



Use BlueXP ransomware protection

BlueXP ransomware protection

NetApp
March 22, 2024

Table of Contents

- Use BlueXP ransomware protection 1
- Use BlueXP ransomware protection 1
- View workload health at a glance using the Dashboard 1
- Protect workloads against ransomware attacks 4
- Respond to a detected ransomware alert 10
- Recover from a ransomware attack (after incidents are neutralized) 12

Use BlueXP ransomware protection

Use BlueXP ransomware protection

Using BlueXP ransomware protection, you can view workload health and protect workloads.

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

View workload health at a glance using the Dashboard

The BlueXP ransomware protection Dashboard provides at-a-glance information about the protection health of your workloads. You can quickly determine workloads that are at risk or protected, identify workloads impacted by an incident or in recovery, and gauge the extent of protection by looking at how much storage is protected or at risk.

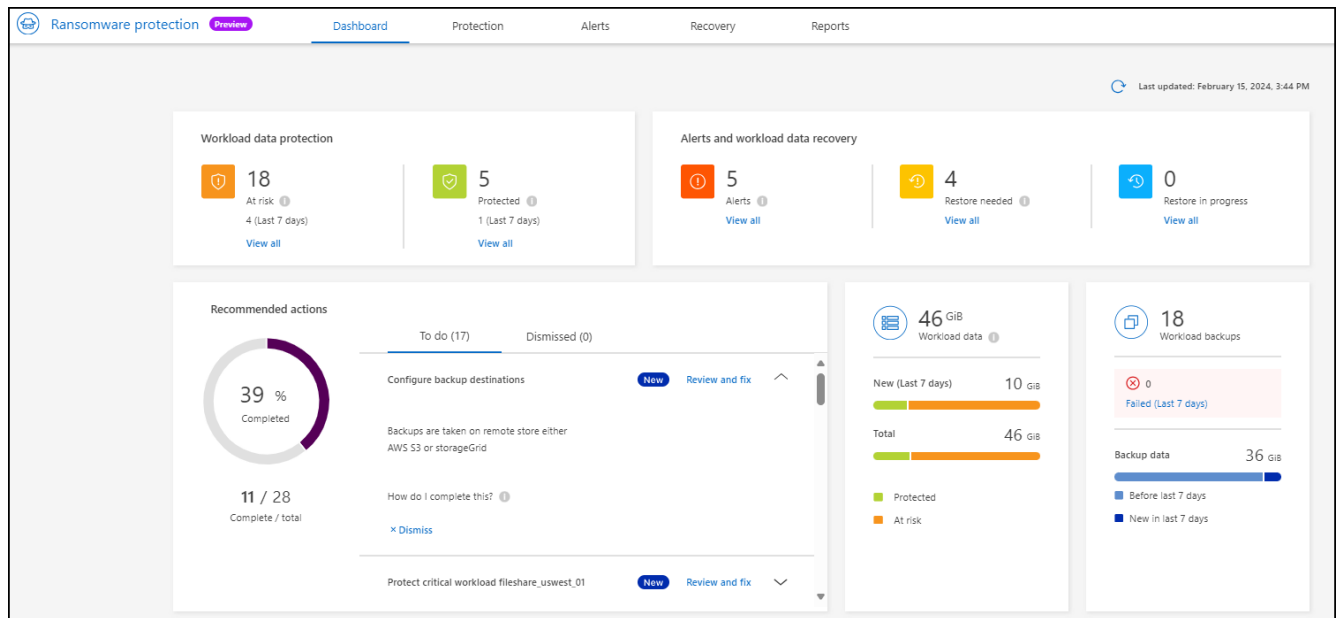
You can also use the Dashboard to review and act on protection recommendations.

Review workload health using the Dashboard

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.

After discovery, the Dashboard shows you the health of workload data protection.



2. From the Dashboard, you can view and do any of the following in each of the panes:

- **Workload data protection:** Click **View all** to see all workloads that are at risk or protected on the Protection page. Workloads are at risk when protection levels don't match a protection policy. Refer to [Protect workloads](#).
- **Alerts and workload data recovery:** Click **View all** to see active incidents that have impacted your workload, are ready for recovery after incidents are neutralized, or are in recovery. Refer to [Respond to a detected alert](#).

An incident is categorized in one of the following states:

- Impacted (shows on Alerts page)
- Ready for recovery (shows on Recovery page)
- Recovering (shows on Recovery page)
- Recovery failed (shows on Recovery page)
- Recovered (shows on Recovery page)
- **Recommended actions:** To increase protection, review each recommendation and click **Review and fix**.

Refer to [Review protection recommendations on the Dashboard](#) or [Protect workloads](#).

Any recommendations that were added since you last visited the Dashboard are indicated with "New" for at least 24 hours. Actions are listed in priority order with the most important at the top. You can review and act on each one or dismiss it.

The total number of actions does not include dismissed actions.

- **Workload data:** Monitor changes in protection coverage over the last 7 days.
- **Workload backups:** Monitor changes in workload backups created by the service that failed or completed successfully in the last 7 days.

Review protection recommendations on the Dashboard

BlueXP ransomware protection assesses the protection on your workloads and recommends actions to improve that protection.

