

# Proteja workloads

BlueXP ransomware protection

NetApp December 20, 2024

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

# Índice

Proteja workloads	1
Proteja workloads com estratégias de ransomware	1
Procure informações pessoalmente identificáveis com a classificação BlueXP	5

# Proteja workloads

# Proteja workloads com estratégias de ransomware

Você pode proteger workloads contra ataques de ransomware executando as seguintes ações usando a proteção contra ransomware do BlueXP.

- Habilite a proteção consistente com o workload, que funciona com o software SnapCenter ou o plug-in SnapCenter para VMware vSphere.
- Crie ou gerencie estratégias de proteção contra ransomware, que incluem políticas criadas para snapshots, backups e proteção contra ransomware (conhecidas como *políticas de detecção*).
- Importe uma estratégia e ajuste-a.
- Compartilhe arquivos de grupo para facilitar a proteção de workloads em vez de protegê-los individualmente.
- Exclua uma estratégia de proteção contra ransomware.

Que serviços são utilizados na proteção? Os seguintes serviços podem ser usados para gerenciar políticas de proteção. As informações de proteção contra esses serviços aparecem na proteção contra ransomware do BlueXP :

- Backup e recuperação do BlueXP para compartilhamentos de arquivos e compartilhamentos de arquivos VM
- SnapCenter para VMware para armazenamentos de dados de VM
- SnapCenter para Oracle e MySQL

## Políticas de proteção

Você pode achar útil analisar informações sobre as políticas de proteção que você pode alterar e quais tipos de políticas estão em uma estratégia de proteção.

#### Que políticas de proteção você pode mudar?

É possível alterar as políticas de proteção com base na proteção de workload que você tem:

- Cargas de trabalho não protegidas pelos aplicativos NetApp: Essas cargas de trabalho não são gerenciadas pelo SnapCenter, pelo plug-in SnapCenter para VMware vSphere ou pelo backup e recuperação do BlueXP. Essas cargas de trabalho podem ter snapshots feitos como parte da ONTAP ou de outros produtos. Se a proteção do ONTAP FPolicy estiver em vigor, você poderá alterar a proteção do FPolicy usando o ONTAP.
- Cargas de trabalho com proteção existente pelos aplicativos NetApp: Essas cargas de trabalho têm políticas de backup ou snapshot gerenciadas pelo SnapCenter, SnapCenter para VMware vSphere ou backup e recuperação do BlueXP.
  - Se as políticas de snapshot ou backup estiverem sendo gerenciadas pelo SnapCenter, SnapCenter para VMware ou backup e recuperação do BlueXP, elas continuarão sendo gerenciadas por esses aplicativos. Ao usar a proteção contra ransomware do BlueXP, você também aplica uma política de detecção de ransomware a esses workloads.
  - Se uma política de detecção de ransomware estiver sendo gerenciada pela Autonomous ransomware Protection (ARP) e pela FPolicy no ONTAP, essas cargas de trabalho serão protegidas e continuarão

sendo gerenciadas pelo ARP e pelo FPolicy.

#### Quais políticas são necessárias em uma estratégia de proteção contra ransomware?

As seguintes políticas são necessárias na estratégia de proteção contra ransomware:

- · Política de detecção de ransomware
- · Política do Snapshot

Não é necessária uma política de backup na estratégia de proteção de ransomware da BlueXP .

#### Ver a proteção contra ransomware em um workload

Uma das primeiras etapas para proteger cargas de trabalho é visualizar suas cargas de trabalho atuais e seu status de proteção. Você pode ver os seguintes tipos de workloads:

- · Workloads de aplicação
- Workloads de VM
- · Workloads de compartilhamento de arquivos

#### Passos

- 1. Na navegação à esquerda do BlueXP, selecione proteção > proteção contra ransomware.
- 2. Execute um dos seguintes procedimentos:
  - No painel proteção de dados no Painel, selecione Exibir tudo.
  - No menu, selecione proteção.

16 4 (Latt 7 c	e deysti		32 Gill Data at Hak			Sectored	d 0 raye	14 Gi8 Data protecte	c.		
Workloads		Frotection grou	ga .								
Vorkloads (24)									Q	1 Manage p	otection strategies
Workload 0	Type = 4	Connector \$	Importance # 0	Ø maye	Protection., 7 2	Protection., 7 \$	Detection V 4	Detection マロー	Snapshot	Backup desti \$	
Wei, datartore, useas	VM Neshare	avi-connector-us	Critical	n/a	D Protected	ri(b	Adle	rps-policy-all	Build randomia	rwtapp-bickup-vs	(1dt protection
Ve_datactore_uneer	VM Neishare	avi-contector-us	Criscal	10	Protected	P/9	Learning mode	rps-policy-all	Bluet/Francomwa	NHopp-bickup-vs	(Tat patecion
Vm, datastore, useen	vM file share	avs-connector-us	Standard	n/a	🔘 Atrok	0.9	None	Norw	None	Netiep-backup-vs	Protect
Vin, datastore, usee	VM file share	avs-connector-us	Sandard	n/a	🕐 atrok	0,9	None	Nonw	None	NHIEP-bickup-vs	Protect
Vin_datastore_useus	VM file share	avs-connector-us	thendard	nia -	🕡 atrisk	e, a	None	None	Nore	whipp-backsp-ys-	Protect
Vm, datastore, 201, 3	VM Ne share	orprem-connecto	Standard	eva	🕑 atriik	11.0	None	None	None	retapp-backup-vs	Protect
Oracle_6521	Orade	avi-contector-us	Orthoal	10	Protected	1.9	Actor	rps-policy-all	busk? rancomea	netapp-backup-vs	(Edt protection

