

Protect workloads

BlueXP ransomware protection

NetApp December 20, 2024

This PDF was generated from https://docs.netapp.com/us-en/bluexp-ransomware-protection/rp-use-protect.html on December 20, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Protect workloads	1
Protect workloads with ransomware strategies	1
Scan for personally identifiable information with BlueXP classification	. 14

Protect workloads

Protect workloads with ransomware strategies

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

- Enable workload-consistent protection, which works with SnapCenter Software or SnapCenter Plug-in for VMware vSphere.
- Create or manage ransomware protection strategies, which include policies that you create for snapshots, backups, and ransomware protection (known as *detection policies*).
- Import a strategy and adjust it.
- Group file shares to make it easier for you to protect workloads rather than protect them individually.
- Delete a ransomware protection strategy.

Which services are used in protection?

The following services can be used to manage protection policies. Protection information from these services appears in BlueXP ransomware protection:

- BlueXP backup and recovery for file shares, VM file shares
- SnapCenter for VMware for VM datastores
- SnapCenter for Oracle and MySQL

Protection policies

You might find it helpful to review information about the protection policies you can change and what types of policies are in a protection strategy.

Which protection policies can you change?

You can change protection policies based on the workload protection you have:

- Workloads not protected by NetApp applications: These workloads are not managed by SnapCenter, SnapCenter Plug-in for VMware vSphere, or BlueXP backup and recovery. These workloads might have snapshots taken as part of ONTAP or other products. If ONTAP FPolicy protection is in place, you can change the FPolicy protection using ONTAP.
- Workloads with existing protection by NetApp applications: These workloads have backup or snapshot policies managed by SnapCenter, SnapCenter for VMWare vSphere, or BlueXP backup and recovery.
 - If snapshot or backup policies are being managed by SnapCenter, SnapCenter for VMWare, or BlueXP backup and recovery, they will continue to be managed by these applications. Using BlueXP ransomware protection, you can also apply a ransomware detection policy to those workloads.
 - If a ransomware detection policy is being managed by Autonomous Ransomware Protection (ARP) and FPolicy in ONTAP, those workloads are protected and will continue to be managed by ARP and FPolicy.

Which policies are required in a ransomware protection strategy?

The following policies are required in ransomware protection strategy:

- · Ransomware detection policy
- Snapshot policy

A backup policy is not required in the BlueXP ransomware protection strategy.

View ransomware protection on a workload

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:

- · Application 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 Data Protection pane on the Dashboard, select View all.
 - From the menu, select **Protection**.

16 Atria 0 4 Gatt 7 0	e Seysti		32 dia Desistina			Rectaction	t () mysi	14 G8 Data protecte	r.		
Workloads		Protection grou	pa								
Vorkloads (24)									٩	1 Manage pr	otection strategies
Workload 0	Type = 1	Connector \$	Importance # 0	Ø maye. :	Protection 7 2	Protection V 0	Detection V 0	Detection マコー	Snapshot	Backup dest	
Ve_datantore_useas	VM Ne share	avi-contector-us	Critical	n/a	Protected	n/9	Active	rps-policy-all	BLet?? rancohwa	netapp-bickup-vs	(141 proversion
We_datastore_unsee	VM Neishare	avs-connector-us	criscat	na-	Protected	r\9	Learning mode	rps-policy-all	BLWXP rancomwa	NHopp-bickup-vs	(Tat polacion
Vm, datastore, useen	VM file share	avs-connector-us	Standard	n/a	🛈 at rok	0,9	None	Norw	None	Netiep-bickup-vs	Protect
Vm, datastore, usee	VM file share	avs-connector-us	Standard	n/a	🕑 až rok	n9	None	Norw	None	NHIEP-bickup-vs	Protect
Vm_datastore,useas	VM file share	avs-connector-us	Mandard	Nie	🛈 42 risk	11/2	hone	None	Nore	Helep-bolsp-vs-	Protect
Vm, datastore, 201, 3	VM Ne share	onprem-connecto	Standard	n/a	🕑 atriik	1/3	None	None	None	netapp-backup-vs	Protect
Oracle_6821	Oracle	avi-comedor-us	Critical	10	Protected	0.9	Active	rps-policy-all	buex7 rancomea	netapp-backup-us	(Edt protection

3. From this page, you can view and change protection details for the workload.



For workloads that already have a protection policy with SnapCenter or BlueXP backup and recovery service, you cannot edit the protection. For these workloads, BlueXP ransomware enables Autonomous Ransomware Protection and/or FPolicy protection if they are already activated in other services. Learn more about Autonomous Ransomware Protection, BlueXP backup and recovery, and ONTAP FPolicy.