You can review a recommendation and act on it, which changes the recommendation status to Complete. Or, if you want to act on it later, you can dismiss it. Dismissing an action moves the recommendation to a list of dismissed actions, which you can review later.

Here is a sampling of the recommendations that the service offers.

Recommendation	Description	How to resolve
Add a ransomware protection policy	The workload is currently not protected.	Assign a policy to the workload. Refer to Protect workloads against ransomware attacks .
Configure backup destinations	The workload does not currently have any backup destinations.	Add backup destinations to this workload to protect it. Refer to Configure protection settings .
Make a policy stronger.	Some workloads might not have enough protection. Strengthen protection on workloads with a policy.	Increase retention, add backups, enforce immutable backups, block suspicious file extensions, enable detection on secondary storage and more. Refer to Protect workloads against ransomware attacks .
Protect critical or important application workloads against ransomware.	The Protect page displays critical or important (based on the Priority level assigned) application workloads that are not protected.	Assign a policy to these workloads. Refer to Protect workloads against ransomware attacks .
Protect critical or important file share workloads against ransomware.	The Protection page displays critical or important workloads of the type File Share or Datastore that are not protected.	Assign a policy to each of the workloads. Refer to Protect workloads against ransomware attacks .
Review new alerts	New alerts exist.	Review the new alerts. Refer to Respond to a detected ransomware alert .

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. From the Recommended actions pane, select a recommendation and select **Review and fix**.
3. To dismiss the action until later, select **Dismiss**.

The recommendation clears from the To Do list and appears on the Dismissed list.



You can later change a dismissed item to a To Do item. When you mark an item completed or you change a dismissed item to a To Do action, the Total actions increases by 1.

4. To review information on how to act on the recommendations, select the **information** icon.

Protect workloads against ransomware attacks

You can protect workloads against ransomware attacks by completing the following actions using BlueXP ransomware protection.

- View existing workload protection.
- Assign a policy to a workload.
 - Increase application protection to prevent future RW attacks.
 - Change the protection for a workload that was previously protected in the RW service.
- Manage policies (only the ones that you created).

BlueXP ransomware protection assigns a priority to each workload during discovery. The workload priority is determined by the following Snapshot frequencies:

- **Critical:** Snapshot copies taken less than 1 per hour (highly aggressive protection schedule)
- **Important:** Snapshot copies taken less than 1 per day but greater than 1 per hour
- **Standard:** Snapshot copies taken more than 1 per day

Protection status: A workload can show one of the following protection statuses to indicate whether a policy is applied or not:

- **Protected:** A policy is applied.
- **At risk:** No policy is applied.
- **In progress:** A policy is being applied but not completed yet.
- **Failed:** A policy is applied but is not working.

Protection health: A workload can have one of the following protection health statuses:

- **Healthy:** The workload has protection enabled and backups and Snapshot copies have been completed.
- **In progress:** Backups or Snapshot copies are in progress.
- **Failed:** Backups or Snapshot copies have not completed successfully.
- **N/A:** Protection is not enabled or sufficient on the workload.

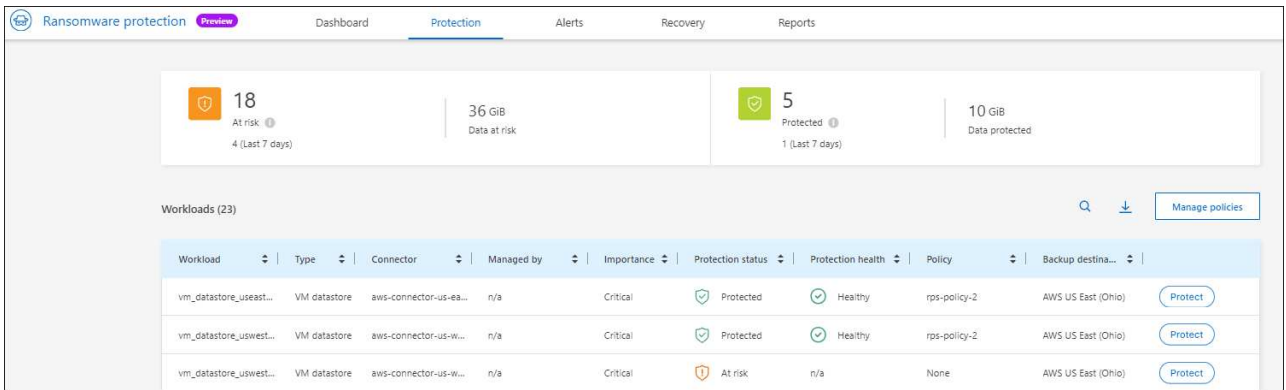
View workload ransomware protection

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

- VM workloads
- File share workloads

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. Do one of the following:
 - From the Dashboard Data Protection pane, select **View all**.
 - From the menu, select **Protection**.



3. From this page, you can assign a policy to a workload.

Assign a predefined protection policy to workloads

To help protect your data, you can assign an existing ransomware protection policy to one or more workloads. You can also assign a different policy to a workload that already has a policy.