3. Nesta página, você pode visualizar e alterar os detalhes de proteção para a carga de trabalho.



Para workloads que já têm uma política de proteção com o serviço de backup e recuperação SnapCenter ou BlueXP, não é possível editar a proteção. Para essas cargas de trabalho, o BlueXP ransomware habilita a proteção autônoma contra ransomware e/ou a proteção FPolicy, se eles já estiverem ativados em outros serviços. Saiba mais sobre "Proteção autônoma contra ransomware", "Backup e recuperação do BlueXP" e "Política de ONTAP".

#### Detalhes de proteção na página proteção

A página proteção mostra as seguintes informações sobre a proteção da carga de trabalho:

**Status de proteção**: Uma carga de trabalho pode mostrar um dos seguintes status de proteção para indicar se uma política é aplicada ou não:

- Protegido: É aplicada uma política. O ARP é ativado em todos os volumes relacionados à carga de trabalho.
- Em risco: Nenhuma política é aplicada. Se uma carga de trabalho não tiver uma política de deteção primária ativada, ela estará "em risco" mesmo que tenha uma política de snapshot e backup ativada.
- Em andamento: Uma política está sendo aplicada, mas ainda não foi concluída.
- Falhou: Uma política é aplicada, mas não está funcionando.

Status da deteção: Uma carga de trabalho pode ter um dos seguintes status de deteção de ransomware:

- **Aprendizagem**: Uma política de deteção de ransomware foi atribuída recentemente à carga de trabalho e o serviço está verificando as cargas de trabalho.
- Ativo: É atribuída uma política de proteção para detecção de ransomware.
- Não definido: Uma política de proteção de deteção de ransomware não é atribuída.
- Erro: Uma política de deteção de ransomware foi atribuída, mas o serviço encontrou um erro.



Quando a proteção é ativada na proteção contra ransomware do BlueXP, a detecção e a geração de relatórios começam após as alterações de status da política de detecção de ransomware do modo de aprendizado para o modo ativo.

**Política de deteção**: O nome da política de deteção de ransomware aparece, se tiver sido atribuído. Se a política de deteção não tiver sido atribuída, é apresentado "N/A".

**Snapshot e políticas de backup**: Esta coluna mostra as políticas de snapshot e backup aplicadas à carga de trabalho e ao produto ou serviço que está gerenciando essas políticas.

- Gerenciado por SnapCenter
- · Gerenciado pelo plug-in SnapCenter para VMware vSphere
- · Gerenciado por backup e recuperação do BlueXP
- Nome da política de proteção de ransomware que governa snapshots e backups
- Nenhum

#### Importância da carga de trabalho

A proteção contra ransomware do BlueXP atribui uma importância ou prioridade a cada workload durante a detecção com base em uma análise de cada workload. A importância da carga de trabalho é determinada pelas seguintes frequências de instantâneos:

- Crítico: Cópias snapshot feitas mais de 1 MB por hora (programação de proteção altamente agressiva)
- Importante: Cópias snapshot feitas com menos de 1 MB por hora, mas superiores a 1 MB por dia
- Standard: Cópias snapshot feitas mais de 1 por dia

#### Políticas de deteção predefinidas

Você pode escolher uma das seguintes políticas predefinidas de proteção contra ransomware da BlueXP , que estão alinhadas com a importância do workload:

Nível de política	Snapshot	Frequência	Retenção (dias)	nº de cópias snapshot	Número máximo total de cópias snapshot
Política de carga	Quarto por hora	A cada 15 min	3	288	309
de trabalho	Diariamente	A cada 1 dias	14	14	309
Critica	Semanalmente	A cada 1 semanas	35	5	309
	Mensalmente	A cada 30 dias	60	2	309
Important e política	Quarto por hora	A cada 30 minutos	3	144	165
de carga de trabalho	Diariamente	A cada 1 dias	14	14	165
trapamo	Semanalmente	A cada 1 semanas	35	5	165
	Mensalmente	A cada 30 dias	60	2	165
Política de carga	Quarto por hora	A cada 30 min	3	72	93
de trabalho	Diariamente	A cada 1 dias	14	14	93
paurao	Semanalmente	A cada 1 semanas	35	5	93
	Mensalmente	A cada 30 dias	60	2	93

# Habilite a proteção consistente com aplicações ou VM com o SnapCenter

Ativar a proteção consistente com aplicações ou VM ajuda você a proteger seus workloads de aplicações ou VMs de maneira consistente, alcançando um estado inativo e consistente para evitar a perda de dados em potencial mais tarde, caso seja necessária recuperação.

