



Proteja workloads

BlueXP ransomware protection

NetApp
December 20, 2024

Índice

- Proteja workloads 1
 - Proteja workloads com estratégias de ransomware 1
 - Procure informações pessoalmente identificáveis com a classificação BlueXP 15

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 .

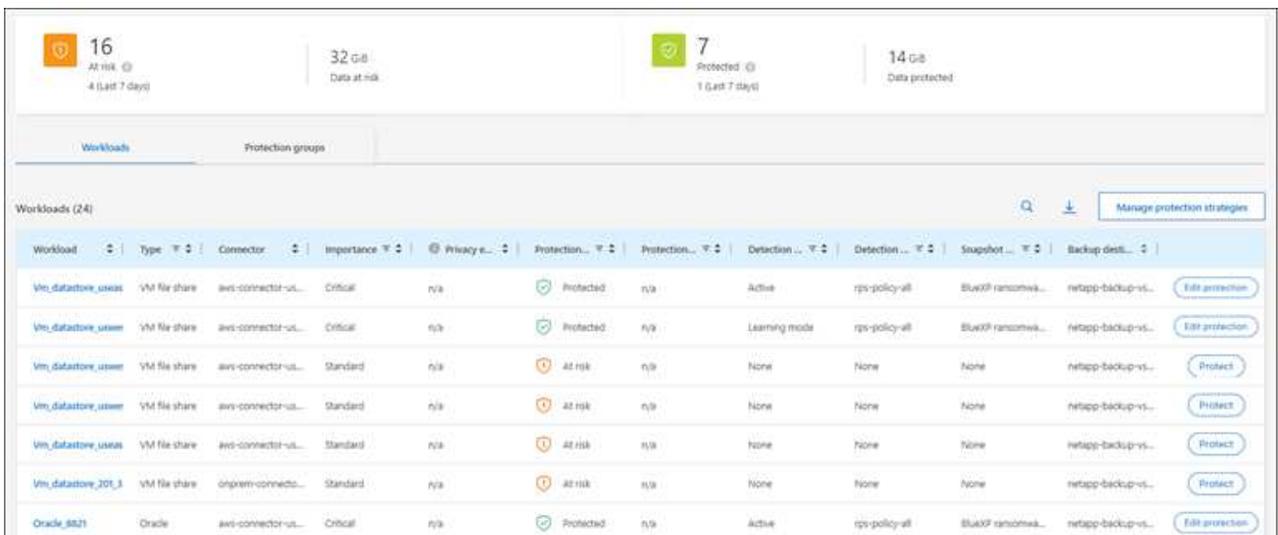
Ver a proteção contra ransomware em um workload

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**.



The screenshot displays the BlueXP interface for workload protection. At the top, there are three summary cards: 'At risk' (16 items, 4 last 7 days), 'Protected' (32 GiB, Data at risk), and 'Protected' (7 items, 1 last 7 days, 14 GiB Data protected). Below these is a navigation bar with 'Workloads' and 'Protection groups'. The main area shows a table of 24 workloads with columns for Workload, Type, Connector, Importance, Privacy, Protection, Detection, and Backup details. The table includes rows for various file shares and VMs, with protection status indicators like 'Protected', 'At risk', and 'Active'.

Workload	Type	Connector	Importance	Privacy e...	Protection...	Protection...	Detection ...	Detection ...	Snapshot ...	Backup detil...	
vm_datastore_usas	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rpo-policy-all	BlueXP ransomw...	netapp-backup-vs...	Edit protection
vm_datastore_usas	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Learning mode	rpo-policy-all	BlueXP ransomw...	netapp-backup-vs...	Edit protection
vm_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
vm_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
vm_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
vm_datastore_201_3	VM file share	onprem-connects...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Oracle_8821	Oracle	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rpo-policy-all	BlueXP ransomw...	netapp-backup-vs...	Edit 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 detecção 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 detecção: Uma carga de trabalho pode ter um dos seguintes status de detecção de ransomware:

- **Aprendizagem:** Uma política de detecção 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 detecção de ransomware não é atribuída.
- **Erro:** Uma política de detecção 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 detecção: O nome da política de detecção de ransomware aparece, se tiver sido atribuído. Se a política de detecção 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 detecção 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 de trabalho crítica	Quarto por hora	A cada 15 min	3	288	309
	Diariamente	A cada 1 dias	14	14	309
	Semanalmente	A cada 1 semanas	35	5	309
	Mensalmente	A cada 30 dias	60	2	309
Important e política de carga de trabalho	Quarto por hora	A cada 30 minutos	3	144	165
	Diariamente	A cada 1 dias	14	14	165
	Semanalmente	A cada 1 semanas	35	5	165
	Mensalmente	A cada 30 dias	60	2	165
Política de carga de trabalho padrão	Quarto por hora	A cada 30 min	3	72	93
	Diariamente	A cada 1 dias	14	14	93
	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 detecção 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 detecção 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 risk (4 last 7 days) | 32 GiB Data at risk | 7 Protected (1 last 7 days) | 14 GiB Data protected