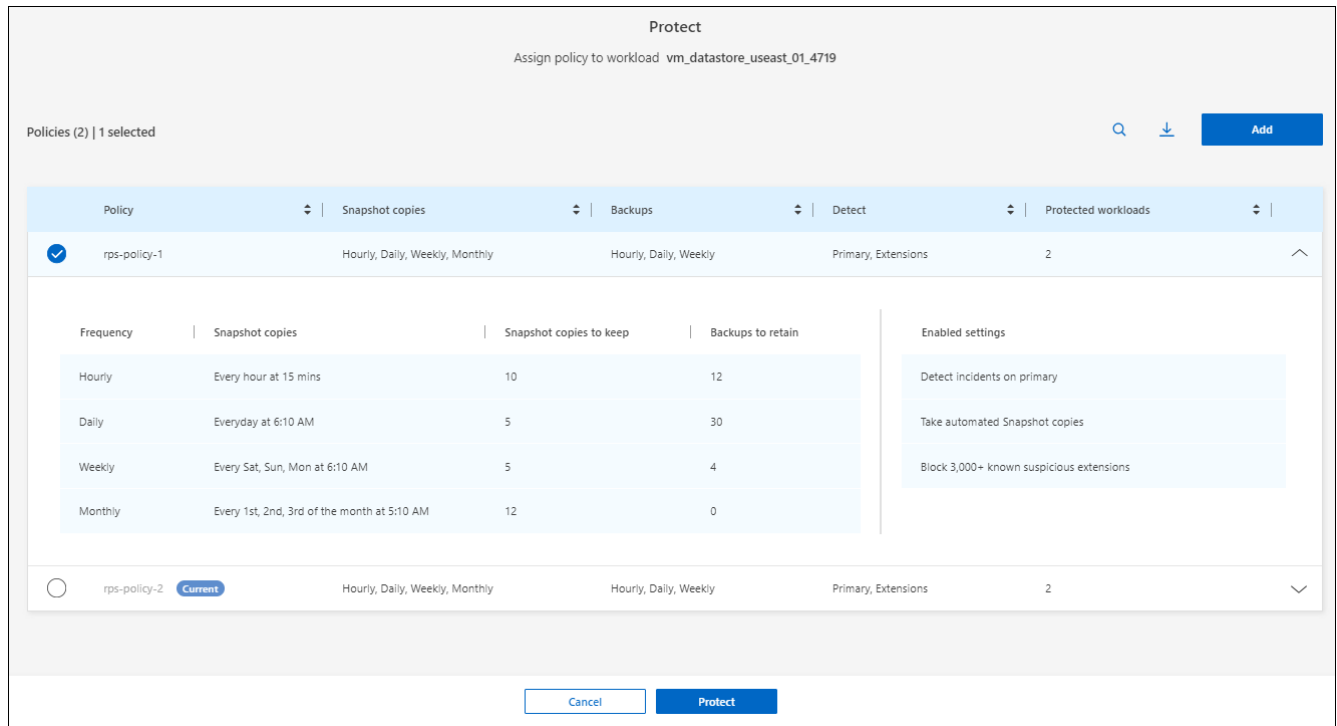
BlueXP ransomware protection includes the following predefined policies that are aligned with workload priority:

Policy level	Snapshot	Frequency	Retention (Days)	# of Snapshot copies	Total Max # of Snapshot copies
Critical workload policy	Quarter hourly	Every 15 min	3	288	309
	Daily	Every 1 day	14	14	309
	Weekly	Every 1 week	35	5	309
	Monthly	Every 30 days	60	2	309
Important workload policy	Quarter hourly	Every 30 mins	3	144	165
	Daily	Every 1 day	14	14	165
	Weekly	Every 1 week	35	5	165
	Monthly	Every 30 days	60	2	165
Standard workload policy	Quarter hourly	Every 60 min	3	72	93
	Daily	Every 1 day	14	14	93
	Weekly	Every 1 week	35	5	93
	Monthly	Every 30 days	60	2	93

Steps

1. From BlueXP ransomware protection, do one of the following:
 - From the Dashboard Data Protection pane, select **View all**.
 - From the Dashboard Recommendation pane, select a recommendation about assigning a policy and select **Review and fix**.
 - From the menu, select **Protection**.
2. From the Protection page, review the workloads and select **Protect** next to the workload.

A list of policies appears.



3. To see details, click on the down arrow on a policy.
4. Select a policy to assign to the workload.
5. Select **Protect**.
6. Review the Dashboard Recommended actions pane, which shows the action as "Completed."

Create a protection policy

If the existing policies do not meet your business needs, you can create a new protection policy. You can create your own from scratch or use an existing policy and modify its settings.

You can create policies that govern primary and secondary storage and treat primary and secondary storage the same or differently.

You can create a policy when you are managing them or during the process of assigning a policy to a workload.

Steps to create a policy during policy management

1. From the BlueXP ransomware protection menu, select **Protection**.

18 At risk (4 Last 7 days) | 36 GiB Data at risk | 5 Protected (1 Last 7 days) | 10 GiB Data protected

Workloads (23) Manage policies

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...
vm_datastore_useast...	VM datastore	aws-connector-us-aa...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)

2. From the Protection page, select **Manage policies**.

Protection > Manage policies

Manage policies

Policies (3) Add

Policy	Snapshot copies	Backups	Detect	Protected workloads
RPS-Policy-Critical	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
RPS-Policy-Importatnt	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
RPS-Policy-Standard	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	0

3. From the Manage policies page, select **Add**.

Protection > Manage policies > Add policy

Add policy

Policy name: test-policy

Copy from existing policy: No policy selected Select

Primary storage

- Snapshot copy schedules: Weekly
- Primary detection: Disable
- Block file extensions: Disable

Secondary storage

- Backup schedules: Weekly
- Secondary detection: Disable

Cancel Add

4. Enter a new policy name, or enter an existing policy name to copy it. If you enter an existing policy name, choose which policy to copy.