Esse processo inicia o Registro do servidor de software SnapCenter para aplicativos ou do plug-in SnapCenter para VMware vSphere para VMs usando o backup e a recuperação do BlueXP.

Depois de habilitar a proteção consistente com o workload, você pode gerenciar estratégias de proteção na proteção contra ransomware do BlueXP . A estratégia de proteção inclui políticas de snapshot e backup gerenciadas em outros lugares, além de uma política de detecção de ransomware gerenciada na proteção contra ransomware da BlueXP .

Para saber mais sobre como Registrar o SnapCenter ou o plug-in do SnapCenter para VMware vSphere usando o backup e a recuperação do BlueXP, consulte as seguintes informações:

- "Registre o software do servidor SnapCenter"
- "Registre o plug-in do SnapCenter no VMware vSphere"

#### Passos

- 1. No menu de proteção contra ransomware do BlueXP, selecione Painel.
- 2. No painel recomendações, localize uma das seguintes recomendações e selecione Revisão e correção:
  - Registre o servidor SnapCenter disponível com o BlueXP
  - · Registre o plug-in do SnapCenter disponível para VMware vSphere (SCV) com o BlueXP
- 3. Siga as informações para Registrar o plug-in do SnapCenter ou do SnapCenter para o host VMware vSphere usando o backup e a recuperação do BlueXP .
- 4. Voltar à proteção contra ransomware BlueXP.
- 5. Contra a proteção contra ransomware do BlueXP, acesse o Dashboard e inicie o processo de descoberta novamente.
- 6. Na proteção contra ransomware BlueXP, selecione **proteção** para visualizar a página proteção.
- 7. Analise os detalhes na coluna políticas de snapshot e backup na página proteção para ver se as políticas são gerenciadas em outro lugar.

## Adicione uma estratégia de proteção contra ransomware

Você pode adicionar uma estratégia de proteção contra ransomware aos workloads. A maneira como você faz isso depende se as políticas de snapshot e backup já existem:

- \* Crie uma estratégia de proteção contra ransomware se você não tiver políticas de snapshot ou backup\*. Se as políticas de snapshot ou backup não existirem na carga de trabalho, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas na proteção contra ransomware do BlueXP :
  - · Política do Snapshot
  - · Política de backup
  - · Política de detecção de ransomware
- Crie uma política de deteção para cargas de trabalho que já tenham políticas de snapshot e backup, que são gerenciadas em outros produtos ou serviços da NetApp. A política de deteção não alterará as políticas gerenciadas em outros produtos.

# Criar uma estratégia de proteção contra ransomware (se você não tiver políticas de snapshot ou backup)

Se as políticas de snapshot ou backup não existirem na carga de trabalho, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas na proteção contra ransomware do BlueXP :

- · Política do Snapshot
- · Política de backup
- Política de detecção de ransomware

#### Etapas para criar uma estratégia de proteção contra ransomware

1. No menu proteção contra ransomware BlueXP, selecione proteção.

16 At no. 0 4 (Latt 7 c	i Saysti		32 Gill Data at Hilk			Rectaction	d Q	14 G-8 Data protecte	¢		
Workloads		Protection grou	pa								
Workloads (24)									Q	± Manage p	otection strategies
workload 0	Type = 0	Connector \$	Importance = 0	Ø maye_ =	Protection 7 2	Protection T 0	Detection V \$	Detection * 0	Stopshot = 0	Backup desti 9	
Ve_datastore_useas	VM Ne share	avs-connector-us	Critical	Ně	Protected	n/0	Adlet	rps-policy-all	Blacch rancomva	rwtapp-bickup-vs	(1dt protection)
Ve_datactore_unive	SM Ne share	ava-connector-us	Criscal	10	Protected	n/a	Learning mode	rps-policy-all	Bluetth rancomwa	(Hopp-bickup-vs.,	(Int puterios)
Vm_datastore_usee	vM file share	avs-connector-ut	Standard	n/a	🕑 azırşk	0.9	None	Norw	None	Netipp-backup-vs	Protect
Vm, datastore, usee	VM Ne share	avs-conrector-us	Standard	n/#	🕑 az tişk	0.9	None	None	None	NHIEP-bickup-vs	Protect
Vm_datastore_useas	VM file share	ava-connector-us	Mandard	nia	🕡 42.65k	et/a	None	None	Nore	Helep-backsprys	Protect
Vm, datastore, 201, 3	vM Ne share	onprem-connecto	Standard	N/A	🕑 atmk	1/3	None	None	None	retapp-backup-us	Protect
Oracle_6521	Oracle	avs-contector-us	Critical	10	Protected	e.o	Active	rps-policy-all	Buelof rancomea	netapp-backup-us	(fill purection)

2. Na página proteção, selecione Gerenciar estratégias de proteção.

Protection 3: Ransonware protection strategies							
		Ransomware protectio	on strategies				
Ransomware protection strategies (3)				Q	±	A05	
Ranserware protection strategy	<ul> <li>Snapshot policy</li> </ul>	C Backup policy	C Delection policy	Protected workloads		en a	
rpi-mategy-oritical	ortical-si-policy	official-bu-policy	rpt-policy-all	1		$\sim$	
rpi-strategy-important	important-us-policy	important-bu-policy	rps-policy-all	*5		$\sim$	1997)
rpustrateg/standard	standard-sirpolicy	standard bu policy	ips-policy-all	0.0		$\sim$	

