



Secure your data from ransomware and internal attacks

Cloud Manager

NetApp
March 10, 2022

This PDF was generated from <https://docs.netapp.com/us-en/occm/concept-ransomware-protection.html> on March 10, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Secure your data from ransomware and internal attacks. 1
 - Learn about Ransomware Protection. 1
 - Managing cyber security recommendations for your data sources 2

Secure your data from ransomware and internal attacks

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 data 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^].

[Link to Cloud Central Ransomware Protection page](#)



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 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.
- 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.

[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
- OneDrive accounts
- SharePoint 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 Data Sense, Cloud Backup, and from other Cloud Manager resources, to populate the Ransomware Protection Dashboard.
2. You use the Ransomware Protection dashboard to gather 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.

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 <i>Working Environment</i> and <i>Category</i> (<i>Encrypted and Corrupted</i>) to view the list of all encrypted and corrupted files.

Alert	Description	Remediation
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 <i>Working Environment</i> , <i>Sensitivity Level (Sensitive Personal)</i> , and <i>Open Permissions</i> 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.

Top data repositories by data sensitivity

The *Top Data Repositories by Sensitivity Level* area 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* area shows the most recent five 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.

Domain Administrative Groups control ⓘ	
User "Ariel.Z" has joined "911" group	Dec 21, 2021
User "Shahar.Livschitz" has joined "enterprise_..."	Dec 21, 2021
User "Golan.K" has joined "system_administrators" group	Dec 21, 2021
User "Adi.M" has joined "123" group	Dec 21, 2021

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* area 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.

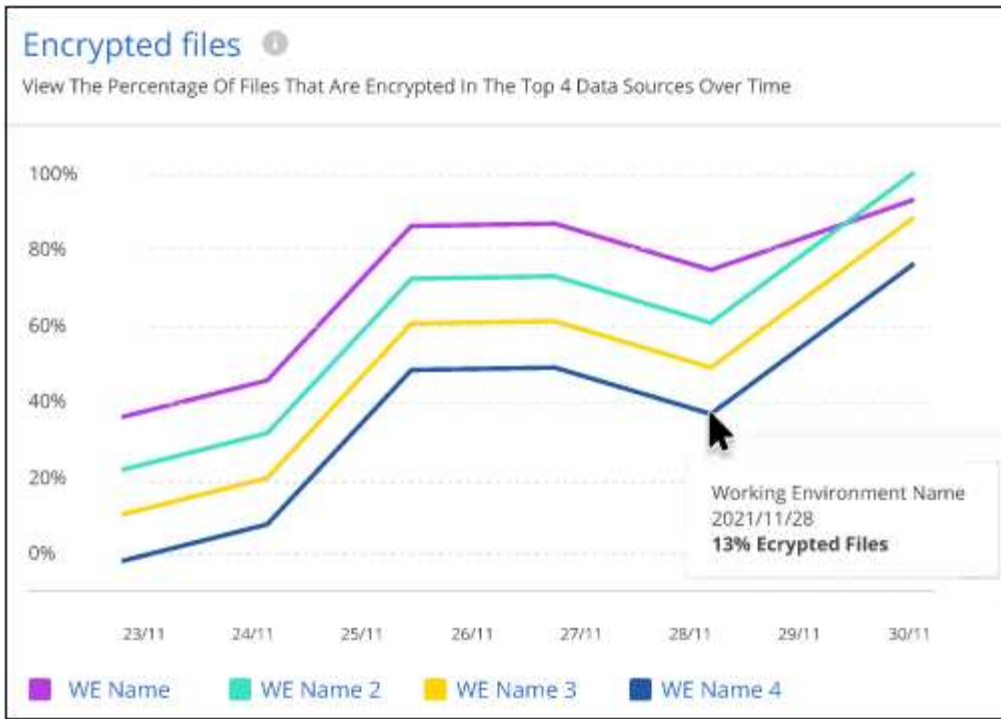
Click each area to view the filtered results in the Data Sense Investigation page so that you can investigate further.



Files in OneDrive accounts, SharePoint accounts, and in databases are not represented in this chart.

Data listed by encrypted files

The *Encrypted Files* area 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.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.