If you choose to copy and modify an existing policy, you must change at least one setting to make it unique.

5. For each item, select the Down arrow.

◦ **Primary storage:**

- **Snapshot copy schedules:** Choose schedule options, the number of Snapshot copies to keep, and select to enable the schedule.
- **Primary detection:** Enable the service to detect ransomware incidents on primary storage.
- **Block file extensions:** Enable this to have the service block known suspicious file extensions. The service takes automated Snapshot copies when Primary detection is enabled.

◦ **Secondary storage:**

- **Backup schedules:** Choose schedule options for secondary storage and enable the schedule.
- **Secondary detection:** Enable the service to detect ransomware incidents on secondary storage.
- **Lock backups:** Choose this to prevent backups on secondary storage from being modified or deleted for a certain period of time. This is also called *immutable storage*.

This option uses NetApp DataLock technology, which locks backups on secondary storage. The period of time that the backup file is locked (and retained) is called the DataLock Retention Period. It is based on the backup policy schedule and retention setting that you defined, plus a 14-day buffer. Any DataLock retention policy that is less than 30 days is rounded up to 30 days minimum.

6. Select **Add**.

Steps to create a policy during protection policy assignment

1. From the BlueXP ransomware protection menu, select **Protection**.

The screenshot displays the BlueXP ransomware protection dashboard. At the top, there are two summary cards: one for 'At risk' data (18 items, 36 GiB) and one for 'Protected' data (5 items, 10 GiB). Below these is a table of workloads with columns for Workload, Type, Connector, Managed by, Importance, Protection status, Protection health, Policy, and Backup destination. Each row includes a 'Protect' button.

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...	
vm_datastore_useast...	VM datastore	aws-connector-us-ea...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect

2. From the Protection page, select **Protect**.

3. From the Protect page, select **Add**.

Protection > Manage policies > Add policy

Add policy

Policy name

Copy from existing policy [Select](#)

Primary storage

Snapshot copy schedules	Weekly	▼
Primary detection	Disable	▼
Block file extensions	Disable	▼

Secondary storage

Backup schedules	Weekly	▼
Secondary detection	Disable	▼

4. Complete the process, which is the same as creating a policy from the Manage policies page.

Assign a different protection policy

You can choose a different protection policy for a workload.

You might want to increase the protection to prevent future ransomware attacks by changing the protection policy.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protect page, select a workload, and select **Protect**.
3. In the Protect page, select a different policy for the workload.
4. To change any details for the policy, select the down arrow on the right and change the details.
5. Select **Save** to finish the change.

Edit an existing policy

You can change the details of a policy only when the policy is not associated with a workload.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protection page, select **Manage policies**.
3. In the Manage policies page, select the **Actions** option for the policy you want to change.
4. From the Actions menu, select **Edit policy**.
5. Change the details.
6. Select **Save** to finish the change.

Delete a policy

You can delete a protection policy that is not currently associated with any workloads.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protection page, select **Manage policies**.
3. In the Manage policies page, select the **Actions** option for the policy you want to delete.
4. From the Actions menu, select **Delete policy**.

Respond to a detected ransomware alert

If BlueXP ransomware protection detects a possible attack, an alert appears on the BlueXP ransomware protection Dashboard and in the BlueXP Notifications in the upper right indicating a potential ransomware attack. The service also immediately initiates taking a Snapshot copy. At this point, you should look at the potential risk in the BlueXP ransomware protection **Alerts** tab.

To begin to recover your data, mark the alert as ready for recovery so that your storage administrator can begin the recovery process.

Each alert could have multiple incidents on different volumes with different statuses, so be sure to look at all incidents.

The service provides information called *evidence* about what caused the alert to be issued, such as the following:

- File extensions were created or changed
- File creation occurred and increased by a listed percentage
- File deletion occurred and increased by a listed percentage

An alert is based on the following types of behavior:

- **Potential attack:** An alert occurs when Autonomous Ransomware Protection detects a new extension and the occurrence is repeated more than 20 times in the last 24 hours (default behavior).
- **Warning:** A warning occurs based on the following behaviors:
 - Detection of a new extension has not been identified before and the same behavior does not repeat enough times to declare it as an attack.
 - High entropy is observed.
 - File read/write/rename/delete operations incurred a 100% surge in activity beyond the baseline.