3. Na página estratégias de proteção contra ransomware, selecione Adicionar.

Protection > Manage protection strategies > Add ransomware	e protection strategy		Add ransomware j	protection strategy	
	Ransomware protection strategy nar	ne.		Copy from existing ransomware protection strategy No policy selected	다. Select
	Detection policy	rps-policy-primary			~
	Snapshot policy	important-ss-policy			~
	Backup policy	None			~
			Cancel	Add	

4. Introduza um novo nome de estratégia ou introduza um nome existente para o copiar. Se você inserir um nome existente, escolha qual copiar e selecione **Copiar**.



Se você optar por copiar e modificar uma estratégia existente, o serviço anexa "\_copy" ao nome original. Você deve alterar o nome e pelo menos uma configuração para torná-lo único.

- 5. Para cada item, selecione a seta para baixo.
  - Política de deteção:
    - Política: Escolha uma das políticas de deteção pré-projetadas.
    - Detecção primária: Habilite a detecção de ransomware para que o serviço detete possíveis ataques de ransomware.
    - \* Bloquear extensões de arquivo\*: Ative-o para que o bloco de serviço tenha extensões de arquivo suspeitas conhecidas. O serviço realiza cópias snapshot automatizadas quando a detecção primária está ativada.

Se você quiser alterar as extensões de arquivo bloqueadas, edite-as no System Manager.

- Política de instantâneos:
  - Nome da base de política de instantâneo: Selecione uma política ou selecione criar e insira um nome para a política de instantâneo.
  - Bloqueio instantâneo: Ative-o para bloquear as cópias snapshot no armazenamento primário para que elas não possam ser modificadas ou excluídas por um determinado período de tempo, mesmo que um ataque de ransomware gerencie seu caminho para o destino do armazenamento de backup. Isso também é chamado de *armazenamento imutável*. Isso permite um tempo de restauração mais rápido.

Quando um instantâneo é bloqueado, o tempo de expiração do volume é definido para o tempo de expiração da cópia instantânea.

O bloqueio de cópias snapshot está disponível com o ONTAP 9.12,1 e posterior. Para saber mais sobre o SnapLock, "SnapLock em ONTAP" consulte .

- Horários de instantâneos: Escolha as opções de agendamento, o número de cópias instantâneas a serem mantidas e selecione para ativar a programação.
- Política de backup:
  - Nome de base da política de backup: Insira um nome novo ou escolha um nome existente.
  - Backup programações: Escolha as opções de agendamento para armazenamento secundário e ative a programação.



Para ativar o bloqueio de cópias de segurança no armazenamento secundário, configure os destinos de cópia de segurança utilizando a opção **Definições**. Para obter detalhes, "Configure as definições"consulte .

#### 6. Selecione Adicionar.

#### Adicione uma política de detecção a workloads que já tenham políticas de snapshot e backup

Com a proteção contra ransomware do BlueXP, você pode atribuir uma política de detecção de ransomware a workloads que já tenham políticas de snapshot e backup, gerenciados em outros produtos ou serviços da NetApp. A política de deteção não alterará as políticas gerenciadas em outros produtos.

Outros serviços, como backup e recuperação do BlueXP e SnapCenter, usam os seguintes tipos de políticas para governar cargas de trabalho:

- · Políticas que regem snapshots
- · Políticas que regem a replicação para storage secundário
- Políticas que regem os backups para o storage de objetos

#### Passos

1. No menu proteção contra ransomware BlueXP , selecione **proteção**.

16 At init, 0 At last 70	i Aeyi)		32 die Dersist Hek			Sectories	a ()	14 dia Data protecte	¢		
Workloads		Protection grou	pa								
Vorkloads (24)									٩	± Manage pr	otection strategies
workload 0	Type = 1	Connector \$	Importance # 0	Ø maye. :	Protection V 2	Protection V 0	Detection V 0	Detection ¥ 0	Stopshot	Backup desti	
Vro_datantove_useas	VM Neshare	avs-connector-us	critical	rvie -	Protected	6/7	Adlet	rps-policy-all	Bluetti ransonivik	retapp-backup-is	(1dt proverties
Ve_datastore_unsee	SM Neshare	avs-connector-us	Critical	6.06	Divolacted	1/3	Learning mode	rps-policy-all	Blast/Francomwa	retapp-backup-vs	(Tat polacion
Vm, datastore, useen	vM file share	avs-connector-us	Standard	n/#	🕑 at rijk	0.9	None	None	None	netep-backup-st	Protect
lim, datastore, usee	VM file share	avs-conrector-us	Standard	n/a	🕑 az ingk	0.9	None	Norw	None	netep-bickup-vs	Protect
Vis_datastore,useas	VM file share	avs-connector-us	thandard	nia	🕡 42.65k	n/a	None	None	None	whee-backerys	Protect
Vm, datastore, 201, 3	vM Ne share	onprem-connecto	Standard	n/a	🕢 at mik	1/3	None	None	None	netapp-backup-vs	Protect
Oracle_6521	Oracle	avs-comedor-us	Critical	10	Profected	0.9	Active	rps-policy-all	Buex7 sanconwa	netapp-backup-us	(Edt protection

2. Na página proteção, selecione uma carga de trabalho e selecione proteger.

A página proteger mostra as políticas gerenciadas pelo software SnapCenter, pelo SnapCenter para VMware vSphere e pelo backup e recuperação do BlueXP.

