted and corrupted files.
Sensitive data with wide permissions found	Sensitive data is found in files and the access permissions level is too high in a data source.	Click the link to launch the Data Sense Investigation page. There you can select the filters for the specific *Working Environment*, *Sensitivity Level (Sensitive Personal)*, and *Open Permissions* to view the list of the files that have this issue.
One or more volumes are not backed up using Cloud Backup	Some volumes in the working environment aren't being protected using Cloud Backup.	Click the link to launch Cloud Backup and then you can identify the volumes that aren't being backed up in the working environment, and then decide if you want to enable backups on those volumes.
One or more repositories (volumes, buckets, etc.) in your data sources are not being scanned by Data Sense	Some data in your data sources isn't being scanned using Cloud Data Sense to identify compliance and privacy concerns and find optimization opportunities.	Click the link to launch Data Sense and enable scanning and mapping for the items that are not being scanned.
On-box anti-ransomware is not active for all volumes	Some volumes in the on-prem ONTAP system don't have the NetApp anti-ransomware feature enabled.	Click the link and you are redirected to the Harden your ONTAP environment panel and to the working environment with the issue. There you can investigate how best to fix the issue.
ONTAP version is not updated	The version of ONTAP software installed on your clusters are not in accordance with the recommendations from the NetApp Security Hardening Guide for ONTAP Systems.	Click the link and you are redirected to the Harden your ONTAP environment panel and to the working environment with the issue. There you can investigate how best to fix the issue.
Snapshots not configured for all volumes	Some volumes in the working environment aren't being protected by creating volume snapshots.	Click the link and you are redirected to the Harden your ONTAP environment panel and to the working environment with the issue. There you can investigate how best to fix the issue.

Top data repositories by data sensitivity

The *Top Data Repositories by Sensitivity Level* panel lists up to the top four data repositories (working environments and data sources) that contain the most sensitive items. The bar chart for each working environment is divided into:

- Non-Sensitive data
- Personal data
- Sensitive Personal data
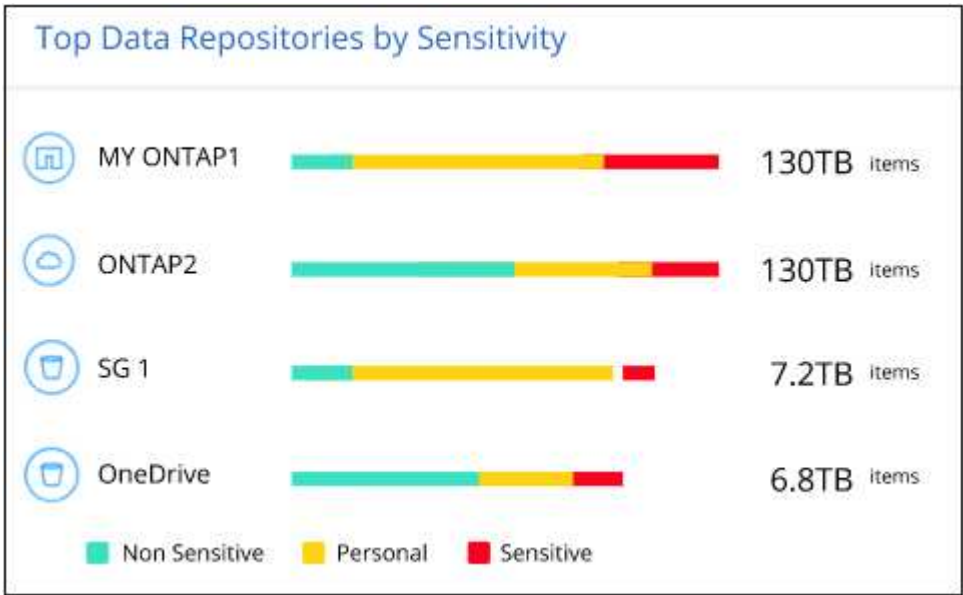
You can hover over each section to see the total number of items in each category.

Click each area to view the filtered results in the Data Sense Investigation page so that you can investigate further.

Domain Administrator Group control

The *Domain Administrator Group control* panel shows the most recent users who have been added into your domain administrator groups so that you can see if all the users should be allowed in those groups. You must have integrated a global Active Directory into Cloud Data Sense for this panel to be active.

The default administrative admin groups include "Administrators", "Domain Admins", "Enterprise Admins", "Enterprise Key Admins", and "Key Admins".