Protection details on the Protection page

The Protection page shows the following information about workload protection:

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. ARP is enabled on all volumes related to the workload.
- At risk: No policy is applied. If a workload does not have a primary detection policy enabled, it is "at risk" even if it has a snapshot and backup policy enabled.
- In progress: A policy is being applied but not completed yet.
- Failed: A policy is applied but is not working.

Detection status: A workload can have one of the following ransomware detection statuses:

- Learning: A ransomware detection policy was recently assigned to the workload and the service is scanning workloads.
- Active: A ransomware detection protection policy is assigned.
- Not set: A ransomware detection protection policy is not assigned.
- Error: A ransomware detection policy was assigned, but the service has encountered an error.



When protection is enabled in BlueXP ransomware protection, alert detection and reporting begins after the ransomware detection policy status changes from Learning mode to Active mode.

Detection policy: The name of the ransomware detection policy appears, if one has been assigned. If the detection policy has not been assigned, "N/A" appears.

Snapshot and backup policies: This column shows the snapshot and backup policies applied to the workload and the product or service that is managing those policies.

- Managed by SnapCenter
- Managed by SnapCenter Plug-in for VMware vSphere
- Managed by BlueXP backup and recovery
- · Name of ransomware protection policy that governs snapshots and backups
- None

Workload importance

BlueXP ransomware protection assigns an importance or priority to each workload during discovery based on an analysis of each workload. The workload importance is determined by the following snapshot frequencies:

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

Predefined detection policies

You can choose one of the following BlueXP ransomware protection predefined policies, which are aligned with workload importance:

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

Enable application- or VM-consistent protection with SnapCenter

Enabling application- or VM-consistent protection helps you protect your application or VM workloads in a consistent manner, achieving a quiescent and consistent state to avoid potential data loss later if recovery is needed.

This process initiates registering SnapCenter Software Server for applications or SnapCenter Plug-in for VMware vSphere for VMs using BlueXP backup and recovery.

After you enable workload-consistent protection, you can manage protection strategies in BlueXP ransomware protection. The protection strategy includes the snapshot and backup policies managed elsewhere along with a ransomware detection policy managed in BlueXP ransomware protection.

To learn about registering SnapCenter or SnapCenter Plug-in for VMware vSphere using BlueXP backup and recovery, refer to the following information:

- Register SnapCenter Server Software
- Register SnapCenter Plug-in for VMware vSphere

Steps

- 1. From the BlueXP ransomware protection menu, select **Dashboard**.
- 2. From the Recommendations pane, locate one of the following recommendations and select **Review and fix**:
 - Register available SnapCenter Server with BlueXP
 - Register available SnapCenter Plug-in for VMware vSphere (SCV) with BlueXP
- 3. Follow the information to register the SnapCenter or SnapCenter Plug-in for VMware vSphere host using BlueXP backup and recovery.
- 4. Return to BlueXP ransomware protection.
- 5. From BlueXP ransomware protection, go the Dashboard and initiate the discover process again.
- 6. From BlueXP ransomware protection, select Protection to view the Protection page.
- 7. Review details in the snapshot and backup policies column on the Protection page to see that the policies are managed elsewhere.

Add a ransomware protection strategy

You can add a ransomware protection strategy to workloads. The way you do this depends on whether snapshot and backup policies exist already:

- Create a ransomware protection strategy if you have no snapshot or backup policies. If snapshot or backup policies do not exist on the workload, you can create a ransomware protection strategy, which can include the following policies that you create in BlueXP ransomware protection:
 - Snapshot policy
 - Backup policy
 - Ransomware detection policy
- Create a detection policy to workloads that already have snapshot and backup policies, which are managed in other NetApp products or services. The detection policy will not change the policies managed in other products.