O exemplo a seguir mostra as políticas gerenciadas pelo SnapCenter:

			Protect			
			Select a detection policy to apply to t	he workload C	Dracle_9819.	
De	tection policies (2	)   1 selected		Q	Policies managed by SnapCenter	
	Name	Primary detection	Block suspicious file extensions	÷	These policies managed by SnapCenter will not be modified by	î
0	rps-policy-1	Yes	Yes		applying a detection policy to this workload.	- 1
0	rps-policy-2	Yes	No		(a) ss-policy-daily1 Snapshot policy	~
					ss-policy-weekly1 Snapshot policy	~
					ss-policy-weekly2 Snapshot policy	~
					ss-policy-monthly1 Snapshot policy	~ *
			Cancel	rotect		

O exemplo a seguir mostra as políticas gerenciadas pelo backup e recuperação do BlueXP :

			Protect	the workload M	NCO1 2000
			select a detection policy to apply to	ine workload im	J24L_9009.
Dete	ction policies (2	)   1 selected		Q	Delicies 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 ~
					standart-backup-policy Backup policy
			Cancel	Protect	

3. Para ver detalhes das políticas gerenciadas em outro lugar, clique na seta para baixo.

- Para aplicar uma política de deteção além das políticas de instantâneos e backup gerenciadas em outro lugar, selecione a política detecção.
- 5. Selecione Protect.
- 6. Na página proteção, revise a coluna Política de detecção para ver a diretiva detecção atribuída. Além disso, a coluna políticas de snapshot e backup mostra o nome do produto ou serviço que gerencia as políticas.

#### Atribua uma política diferente

Você pode atribuir uma política de proteção diferente substituindo a atual.

#### Passos

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, na linha carga de trabalho, selecione Editar proteção.
- 3. Na página políticas, clique na seta para baixo da política que você deseja atribuir para revisar os detalhes.
- 4. Selecione a política que pretende atribuir.
- 5. Selecione **Protect** para concluir a alteração.

## Compartilhe arquivos de grupo para facilitar a proteção

Agrupar compartilhamentos de arquivos facilita a proteção de seu data Estate. O serviço pode proteger todos os volumes em um grupo ao mesmo tempo em vez de proteger cada volume separadamente.

#### Passos

1. No menu proteção contra ransomware BlueXP, selecione proteção.

16 Atria @ Atria @	layst		32 c.e Data at Hilk			7 Sector 1 Gast 7	a (i) aya	14 G8 Data protecte	ŕ.		
Workloads		Protection grou	pa								
Workloads (24)									٩	🛓 🛛 Managa pr	atection strategies
Workload 0	type = 0	Connector \$	Importance # 0	Ø maye_ 0	Protection 7 2	Protection V \$	Detection V 2	Detection * \$	Snapshot = 5	Backup desti 🤤	
Ve_datactore_useas	VM Ne share	avs-connector-us	critical	rvie .	Protected	6/7	Active	rps-policy-all	Bluetti ransonivia	rwtapp-bickup-us	(Idt protection)
Ve_datadore.onem	shi file share	ava-connector-us	critical	6,0	Detroted	P/9	Learning mode	rps-policy-all	Bluetth ransomwa	wtopp-backup-vs	(Int protection)
Vm, datastore, useen	vM file share	avs-connector-us	Standard	n/a	🕑 at rijk	n.9	None	Norw	None	netipp-backup-vs	Protect
Vm, datastore, useen	VM file share	avis-connector-us	Standard	n/a	🕑 az rok	0.9	None	None	None	hetep-bickup-vs	Protect
Vm_datastore_useas	VM file share	ava-connector-us	thandard	n/a	🛈 42 tisk	e(3)	None	None	Nore	Hetep-backsp-vs-	Protect
Vm, datastore, 201, 3	vM Ne share	onprem-connecto	Standard	n/a	🕑 senik	1/3	None	None	None	retapp-backup-us	Protect
Oracle_6521	Oracle	avs-contector-us	Critical	na.	Protected	0.9	Active	rps-policy-all	Buex7 rancomea	retapp-backup-us	(Edit protection)

2. Na página proteção, selecione a guia grupos de proteção.

0 16 M mak (0) 4 (Last 7 Calut)	32 G Ceta at	5 nik		Protected @ 1 Gast 7 days		14 Gits Deta protected			
Workloads	Protection groups	<u>l</u>							
otection groups (1) Id proups to manage protection across m	utiple workloads which share similar	dunidaridics.					٩	Ŧ	Add
Protection group 2   Detect	on policy T 2	Snapshot and backup policies	(**)	Protection status	vs i 0 mi	tected count	π ≎   Backup d	etinution	
hisp-dev apprigroup is po	icy-#ll	SnapCenter		Protected	:428		avo st-de	st-1, avo-s3-dect-2	