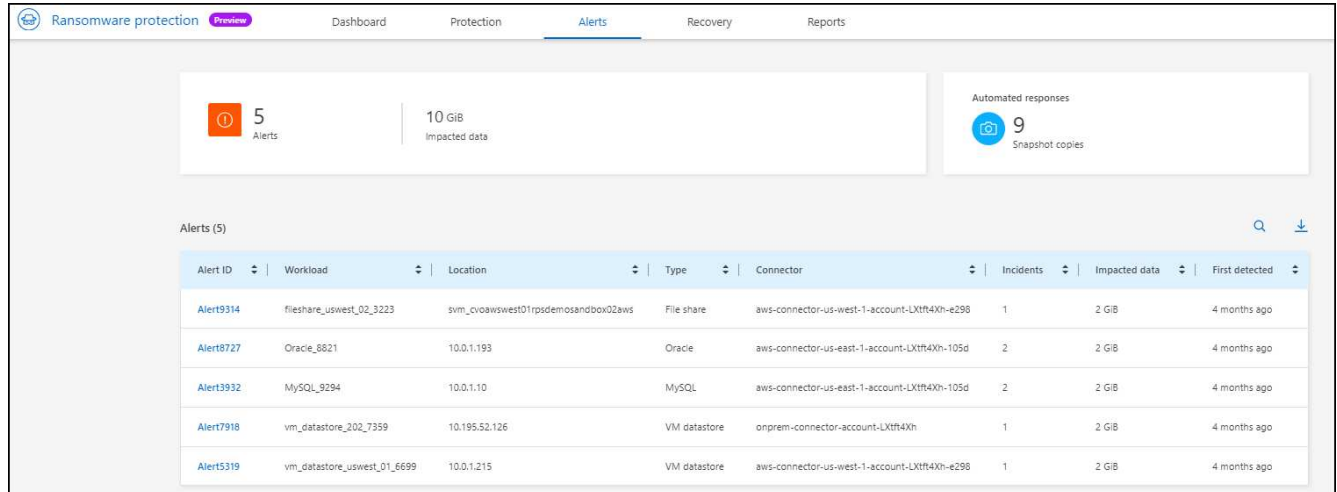
Evidence is based on information from Autonomous Ransomware Protection in ONTAP. For details, refer to [Autonomous Ransomware Protection overview](#).

View alerts

You can access alerts from BlueXP ransomware protection Dashboard or from the **Alerts** tab.

Steps

1. In the BlueXP ransomware protection Dashboard, review the Alerts pane.
2. Select **View all** under one of the statuses.
3. Click on an alert to review all incidents on each volume for each alert.
4. To review additional alerts, click on **Alert** in the breadcrumbs at the upper left.
5. Review the alerts on the Alerts page.



Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	filesystem_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtft4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	4 months ago

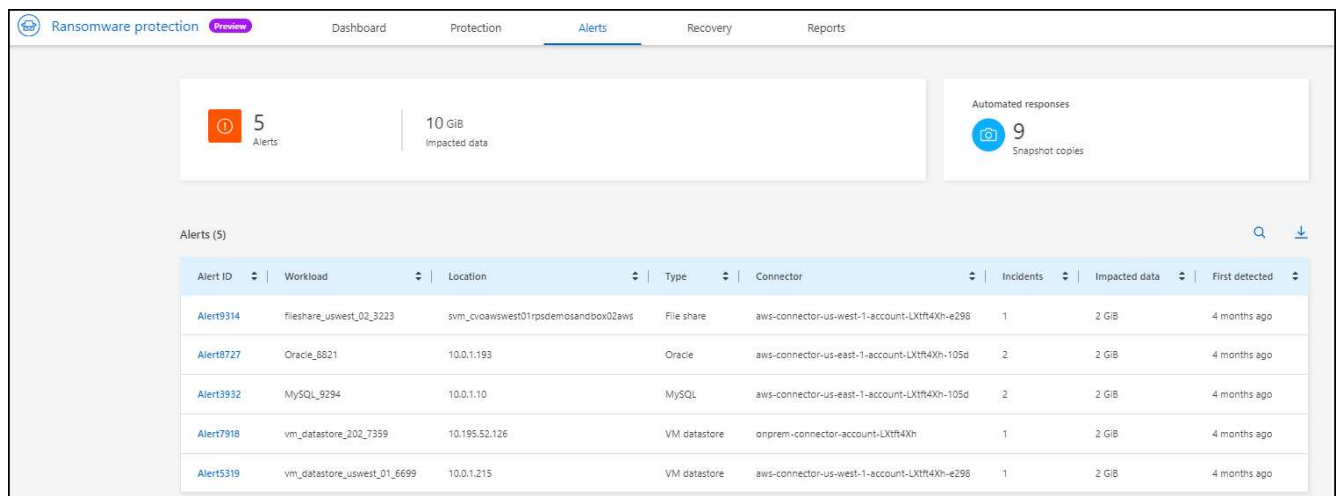
6. Continue with [Mark ransomware incidents as ready for recovery \(after incidents are neutralized\)](#).

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

After you have mitigated the attack and are ready to recover workloads, you should communicate with your storage admin team that the data is ready for recovery so that they can start the recovery process.