Create a ransomware protection strategy (if you have no snapshot or backup policies)

If snapshot or backup policies do not exist on the workload, you can create a ransomware protection strategy, which can include the following policies that you create in BlueXP ransomware protection:

- Snapshot policy
- Backup policy
- Ransomware detection policy

Steps to create a ransomware protection strategy

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

16 Atria 0 40.4170	i Seysti		32 Gill Data at Hilk			Restance 1 Gent 7	f Q daya	14 G8 Data potecte	r		
Workloads		Protection grou	pa								
Workloads (24)									Q	± Manage p	otection strategies
Workload 0	Type = 0	Connector \$	Importance = 0	Ø maye_ =	Protection 7 2	Protection V 0	Detection T \$	Detection * \$	Snapshot * \$	Backup desti \$	
Wei, datactore, useas	VM Ne share	avs-connector-us	cynos	n/a	Protected	n/9	A.Cist	rps-policy-all	Burth ranconwa	wtapp-backup-vs	(1dt prmettan)
Ve_datadore.power	shi file share	ava-connector-us	crical	60	Protected	n/9	Learning mode	rps-policy-all	Bluet/Pranscriwk	wapp-backup-vs	(Int putecion)
Vm, dutactore, useen	vM file share	avs-connector-us	Sandard	n/a	🕑 at rijk	n,9	Norei	None	Note	netop-teckup-vs	Protect
Vm, datastore, asser	VM file share	ava-connector-us	Standard	n/a	🕑 az rijk	6,9	Nore	None	None	netipp-backup-vs	Protect
Vm_datastore_users	VM file share	ava-connect()-vis	thandard	n/a	🛈 azaisk	1/3	hone	None	Note	retep-backsprys-	Protect
Vm_datastove_201_3	vM file share	onpremiconnecto	Standard	ey'a	🕐 semk	15/3	None	None	None	retapp-backup-vs	Protect
Oracle_6521	Oracle	avi-connector-us	Orhall	na -	Protected	n.9	Active	rps-policy-all	BueX7 ransomea	retapp-backup-us	(filt protection)

2. From the Protection page, select Manage protection strategies.

Protection > Ranson	nware protection strategies													
				1	Ransomware protec	tion strate	gies							
	Ransomware protection strategies (I)									a).	±		Add	
	Ransonware protection strategy	*1	Snapshot policy	्रदेश	Backup policy	(#1	Detection policy	(* 1) (* 1)	Protected workloads			0 0 1	. 1	
	(pi-strategy-ortical		intici/-si-policy		orisial-bu-policy		rpt-policy-all		3.				\sim	
	spi-strategy-important		important-sc-policy		important-bu-policy		rps-policy-all		(t)				~ .	
	rps-strategy-standard		standard-supplicy		(tandard bu policy		tps-policy-all		Ø.				~	

3. From the Ransomware protection strategies page, select Add.

Protection > Manage protection strategies > Add ransomware	protection strategy				
			Add ransomware j	protection strategy	
	Ransomware protection strategy name	2		Copy from existing ransomware protection strategy	
	RPS strategy 1			No policy selected	5 Select
	Detection policy	rps-policy-primary			~
	Snapshot policy	important-ss-policy			~
	Backup policy	None			~
			Cancel	Add	

4. Enter a new strategy name, or enter an existing name to copy it. If you enter an existing name, choose which one to copy and select **Copy**.



If you choose to copy and modify an existing strategy, the service appends "_copy" to the original name. You should change the name and at least one setting to make it unique.

5. For each item, select the **Down arrow**.

• Detection policy:

- Policy: Choose one of the predesigned detection policies.
- **Primary detection**: Enable ransomware detection to have the service detect potential ransomware attacks.
- 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.

If you want to change the blocked file extensions, edit them in System Manager.

• Snapshot policy:

- **Snapshot policy base ame**: Select a policy or select **Create** and enter a name for the snapshot policy.
- **Snapshot locking**: Enable this to lock the snapshot copies on primary storage so that they cannot be modified or deleted for a certain period of time even if a ransomware attack manages its way to the backup storage destination. This is also called *immutable storage*. This enables quicker restore time.

When a snapshot is locked, the volume expiration time is set to the expiration time of the snapshot copy.