#### 3. Selecione Adicionar.

<ul> <li>Ransomware protection</li> <li>Add protection group</li> </ul>			Workoods ② Protection	3 Review	
		2	Workloads Select workloads to add to the protection	s graup.	
	Protection group name		Select the ty Workbads v SnapCi	pe of workloads to add to the protect with snapshot and backup policies in inter or Backup and recovery	tion group. nanaged by Ramamware profestion
	Workloads (4)   2 selected	‡ ∣ Type	▼ \$   Connector \$	Importance v =   0	Q. ) Prinacy exposure 💈   Protection status
	Orack, 9819	Oracle.	ave connector-us-east-1	Important in	/a 🕞 Protected
	Oracle,2115	Oracle	aws-connector-us-east-1	Critical no	/a 🕡 Atmik
	MySQL,8294	MySQL	ave connector-us-east-1	Critical ny	/a 🕞 Protected
	MySQL_8009	WySQL	ave-connector-us-east-1	Critical n	ra 🕕 Atmik
			P Next		

- 4. Introduza um nome para o grupo de proteçãoão.
- 5. Execute um dos seguintes passos:
  - a. Se você já tiver políticas de proteção em vigor, selecione se deseja agrupar cargas de trabalho com base no gerenciamento dessas mesmas:
    - Proteção contra ransomware da BlueXP
    - Backup e recuperação do SnapCenter ou BlueXP
  - b. Se você não tiver políticas de proteção já implementadas, a página exibirá as estratégias de proteção de ransomware pré-configuradas.
    - i. Escolha um para proteger o seu grupo e selecione **seguinte**.
    - ii. Se o workload escolhido tiver volumes em vários ambientes de trabalho, selecione o destino do backup para os vários ambientes de trabalho para que eles possam ser copiados para a nuvem.
- 6. Selecione as cargas de trabalho a serem adicionadas ao grupo.



Para ver mais detalhes sobre as cargas de trabalho, role para a direita.

#### 7. Selecione seguinte.

					Protect		
			Select a detectio	n policy to ap	ply to all the workloads in the	e protection gro	up.
Detection p	oöcy (2)   Selected rows (1)					a	SnapCenter and BlueXP backup and recovery
Select	Detection policy	۵)	Primary detection	\$1	Block suspicious file     extensions	•	Existing snapshot and backup policies managed by SnapCenter and BlackP backup and recovery will not be read-fed by applying
0	ros-detection-1		Xee		Yes		a detection policy to the salected workbarts.
0	rps-detection-2		788		No		

- 8. Selecione a política que governará a proteção para este grupo.
- 9. Selecione seguinte.
- 10. Reveja as seleções para o grupo de proteçãoão.
- 11. Selecione Adicionar.

#### Remover workloads de um grupo

Mais tarde, talvez seja necessário remover cargas de trabalho de um grupo existente.

- 1. No menu proteção contra ransomware BlueXP , selecione proteção.
- 2. Na página proteção, selecione a guia grupos de proteção.
- 3. Selecione o grupo do qual você deseja remover uma ou mais cargas de trabalho.

		bo	p-dev-apps-group Protection group				
						Delete p	rotection group
88 Workloads				0 1	rotection		Left protection
E 2 File stares	0 400	cations	2 vvi datastores	۲	rps-policy-all Protection group		
Workloads (4)					Q	Ŧ	All
Workloads (4) Workload C	Type Tr 2	Convector 2:	teportance	): Privacy exposure 💈	Q. Protection status	±	Add Add
Workloads (4) Workload * vm_datattore_202_7359	Type T C	Connector \$   onprem-connector-accou-	Importance T C   () Randard n	) Privacy imposure 💲   ce	Q Protection status	± Detections	
Workloads (4) Workload C wm_datattore_202,7359 wm_datattore_203,2676	Type     T C       VM datastore       VM datastore	Connector \$   onprem-connector-accou	Importance T C   0 Standard n Important n	8 Privacy exponent \$   ca	Q Protection status Protected T Arrisk	± Detection s Active None	ntati

- 4. Na página do grupo de proteção selecionado, selecione a carga de trabalho que deseja remover do grupo e selecione a opção \*ações\*....
- 5. No menu ações, selecione Remover carga de trabalho.
- 6. Confirme se deseja remover a carga de trabalho e selecione **Remover**.

#### Elimine o grupo de proteçãoão

A exclusão do grupo de proteção remove o grupo e sua proteção, mas não remove as cargas de trabalho individuais.