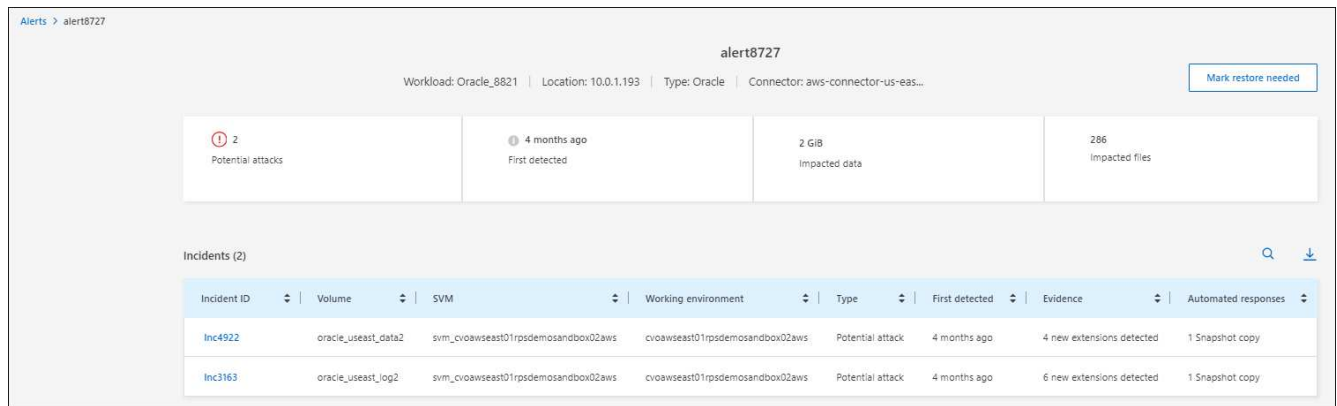
Steps

1. From the BlueXP ransomware protection menu, select **Alerts**.



Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	filesystem_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtft4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	4 months ago

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



- If you determine that the incidents are ready for recovery, select **Mark restore needed**.
- Confirm the action and select **Mark restore needed**.
- To initiate the workload recovery, select **Recover** workload in the message or select the **Recovery** tab.

Result

After the alert is marked for recovery, the alert moves from the Alerts tab to the Recovery tab.

Recover from a ransomware attack (after incidents are neutralized)

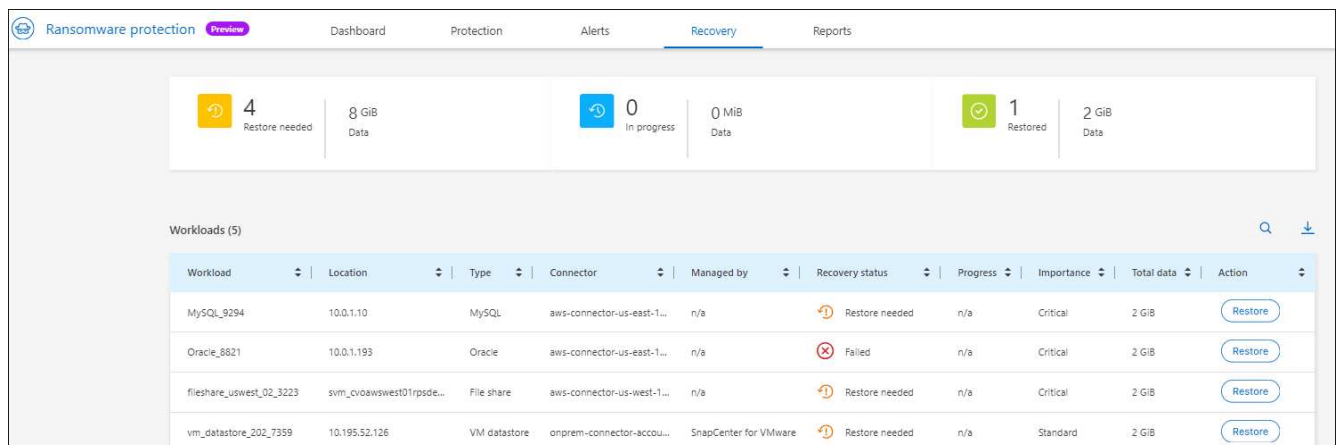
After workloads have been marked "Ready for recovery", BlueXP ransomware protection recommends a recovery point actual (RPA) and orchestrates the workflow for a crash-resistant recovery.

View workloads that are ready to be restored

Review the workloads that are in the "Restore needed" recovery status.

Steps

- Do one of the following:
 - From the Dashboard, review the "Restore needed" totals in the Alerts pane and select **View all**.
 - From the menu, select **Recovery**.
- Review the workload information in the **Recovery** page.



Recover a workload

Using BlueXP ransomware protection, the storage administrator can determine how best to recover workloads either from the recommended restore point or their preferred restore point.

The security storage admin can recover data at different levels:

- Recovery all volumes
- Recover an application at the volume level or file and folder level.
- Recover a file share at the volume level, directory, or file/folder level.
- Recover from a datastore at a VM level.

The process differs slightly depending on the workload type.

Steps

1. From the BlueXP ransomware protection menu, select **Recovery**.
2. Review the workload information in the **Recovery** page.
3. Select a workload that is in the “Restore needed” state.
4. To restore, select **Restore**.
5. **Restore scope**: Select the type of restore you want to complete:
 - All volumes
 - By volume
 - By file: You can specify a folder or single files to restore.