Snapshot copy locking is available with ONTAP 9.12.1 and later. To learn more about SnapLock, refer to SnapLock in ONTAP.

- **Snapshot schedules**: Choose schedule options, the number of snapshot copies to keep, and select to enable the schedule.
- Backup policy:
 - Backup policy basename: Enter a new or choose an existing name.
 - Backup schedules: Choose schedule options for secondary storage and enable the schedule.



To enable backup locking on secondary storage, configure your backup destinations using the **Settings** option. For details, see Configure settings.

6. Select Add.

Add a detection policy to workloads that already have snapshot and backup policies

With BlueXP ransomware protection, you can assign a ransomware detection policy to workloads that already have snapshot and backup policies, which are managed in other NetApp products or services. The detection policy will not change the policies managed in other products.

Other services, such as BlueXP backup and recovery and SnapCenter, use the following types of policies to govern workloads:

- · Policies governing snapshots
- · Policies governing replication to secondary storage

• Policies governing backups to object storage

Steps

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

16 Atria 0 4 (Latt 7)	li dayıştı		32 Gið Data at Hak			8	7 Sectorcles	f () myst	14 G/8 Data protecte	¢		
Workloads		Protection grou	pa									
Vorkloads (24)										٩	± Manag	e protection strategies
Workload C	Type = 0	Connector \$	Importance = 0	Ø maye. :	Protection	v 2 Protect	ion	Detection V 4	Detection * 0	Stupshot * \$	Backup desti \$	j.
We_datartore_useas	VM Neshare	avs-connector-us	cynos	n/b	D Protect	eyn bi		Adist	rps-policy-all	Blueto rancohwa	rwtapp-bickup-vs	. (141 provertion
Ve_datadore_unee	VM Ne share	ava-connector-us	crical	6.0	D Protect	na na		Learning mode	rps-policy-all	Buelli ransoniwa	(wtapp-backup-vs	Tat putecion
Vm, datastore, useen	VM file share	avs-conrector-us	Standard	n/a	🕑 at rok	0.9		Norw	Norw	Note	retep-backup-vs	Protect
Vm, datastore, unwe	VM Ne share	avs-connector-us	Standard	n/a	🕑 az tişk	0,9		None	Nonw	None	nitsep-bickup-vs	Picket
Vm_datastore_useus	VM file share	ava-connector-us	thandard	nia	🕡 szeisk	e/a		None	None	Nore	retipp-biolog-ys	Protect
Vm_datastore_201_3	VM Ne share	onprem-connecto	Standard	n/a	🕑 senik	6/3		None	None	None	netapp-backup-us	Protect
Oracle_6521	Orade	avi-contector-us	Orthoat	na .	Protect	en b		Active	rps-policy-att	Buell? ramonwa	retapp-backup-us	Edt protection

2. From the Protection page, select a workload, and select Protect.

The Protect page shows the policies managed by SnapCenter Software, SnapCenter for VMware vSphere, and BlueXP backup and recovery.

The following example shows policies managed by SnapCenter:

Select a detection policy to apply to the workload Oracle_9819. Detection policies (2) 1 selected Q Name Primary detection Pi Block suspicious file extensions rps-policy-1 Yes Yes rps-policy-2 Yes No (i) rps-policy-2 Yes (ii) ss-policy-daily1 (snapshot policy	by SnapCenter SnapCenter will not be modified by to this workload.
Detection policies (2) 1 selected Q Policies managed by Name Primary detection Block suspicious file extensions rps-policy-1 Yes Yes No ss-policy-daily1 Snapshot policy Ss-policy-daily1 Snapshot policy Ss-policy-daily1 Snapshot policy Snapshot policy Snapshot policy Snapshot policy Snapshot policy Snapshot policy Stanpshot policy <l< th=""><th>by SnapCenter SnapCenter will not be modified by to this workload.</th></l<>	by SnapCenter SnapCenter will not be modified by to this workload.
Name \$ Primary detection \$ Block suspicious file extensions \$ Image: state s	SnapCenter will not be modified by to this workload.
Image: wide of the section policy of the section	to this workload.
rps-policy-2 Yes No Image: State of the state of th	
ss-policy-weekly Snapshot policy	~
	v1 ~
ss-policy-weekly Snapshot policy	^{y2} ~
ss-policy-month Snapshot policy	niyi 🗸 🗸