#### Passos

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, selecione a guia grupos de proteção.
- 3. Selecione o grupo do qual você deseja remover uma ou mais cargas de trabalho.

		bo	kp-dev-apps-group Protection group			_	
						Delete pr	otection group
SS Workloads				0 1	rotection		Idit protection
2 File shares	BB 0	zion	2 vivit datastories	۲	rps policy all Protection group		
Workloads (4)					a	)±	-444
Workloads (4) Workload C (	Type T C	Convector +	Importance T C   (	Privacy exposure	Q. Protection status	± Detection s	All
Workloads (4) Workload C ( vm_datastore_202_7359	Type T C   VM datastore	Convector \$   onprem-connector-accou-	Importance T C   ( Dandard r	B: Privacy exposure \$   1/8	Q Protection status	± Detection s Active	-461 tati
Workloads (4) Workload C ( wm_datastore_202_7359 wm_datastore_203_3676	Type         T 2             VM datastore         VM datastore	Connector ¢   ongrem-connector-accoul	Importance v C   ( Standard r Important r	B: Privacy exposure ÷   1/4 1/4	Q Protection status Protected () at risk	± Detection a Active Trone	AH 01

4. Na página do grupo de proteção selecionado, no canto superior direito, selecione Excluir grupo de

#### proteção.

5. Confirme se deseja excluir o grupo e selecione **Excluir**.

## Gerenciar estratégias de proteção contra ransomware

Você pode excluir uma estratégia de ransomware.

#### Visualize workloads protegidos por uma estratégia de proteção de ransomware

Antes de excluir uma estratégia de proteção contra ransomware, talvez você queira ver quais cargas de trabalho estão protegidas por essa estratégia.

Você pode visualizar as cargas de trabalho a partir da lista de estratégias ou quando estiver editando uma estratégia específica.

#### Etapas ao visualizar a lista de estratégias

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, selecione Gerenciar estratégias de proteção.

A página estratégias de proteção contra ransomware exibe uma lista de estratégias.

Protection #	Ranuomware protection strategies												
					Ransomware protectio	in strateg	ies						
	Ransomware protection strategies (4)								Q	Ŧ		Add	- Ü
	Rationmum protection strategy	•	Stapuhot policy	2	Backup policy		Detection policy	•	Protected workloads		:	ж	
	spi-strategy-critical		critical-sz-policy		critical-bu-policy		spe-policy-all		3			~	
	spi-strategy-important.		important-to-policy		important-du-policy		rps-policy-all		( <b>a</b> ))			~	277
	spi-strategy-standard		standard-to-policy		standard-bu-policy		rps-policy-all		0			~	247
	#PS strategy 4		standard-so-policy-344		standard by policy-344		rps-policy-all		<u></u>			~	***
										Defete	kay policy		

 Na página estratégias de proteção contra ransomware, na coluna cargas de trabalho protegidas, clique na seta para baixo no final da linha.

#### Exclua uma estratégia de proteção contra ransomware

Você pode excluir uma estratégia de proteção que não esteja associada atualmente a nenhuma carga de trabalho.

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, selecione Gerenciar estratégias de proteção.
- 3. Na página Gerenciar estratégias, selecione a opção ações ---para a estratégia que deseja excluir.
- 4. No menu ações, selecione Excluir política.

# Procure informações pessoalmente identificáveis com a classificação BlueXP

No serviço de proteção contra ransomware da BlueXP, você pode usar a classificação do BlueXP, um componente essencial da família BlueXP, para verificar e classificar seus dados em um workload de compartilhamento de arquivos. Classificar dados ajuda a identificar se seus dados incluem informações de identificação pessoal (PII), o que pode aumentar os riscos de segurança.



Esse processo pode afetar a importância da carga de trabalho para garantir que você tenha a proteção adequada.

# Ativar a classificação BlueXP

Antes de usar a classificação do BlueXP no serviço de proteção contra ransomware da BlueXP, você precisa habilitar a classificação do BlueXP para Escanear seus dados.

Usando a IU de classificação do BlueXP como um método alternativo, um administrador pode ativar a classificação do BlueXP na proteção contra ransomware do BlueXP.

Pode ser útil rever estes recursos de classificação do BlueXP antes de começar a utilizar o serviço:

- "Saiba mais sobre a classificação BlueXP"
- "Categorias de dados privados"
- "Investigue os dados armazenados em sua organização"

#### Antes de começar

A verificação de dados PII na proteção contra ransomware do BlueXP está disponível para clientes que implantaram a classificação BlueXP. A classificação do BlueXP está disponível como parte da plataforma BlueXP sem custo adicional e pode ser implantada no local ou na nuvem do cliente.

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, localize uma carga de trabalho de compartilhamento de arquivos na coluna carga de trabalho.

17 At trisk (1) 4 til ant 7 deys)	4			32 GiB Data at rick			0	Protected @	0	14 Git Data protecta	d				
Workloads			Protection groups												
Workloads (24)												۹.	E [	Mana	ige protection strategies
Workload \$	Туре	ra I	Connec_ = C	import_ v t )	O Privacy expos V +	Prote	ecti	Protecti V 🗣 🗎	Detecti = =	Detecti ¥ ¢ ]	Snapsh *	t Bac	kup 1	• • 1	
Fileshare_useast_02	File shar	9	avs-connector	Critical	High	0	At nisk	1/3	None	None	None	net	app-baci	oup	Protect
Fileshare_unwest_01	Ŧile shar	e .	avs-connector	Standard	Medium	0	At risk	n/a	None	None	None	ret	ipp-baci	sup	Protect
Fileshare_useast_03	File star	e	avs-connector	Standard	identify exposure	•	At rok	n/a	None	None	None	net	kpp-back	up	Protect
Filmhare_unwest_02	File star		ans-connector	Critical	identify exposure	0	Protected	6/8	Learning mode	rps-policy-all	BlueXP ranson	s. net	ipp-back	wp	(Edit protection)
Fileshare_useast_01	File shar	w	avs-connector	Standard	identify exposure	0	At mik	n/a	Norie	None	None	r/a			Protect
Gcphu_volt_7496	File shar	æ	Isn-gcp-conne	Critical	identify exposure	0	At tisk	n/a	None	None	None	r/a			Protect
Vm_datastore_useast	VM file	share	aws-connector	Critical	n/a	0	Protected	n/a	Active	sps-policy-ail	BlueXP ransor	n	ipp-back	o.p	(Edit pretection)