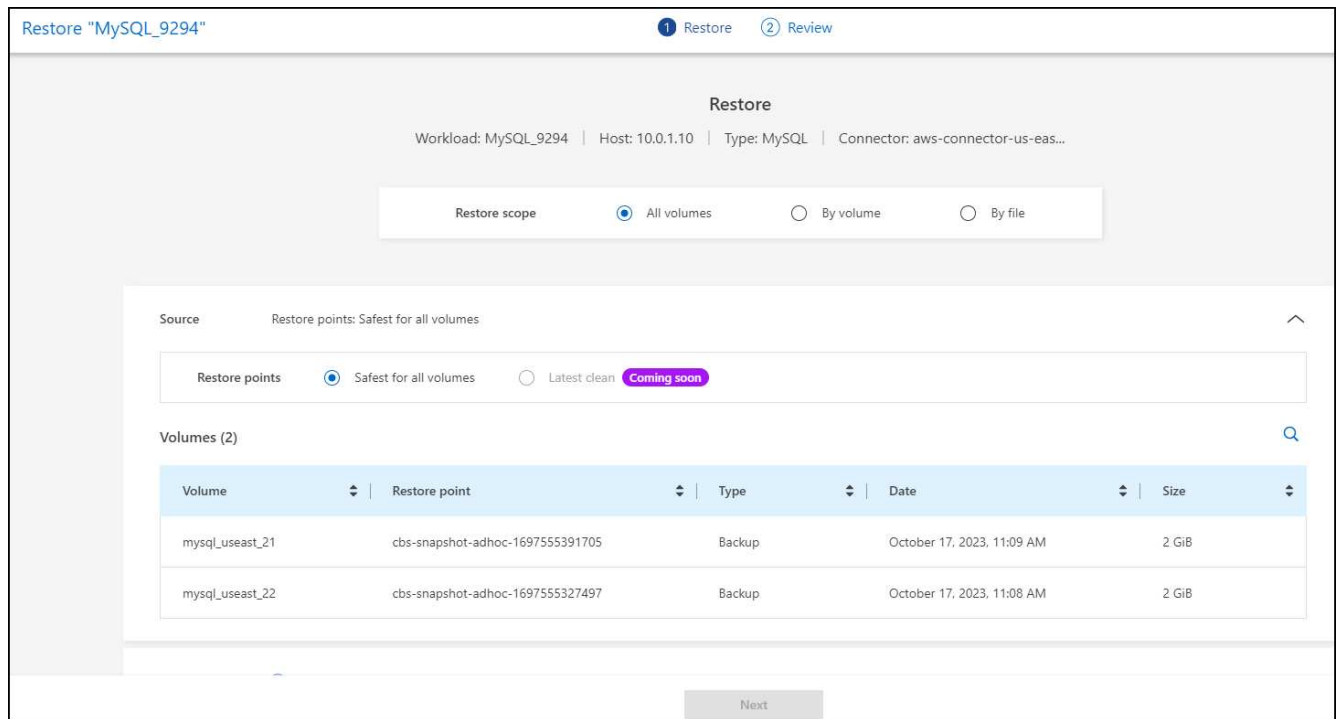


You can select up to 100 files or a single folder.

6. Continue with one of the following procedures depending on whether you chose application, volume, or file.

Restore all volumes

1. On the Restore page, in the Restore scope, select **All volumes**.



2. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Safest for all volumes” indication. This means that all volumes will be restored to a copy prior to the first attack on the first volume detected.

3. **Destination:** Select the down arrow next to Destination to see details.
 - a. Select the working environment.
 - b. Select the Storage VM.
 - c. Select the aggregate.
 - d. Change the volume prefix that will be prepended to all new volumes.

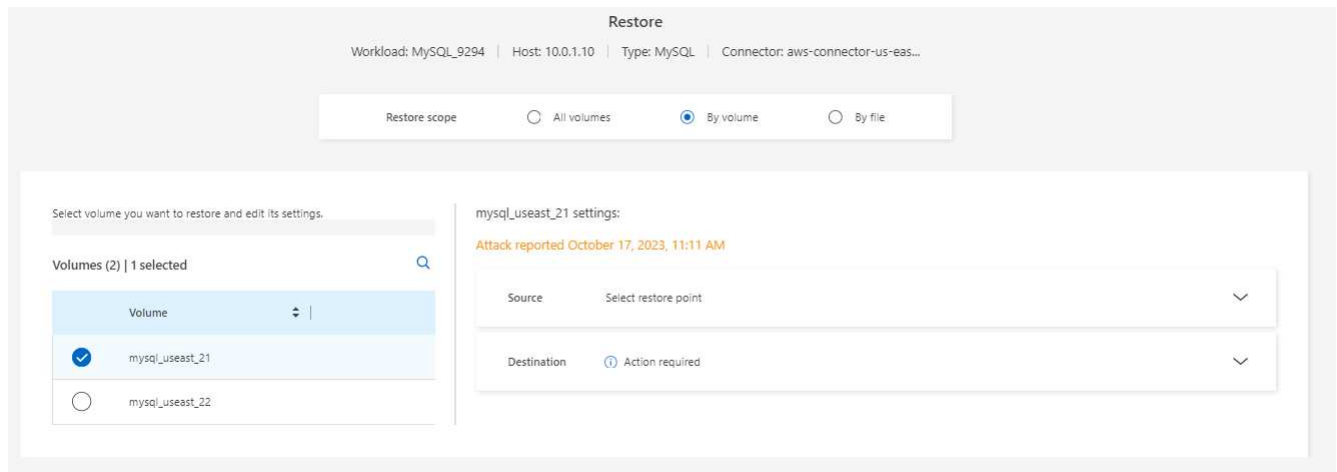


The new volume name appears as prefix + original volume name + backup name + backup date.