The following example shows policies managed by BlueXP backup and recovery:

			Protect	be workload. My	9008 IO2v
			Server a detection pointy to apply to t	ne workload ing	Jude_0000.
Dete	ction policies (2)) 1 selected		Q	Policies managed by BlueXP backup and recovery
	Name	Primary detection	Block suspicious file extensions	÷	These policies managed by BlueXP backup and recovery will not be
0	rps-policy-1	Yes	Yes		modified by applying a detection policy to this workload.
0	rps-policy-2	Yes	No		(a) standart-snapshot-policy Snapshot policy
					standart-backup-policy Backup policy
			Cancel	Protect	

- 3. To see details of the policies managed elsewhere, click the **Down arrow**.
- 4. To apply a detection policy in addition to the snapshot and backup policies managed elsewhere, select the Detection policy.
- 5. Select Protect.
- 6. On the Protection page, review the Detection policy column to see the Detection policy assigned. Also, the snapshot and backup policies column shows the name of the product or service managing the policies.

Assign a different policy

You can assign a different protection policy replacing the current one.

Steps

- 1. From the BlueXP ransomware protection menu, select Protection.
- 2. From the Protection page, on the workload row, select Edit protection.
- 3. In the Policies page, click the down arrow for the policy you want to assign to review the details.
- 4. Select the policy you want to assign.
- 5. Select **Protect** to finish the change.

Group file shares for easier protection

Grouping file shares makes it easier to protect your data estate. The service can protect all volumes in a group at the same time rather than protect each volume separately.

Steps

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

16 At max, 40 4 (Latt 7 o	i Seys)		32 dia Data at Hak			0	7 Protected (0) 1 Gast 7 days	14 Gi8 Data protecte	ŕ		
Workloads		Protection grou	pa								
Workloads (24)									Q	1 Manage p	rotection itrategies
Workload 0	Type = 1	Connector \$	Importance # 0	@ mays_ \$	Protection	7 2 Protection		Detection * * 1	Snapshot = 0	Backup dest \$	
Wei_datastore_useas	VM Ne share	avs-connector-us	critical	n/b	🕑 Protech	e'n bi	Adlet	rps-policy-all	Bluet/Francohiva	rwtapp-blokup-ss.,	(Edit protection)
Ve_datastore_union	sht file share	ava-connector-us	crical	64	Protect	a va	Learning mode	rps-policy-all	BluettP ransomwk	retopp-backup-vs	(Int protection)
Vm, datastore, useen	vtd file share	avs-conrector-us	Standard	n/a	🛈 at rok	0/2	None	Norw	None	Netsep-backup-vs	Protect
Vm, datastore, usee	VM Ne share	avs-connector-us	Sandard	n/a	🕑 at tişk	0/9	None	Nonw	None	Netsep-bickup-vs	Protect
Vm_datastore_useus	VM file share	avs-connector-us	thandard	nia	🛈 42 Aliak	n/m	hone	None	Nore	retapp-backsprys-	Protect
Vm_datastore_201_3	VM Ne share	onprem-connecto	Standard	n/a	🕑 senik	1/3	None	None	None	retupp-backup-ut	Protect
Oracle_6521	Oracle	avi-contector-us	Critical	19	Protects	d na	Active	rps-policy-all	Buell? ransomea	netapp-backup-us	(Edt protection)

2. From the Protection page, select the **Protection groups** tab.

00 16 At Halt © 4 hast 7 days	32 GB Corta at mik	7 Protected 1 Rate 7 of	e O 14 Gas Deta protected		
Workloads	Protection groups				
etection groups (1) Id groups to manage protection across multiple	workloads which share similar characteristics.			¢ ±	Add
	icy T 1 Snapshot and backup policies	T 2 Protection status	v 1 O Protected count	# 2 Backup destinution	
Protection group 2 Detection pol					