3. Para ativar a classificação BlueXP para verificar os seus dados para dados pessoais identificáveis, na coluna **exposição à privacidade**, selecione **Identify exposure**.

#### Resultado

A digitalização pode demorar vários minutos, dependendo da quantidade de dados. A página proteção mostra que a classificação BlueXP está identificando arquivos e fornece uma indicação do número de arquivos que está digitalizando.

Quando a digitalização estiver concluída, a coluna exposição à privacidade exibe o nível de exposição como baixo, Médio ou Alto.

## Reveja a exposição à privacidade

Após a classificação do BlueXP verificar informações de identificação pessoal (PII), você pode olhar para o risco de dados PII.

Os dados PII podem ter um dos seguintes Estados de risco de exposição à privacidade.

- High: Mais de 70% dos arquivos têm PII
- Médio: Maior que 30% e menos de 70% dos arquivos têm PII
- \* Baixo \*: Maior que 0 e menos de 30% dos arquivos têm PII

- 1. No menu proteção contra ransomware BlueXP, selecione proteção.
- 2. Na página proteção, localize a carga de trabalho de compartilhamento de arquivos na coluna carga de trabalho que mostra um status na coluna exposição à privacidade.

5 Mit risk (©) 2 (Last 7 deys)	55 TIB Døta af risk			Protected (1) 4 (Sast 7 days)	23 TiB Data protected		
Workloads Protectio	n groups				Q 1 💷	anage fansomware	protection strategies
Workload \$1	Type = = = =	Location 0	() importance T	O Privacy exposure Preview	▼ 0   Protection status ▼ 0	Detection statu	Action
oraclo-app-01	Oracle	bost.nerve.com	Critical	11/a	O ALHIA	ruta	Protect
Beshare_uswest_03_0192	File share	host.name.com	Critical	Medium	() At rosk	nva	Protect
oracle-app-02	Oracle	bost.name.com	Important	nia	() At muk	n/a	Protect
Reshare_sowest_02_3223	File share	host,name.com	Critical	High	Protected	Active	(Edt protection)
Reshare_iswest_01_3847	File share	host.name.com	Standard	identity exposure	Protected	Error	(Edt printection)
Reshare uswest 04 1231	File share	bost name com	Critical	interested and an an	Di Brodactari	(i) Artist	(La minution)

3. Selecione o link da carga de trabalho na coluna carga de trabalho para ver os detalhes da carga de trabalho.

Critical Importance ©	Protected  Protectize status	S Active Detection status	() 1 Alerts View alerts		Restore needed     Recovery     View recovery
High      High      Phinacy excounts	review) 🛞 investigate	O Protection	Edit protection	🕒 File share	
Total Pit     10.3k identifiers in 3f     Types of Pit identifiers	ta files 🤃	Protection group Rinance-apps View Ransonware rps-strategy-critice protection strategy	1	Location SnapCartier server	acspa2535184001.rtp.openenglab.netap com 10.100.100.100
Credit cants	8.1k = 210 ties	rps-detection-1     Detection policy	~	Storage	
* Passwords	293 in 100 thes	(a) fast-snapshots-vyz Snapshot policy	~	Volume Field	volume1 Value
Data subjects	O in Still flam	() Ipe-backup-xys	~	Field	Value Value

4. Na página Detalhes da carga de trabalho, reveja as informações no mosaico exposição à privacidade.

# Impacto da exposição à privacidade na importância da carga de trabalho

As alterações na exposição à privacidade podem afetar a importância da carga de trabalho.

Quando a exposição à privacidade:	A partir desta exposição à privacidade:	Para esta exposição à privacidade:	Então, a importância da carga de trabalho faz isso:
Diminui	Alta, média ou baixa	Médio, baixo ou nenhum	Permanece o mesmo

Quando a exposição à privacidade:	A partir desta exposição à privacidade:	Para esta exposição à privacidade:	Então, a importância da carga de trabalho faz isso:		
Aumentos	Nenhum	Baixo	Permanece no padrão		
	Baixo	Média	Muda de padrão para importante		
	Baixo ou médio	Alta	Alterações de padrão ou importante para crítico		

# Para mais informações

Para obter detalhes sobre a classificação BlueXP , consulte os seguintes tópicos de classificação BlueXP :

- "Saiba mais sobre a classificação BlueXP"
- "Categorias de dados privados"
- "Investigue os dados armazenados em sua organização"

#### Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

#### Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.