Data listed by types of open permissions

The *Open Permissions* panel shows the percentage for each type of permission that exist for all files that are being scanned. The chart is provided from Data Sense and it shows the following types of permissions:

- No Open Access
- Open to Organization
- Open to Public
- Unknown Access

You can hover over each section to see the percentage and total number of files in each category.

Click each area to view the filtered results in the Data Sense Investigation page so that you can investigate

further.

Data listed by encrypted files

The *Encrypted Files* panel shows the top 4 data sources with the highest percentage of files that are encrypted, over time. These are typically items that have been password protected. It does this by comparing the encryption rates over the past 7 days to see which data sources have a greater than 20% increase. An increase of this amount could mean that ransomware is already attacked your system.
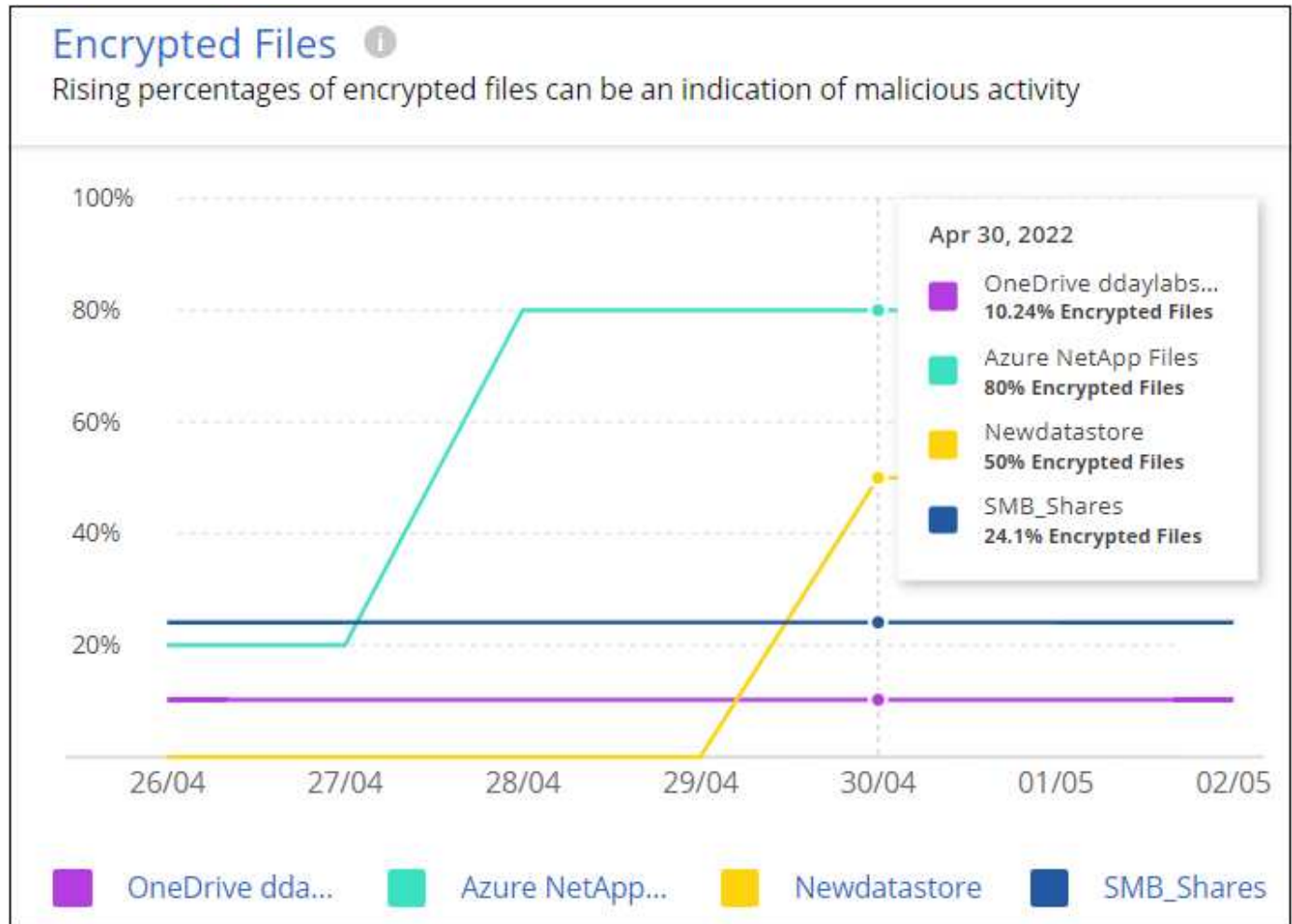
Click a line for one of the data sources to view the filtered results in the Data Sense Investigation page so that you can investigate further.