3. Select Add.

0	Ransomware protection Add protection group					🜒 Wörksoads 🔹	Protection ③ Review		
						Worklo Select workloads to add to	ads the protection group.		
		Protection	ngroup name Igroup inja				Select the type of workloads Workloads with snapshot ar SnapCenter or Backup J	to add to the protection group of backup policies managed by and recovery ① Forcurren	k Y wie geschection
		Workloads	(4) 2 selected Workload	: (Туре	₹ 2 Connector	‡ Importance	τ: © Prioqu	Q exposure 2 Protection status
			Oracle_9819		Oracle .	ave-connects	mui-east-1 Important	1/8	Protected
			Oracle_2115		Oracle	aws-connecto	r-us-east-1 Critical	n/a	🕡 Atmik
			MySQL,8294		MysQL	aws connects	or-us-east-1 Ortical	eva.	Protected
			MysiqL_8009		MysqL	ava-connecto	r-ut-east-1 Critical	n/a	💿 At nuk
		-							

- 4. Enter a name for the protection group.
- 5. Complete one of the following steps:
 - a. If you already have protection policies in place, select whether you want to group workloads based on whether they are managed by one of these:
 - BlueXP ransomware protection
 - SnapCenter or BlueXP backup and recovery
 - b. If you don't have protection policies already in place, the page displays the preconfigured ransomware protection strategies.
 - i. Choose one to protect your group and select Next.
 - ii. If the workload you chose has volumes on multiple working environments, select the backup destination for the multiple working environments so that they can be backed up to the cloud.
- 6. Select the workloads to add to the group.



To see more details on the workloads, scroll to the right.

7. Select Next.

Add protection group	G Works	oeds (Protection ③ Review	6			
			Protect				
	Select a detaction	policy to a	oply to all the workloads in the	protection gro	ugi.		
Detection policy (2) Selected rows (η			۵	SnapCenter and BlueXP backup and recovery		
Select Detection policy	\$ Primary detection	\$1	0 Block tunpicious file extensions	•	Existing snapshot and backup policies managed by SnapCenter and BlackP backup and recovery will not be modified by applying		
Ø 704-detection-1	Xee		Yes		a detection policy to the salected workloads.		
C rps-detection-2	708		No				
	ſ	Previo					

- 8. Select the policy that will govern the protection for this group.
- 9. Select Next.
- 10. Review the selections for the protection group.
- 11. Select Add.

Remove workloads from a group

You might later need to remove workloads from an existing group.

Steps

- 1. From the BlueXP ransomware protection menu, select **Protection**.
- 2. From the Protection page, select the **Protection groups** tab.
- 3. Select the group from which you want to remove one or more workloads.

Accercant y and one abla dumb			bx	p-dev-apps-group Protection group				
	-						Delete p	rotection group
	55 Workloads		L.	2	0,	notection		las prosection.
	File shares	88 0 Apple	atom	VM datastores	۲	Protection group		
	Workloads (4)					٩	±	A41
	Workload C	Туре — 🙂 🛛	Convector \$	Importance $\forall C \mid$	Privacy exposure	Protection status \$	Detection a	uh:
	vm_datastore_202_7359	VM datastore	onprem-connector-accou	Standard	nja	Protected	Active	Θ
	vm_datastore_203_2676	VM datastore	onprem-connector-accou	important	n/a	() At risk	tione	Θ
	fileshare_useast_01	File share	aws-connector-us-east-1	Standard	1/2	1 Atrick	None	Θ

- 4. From the selected protection group page, select the workload you want to remove from the group and select the **Actions** ••• option.
- 5. From the Actions menu, select Remove workload.
- 6. Confirm that you want to remove the workload and select **Remove**.

Delete the protection group

Deleting the protection group removes the group and its protection but doesn't remove the individual workloads.

Steps

- 1. From the BlueXP ransomware protection menu, select **Protection**.
- 2. From the Protection page, select the **Protection groups** tab.
- 3. Select the group from which you want to remove one or more workloads.

		b	kp-dev-apps-group Protection group				
						Delete p	otection group
SS Workloads				O P	rotection		dit profection
C 2 File shares	0 Appt	cations	2 vvir datastores	۲	rps-policy-atl Protection group		
Workloads (4)					a	±	All
Workloads (4) Workload C	Туро та	Connector	Importance TT 0 1	O Privacy exposure 2	Q. Protection status	± Detection s	ANI UR
Workloads (4) Workload C vm_datactore_200_7389	Type # 2	Convector \$	tesportance (V C) (Standard	0: Privacy exposure +	Q Protection status =	± Detection s	AH un
Workloads (4) Workload Workload m_datastore_202_7359 vm_datastore_203_2676	Type # 2 VM datastore VM datastore	Connector : onprem-connector-accou	Importance T C 1 Standard i Important i	O: Privacy exposure + n/a n/a	Q Protection status : O indexted () at risk	Detection s Active None	an O

- 4. From the selected protection group page, at the top right, select **Delete protection group**.
- 5. Confirm that you want to delete the group and select **Delete**.