4. Select **Save**.
5. Select **Next**.
6. Review your selections.
7. Select **Restore**.
8. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the volume level

1. On the Restore page, in the Restore scope, select **By volume**.



2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

4. **Destination:** Select the down arrow next to Destination to see details.
 - a. Select the working environment.
 - b. Select the Storage VM.
 - c. Select the aggregate.
 - d. Review the new volume name.



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

5. Select **Save**.
6. Select **Next**.
7. Review your selections.
8. Select **Restore**.
9. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the file level

1. On the Restore page, in the Restore scope, select **By file**.
2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

b. Select up to 100 files or a single folder to restore.

4. **Destination:** Select the down arrow next to Destination to see details.

a. Choose where to restore the data: original source location or an alternate location that you can specify.



While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

b. Select the working environment.

c. Select the Storage VM.

d. Optionally, enter the path.



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

e. Select whether you want the names of the restored files or directory to be the same names as the current location or different names.

5. Select **Save**.

6. Select **Next**.

7. Review your selections.

8. Select **Restore**.

9. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a file share or datastore at the volume or file level

1. After selecting a file share or datastore to restore, on the Restore page, in the Restore scope, select **By volume** or **By file**.

2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

4. **Destination:** Select the down arrow next to Destination to see details.
 - a. Choose where to restore the data: original source location or an alternate location that you can specify.



While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

- b. Select the working environment.
- c. Select the Storage VM.
- d. Optionally, enter the path.



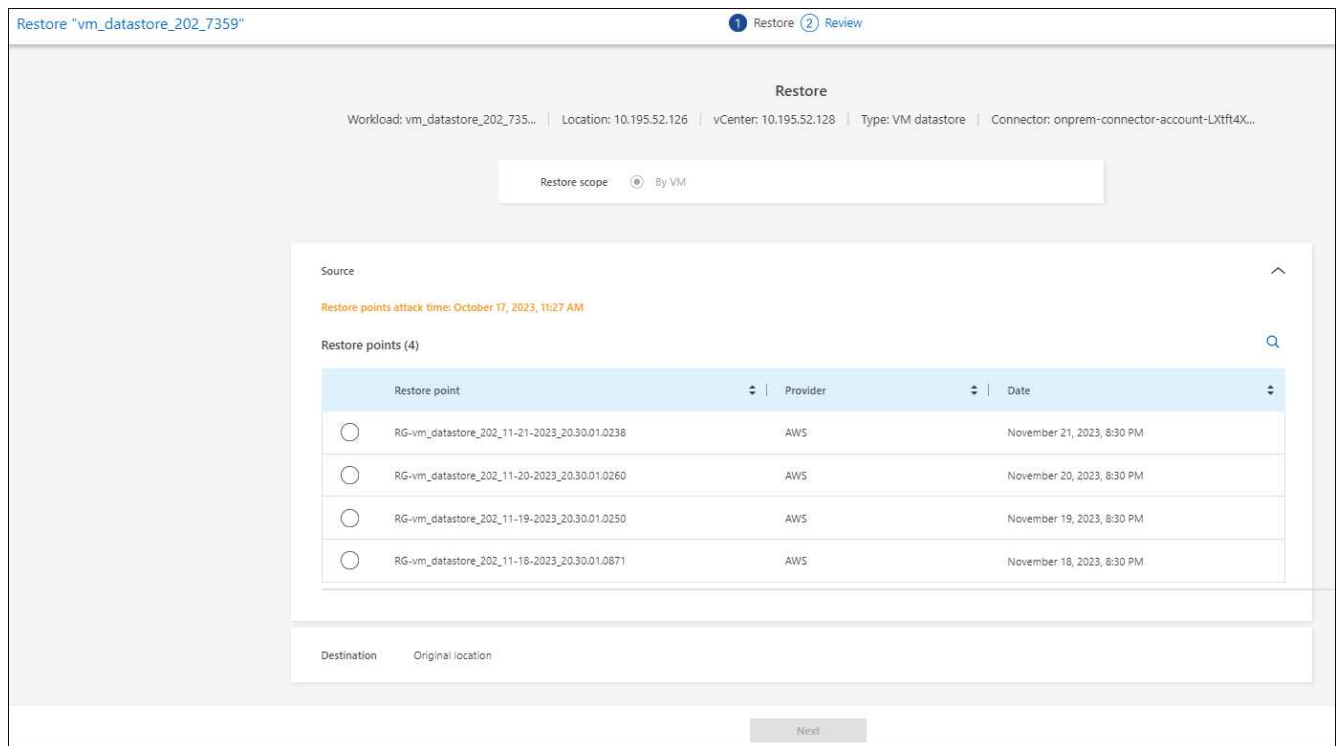
If you don't specify a path for the restore, the files will be restored to a new volume at the top-level directory.

5. Select **Save**.
6. Review your selections.
7. Select **Restore**.
8. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a VM file share at the VM level

On the Recovery page after you selected a VM to restore, continue with these steps.

1. **Source:** Select the down arrow next to Source to see details.



2. Select the restore point that you want to use to restore the data.
3. **Destination:** To original location.
4. Select **Next**.
5. Review your selections.
6. Select **Restore**.
7. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.