Status of ONTAP systems hardening

The *Harden your ONTAP environment* panel provides the status of certain settings in your ONTAP systems that track how secure your deployment is according to the NetApp Security Hardening Guide for ONTAP Systems and to the ONTAP anti-ransomware feature that proactively detects and warns about abnormal activity.

You can review the recommendations and then decide how you want to address the potential issues. You can follow the steps to change the settings on your clusters, defer the changes to another time, or ignore the suggestion.

This panel supports on-prem ONTAP, Cloud Volumes ONTAP, and Amazon FSx for NetApp ONTAP systems at

this time.

The settings that are being tracked include:

Hardening Objective	Description	Remediation
ONTAP Anti-ransomware	The percentage of volumes that have on-box anti-ransomware activated. Valid for on-prem ONTAP systems only. A green status icon indicates > 85% of volumes are enabled. Yellow indicates 40-85% are enabled. Red indicates < 40% are enabled.	See how to enable anti-ransomware on your volumes using System Manager.
ONTAP Version	The version of ONTAP software installed on your clusters. A green status icon indicates that the version is current. A yellow icon indicates that the cluster is behind by 1 or 2 patch versions or 1 minor version for on-prem systems, or behind by 1 major version for Cloud Volumes ONTAP. A red icon indicates that the cluster is behind by 3 patch versions, or 2 minor versions, or 1 major version for on-prem systems, or behind by 2 major versions for Cloud Volumes ONTAP.	See the best way to upgrade your on-prem clusters or your Cloud Volumes ONTAP systems.

Hardening Objective	Description	Remediation
Snapshots	Is the snapshot capability activated on data volumes, and what percentage of volumes have Snapshot copies. A green status icon indicates > 85% of volumes have snapshots enabled. Yellow indicates 40-85% are enabled. Red indicates < 40% are enabled.	See how to enable volume snapshots on your on-prem clusters or on your Cloud Volumes ONTAP systems.

Status of permissions on your critical business data

The *Business critical data permissions analysis* panel shows the permissions status of data that is critical for your business. That way you can quickly assess how well you are protecting your business critical data.
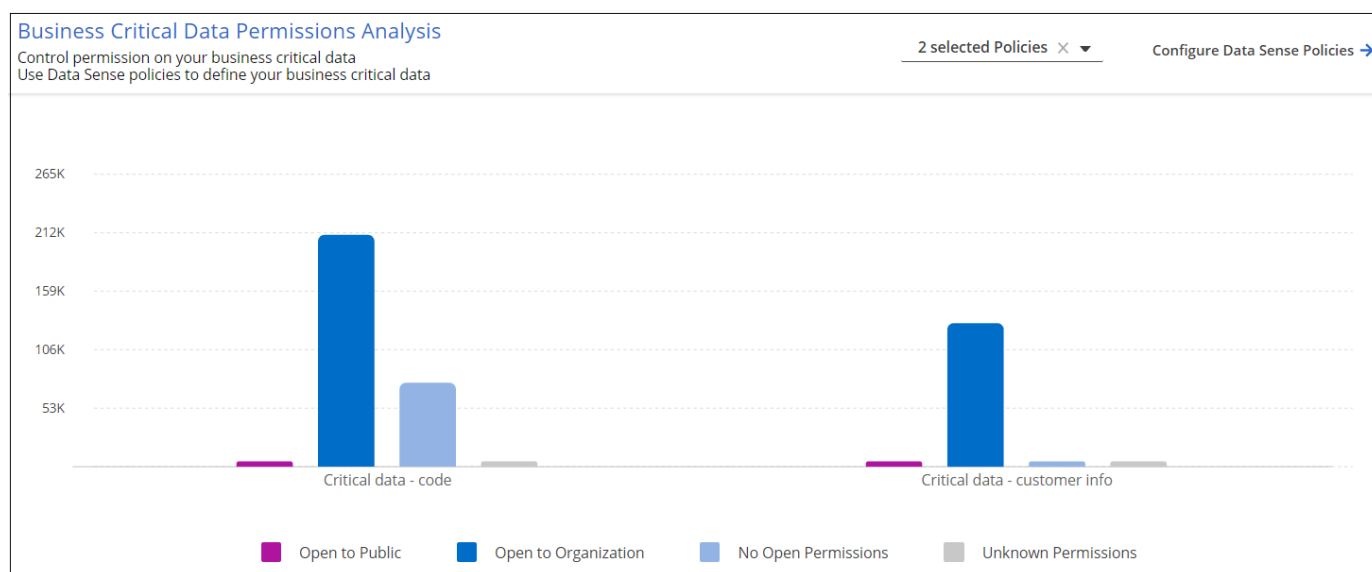
Initially this panel shows data based on default policies that we have selected. But you can select the 2 most important Data Sense *Policies* that you have created to view your most critical business data. See how to create your policies using Data Sense.