Manage ransomware protection strategies

You can delete a ransomware strategy.

View workloads protected by a ransomware protection strategy

Before you delete a ransomware protection strategy, you might want to view which workloads are protected by that strategy.

You can view the workloads from the list of strategies or when you are editing a specific strategy.

Steps when viewing the list of strategies

- 1. From the BlueXP ransomware protection menu, select **Protection**.
- 2. From the Protection page, select Manage protection strategies.

The Ransomware protection strategies page displays a list of strategies.

tection # Ransomware protection strategies		Ransomware protection	n strategies				
Ransomware protection strategies (4)				q	± 🚺	Add	
Ransomware protection strategy	C Shapuhot policy	2 Backup policy	Detection policy	Protected workloads	:		
ips-strategy-critical	ontical-u-policy	critical-bu-policy	spe-policy-all	3		~	***
spi-strategy-important	important to policy	important-bu-policy	rps policy all	(80)		~	277
spi-strategy-standard	standard su-policy	standard-bu-policy	rps-policy-all	0		~	
70% strategy 4	standard-ss-policy-344	standard burpolicy-344	rps godey-all	0		~	•••
					tall policy Delete policy		

3. On the Ransomware protection strategies page, in the Protected workloads column, click the down arrow at the end of the row.

Delete a ransomware protection strategy

You can delete a protection strategy 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 protection strategies.
- 3. In the Manage strategies page, select the Actions --- option for the strategy you want to delete.
- 4. From the Actions menu, select **Delete policy**.

Scan for personally identifiable information with BlueXP classification

Within the BlueXP ransomware protection service, you can use BlueXP classification, a core component of the BlueXP family, to scan and classify your data on a file share workload. Classifying data helps you identify whether your data includes personally identifiable information (PII), which can increase security risks.



This process can impact workload importance to help you ensure that you have the appropriate protection.

Enable BlueXP classification

Before you use BlueXP classification within the BlueXP ransomware protection service, you need to enable BlueXP classification to scan your data.

By using the BlueXP classification UI as an alternate method, an administrator can enable BlueXP classification in BlueXP ransomware protection.

It might be helpful to review these BlueXP classification resources before you begin to use the service:

- Learn about BlueXP classification
- Categories of private data
- Investigate the data stored in your organization

Before you begin

Scanning for PII data in BlueXP ransomware protection is available to customers who deployed BlueXP classification. BlueXP classification is available as part of the BlueXP platform at no extra charge and can be deployed on-premises or in the customer cloud.

Steps

- 1. From the BlueXP ransomware protection menu, select Protection.
- 2. In the Protection page, locate a file share workload in the Workload column.

17 At risk (1) 4 (Last 7 days)				32 Gill Data at risk			ļ	Protected 0	0	14 GB Data protects	ьd				
Workloads			Protection groups												
Workfoads (24)												Q	<u>+</u>	Mar	nage protection strategies
Workload \$	Type	¥.0.]	Connec ¥ \$	import V \$	O Privacy expos V *	Profi	eti V 🗘	Protecti V 😂	Detecti = \$	Detecti V C	Snapsh.	7 2 (Backup	v e i	
Fileshare_useast_02	File si	hane	avs-connector	Critical	High	0	At risk	f/9	None	None	None		netapp-ba	ickup	Protect
Fileshare_unwest_01	Ŧie si	sare	awi-connector	Standard	Medium	0	At risk	n/a	None	None	None		netapp-b	ickup	Protect
Fileshare_useast_03	Files	hare	avs-connector	Standard	identify exposure	•	At risk	n/a	None	None	None		netapp-ba	ickup	Protect
Fileshare_uswest_02	File s	ane	ans-connector	Critical	identify exposure	Ø	Protected	n/a	Learning mode	rps-policy-all	Blue/Pr	ansom	netapp-b	kokup	(Edit protection)
Fileshare_useast_01	Tiq S	are	avs-connector	Standard	identify exposure	0	At mik	n/a	Norie	None	None		n/a		Protect
Gcpha_vol1_7496	File sP	sane	Isn-gcp-conne	Critical	identify exposure	0	At tisk	nva.	None	None	None		n/a		Protect
Vm_datastore_useast	VM fi	le share	aws-connector	Critical	n/a	0	Protected	n/a	Active	rps-policy-ait	Blue Pr	ansom	rwtapp-bi	ockup	(Edit prefection)