The graph shows permission analysis of all the data that meets the criteria from your policies. It lists the number of items that are:

- Open to public permissions – the items which Data Sense considers as open to public
- Open to organization permissions – the items which Data Sense considers as open to organization
- No open permissions – the items which Data Sense considers as no open permissions
- Unknown permissions – the items which Data Sense considers as unknown permissions

Hover over each bar in the charts to view the number of results in each category. Click a bar and the Data Sense Investigation page is displayed so you can investigate further about which items have open permissions and whether you should make any adjustments to file permissions.

Backup status of your critical business data

The *Backup Status* panel shows how different categories of data are being protected using Cloud Backup. This identifies how comprehensively your most important categories of data are backed up in case you need to recover because of a ransomware attack. This data is a visual representation of how many items of a specific category in a working environment are backed up.

Only on-prem ONTAP and Cloud Volumes ONTAP working environments that are already being backed up using Cloud Backup *and* scanned using Cloud Data Sense will appear in this panel.
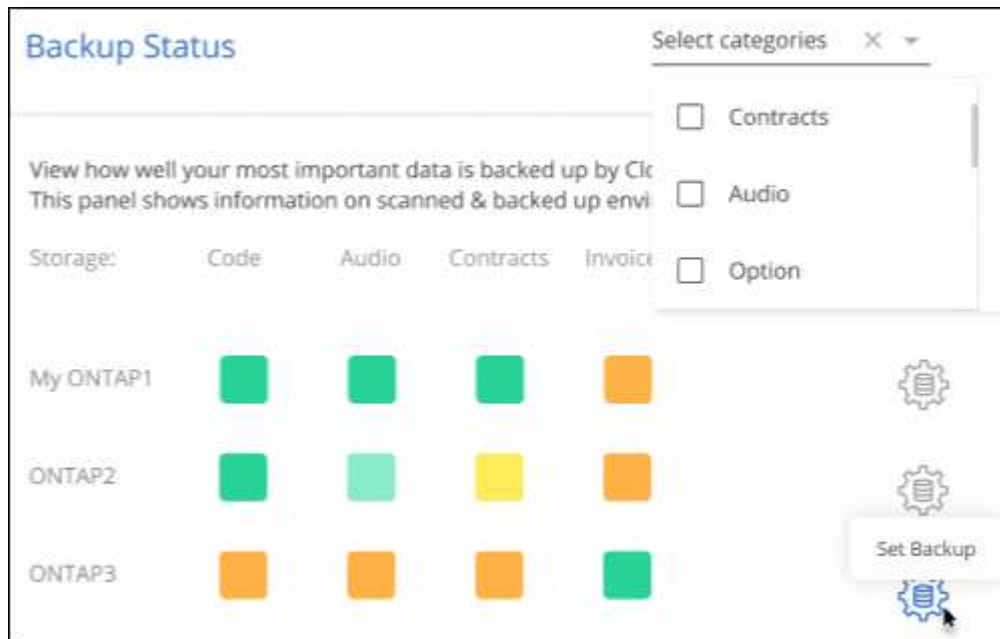
Initially this panel shows data based on default categories that we have selected. But you can select the categories of data that you want to track; for example, codes files, contracts, etc. See the full list of categories that are available from Cloud Data Sense for your working environments. Then select up to 4 categories.

After the data is populated, hover over each square in the charts to view the number of files that are backed up out of all files in the same category in the working environment. A green square means 85% or greater of your files are being backed up. A yellow square means between 40% and 85% of your files are being backed up. And a red square means 40% or fewer files are being backed up.

You can click the Cloud Backup button at the end of the row to go to the Cloud Backup interface to enable backup on more volumes in each working environment.

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, register for one.

2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

3. Click **NSS Management > Add NSS Account**.

4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

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

   This action enables Cloud Manager to use your NSS account.

   Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. In the **Resources** tab, click **Register for Support**.

3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

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

- Knowledge base

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

- Communities

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

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

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

Steps

1. In Cloud Manager, click **Help > Support**.

2. Choose one of the available options under Technical Support:

    a. Click **Call Us** to find phone numbers for NetApp technical support.

    b. Click **Open an Issue**, select one the options, and then click **Send**.

    A NetApp representative will review your case and get back to you soon.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager 3.9