3. To enable BlueXP classification to scan your data for personally identifiable data, in the **Privacy exposure** column, select **Identify exposure**.

Result

Scanning might take several minutes depending on the amount of data. The Protection page shows that BlueXP classification is identifying files and gives you an indication of the number of files it is scanning.

When scanning is complete, the Privacy exposure column displays the exposure level as Low, Medium, or High.

Review the privacy exposure

After BlueXP classification scans for personally identifiable information (PII), you can look at the PII data risk.

PII data can have one of the following privacy exposure risk statuses.

- High: Greater than 70% of files have PII
- Medium: Greater than 30% and less than 70% of files have PII
- Low: Greater than 0 and less than 30% of files have PII

Steps

- 1. From the BlueXP ransomware protection menu, select **Protection**.
- 2. In the Protection page, locate the file share workload in the Workload column that shows a status in the Privacy exposure column.

5 At mak (1) 2 (Lent 7 days)	55 tia Deta at risk			3 Protected (2) 4 (Last 7 days)	23 Ti8 Data protected		
Workloads Protection	groups						
Vorkioads (6)					Q <u>+</u>	Aanage tansomware	protection strategies
Workload \$1	Type W 1	Location 🗧	() Importance	T : O Privacy exposure Preview	▼ \$ Protection status ♥ \$	Detection statu	Action
oracio-app-01	Oracle	host.name.com	Critical		① At risk	rita	Protect
fileshare_uswest_03_0192	File share	host.name.com	Critical	Medium	① At rock	rva	Protect
oracle-app-02	Oracle	bost.name.com	Important	nia	() At risk	n/a	Protect
Reshare_sowest_02_3223	File share	host,name.com	Critical	High	Protected	Active	(Edt protection)
fleshare_isswest_01_3847	File share	host.name.com	Standard	identity exposure	Protected	Error	(Edit printection)
fileshare_uswest_04_1231	File share	host.name.com	Critical	identify exposure	Protected	J Active	Edit printection

3. Select the workload link in the Workload column to see workload details.

		fileshare_uswest_02_	3223		
Critical Inportance ©	Protected Protection status	O Active Determine statue	① 1 Alerty View sierts		Restore needed Recovery View recovery
High (*) Privacy econum	Preview 🛞 investigate	O Protection	Edit protection	🕒 Fär shar	0
Total Pir 10.3k identifiers in Types of Pil identifiers	368 files	Protection group finance-apps View Ransonware rps-strategy-critico protection strategy		Location SnapCarriller server	scspa2536184001.rtp.openenglab.netap com 10.100.100.100
Credit cants	8.1k = 210 ties	(a) rps-detection-1 Detection policy	~	Storage	
Passwords	293 = 100 ties,	(i) fas-snapshots-xyz Snapshot policy	~	Volume Field	volume1 Value
Data subjects	O in Mill Size	() rps-backup-xyz	~	Field	Value Value

4. In the Workload details page, review the information in the Privacy exposure tile.

Impact of privacy exposure on workload importance

Privacy exposure changes can impact the workload importance.

When privacy exposure:	From this privacy exposure:	To this privacy exposure:	Then, workload importance does this:				
Decreases	High, Medium, or Low	Medium, Low, or None	Remains the same				
Increases	None	Low	Remains at Standard				
	Low	Medium	Changes from Standard to Important				
	Low or Medium	High	Changes from Standard or Important to Critical				

For more information

For details about BlueXP classification, refer to the following BlueXP classification topics:

- Learn about BlueXP classification
- Categories of private data
- Investigate the data stored in your organization

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.