Workload Protection groups

Workloads (24)

Workload	Type	Connector	Importance	Privacy	Protection	Protection	Detection	Detection	Snapshot	Backup dest.	
Win_datastore_usas	VM file share	aws-connector-us...	Critical	rya	Protected	rya	Active	rps-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_usam	VM file share	aws-connector-us...	Critical	rya	Protected	rya	Learning mode	rps-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_usam	VM file share	aws-connector-us...	Standard	rya	At risk	rya	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usam	VM file share	aws-connector-us...	Standard	rya	At risk	rya	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usas	VM file share	aws-connector-us...	Standard	rya	At risk	rya	None	None	None	netapp-backup-vs...	Protect
Win_datastore_201_3	VM file share	onprem-connecto...	Standard	rya	At risk	rya	None	None	None	netapp-backup-vs...	Protect
Oracle_8821	Oracle	aws-connector-us...	Critical	rya	Protected	rya	Active	rps-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection

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

Protection > Ransomware protection strategies

Ransomware protection strategies

Ransomware protection strategies (3)

Ransomware protection strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads	
rps-strategy-critical	critical-ss-policy	critical-bu-policy	rps-policy-all	3	▼ ***
rps-strategy-important	important-ss-policy	important-bu-policy	rps-policy-all	1	▼ ***
rps-strategy-standard	standard-ss-policy	standard-bu-policy	rps-policy-all	0	▼ ***

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

Protection > Manage protection strategies > Add ransomware protection strategy

Add ransomware protection strategy

Ransomware protection strategy name: RPS strategy 1

Copy from existing ransomware protection strategy: No policy selected [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 detecção:**

- **Política:** Escolha uma das políticas de detecção 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

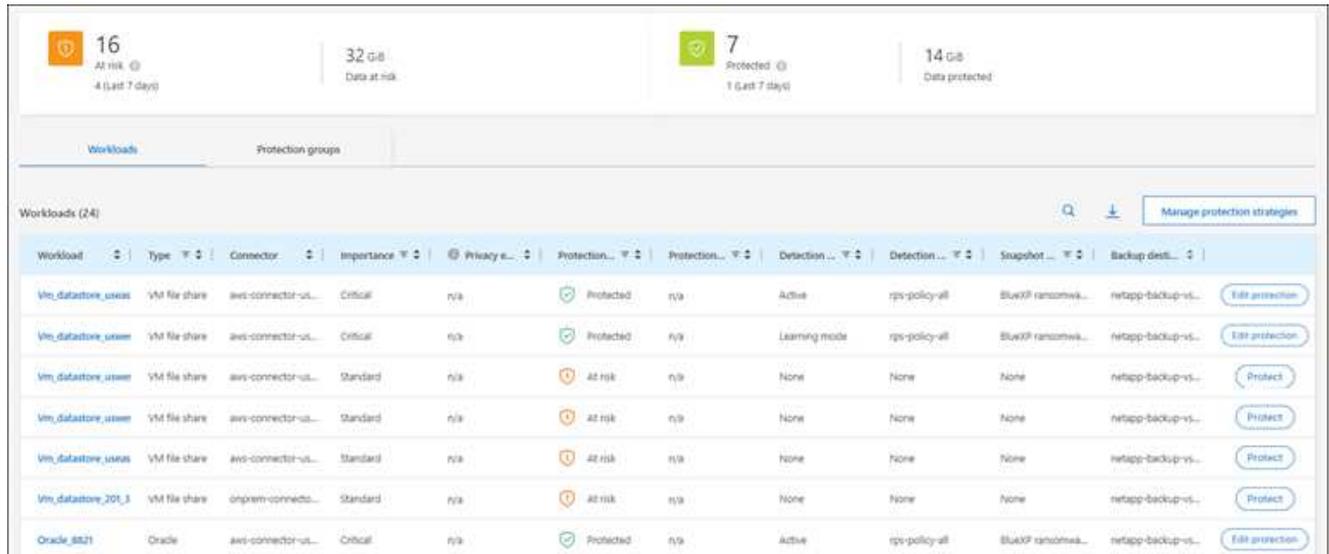
Com a proteção contra ransomware do BlueXP , você pode atribuir uma política de detecção de ransomware a workloads que já tenham políticas de snapshot e backup, gerenciados em outros produtos ou serviços da NetApp. A política de detecção não alterará as políticas gerenciadas em outros produtos.

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**.



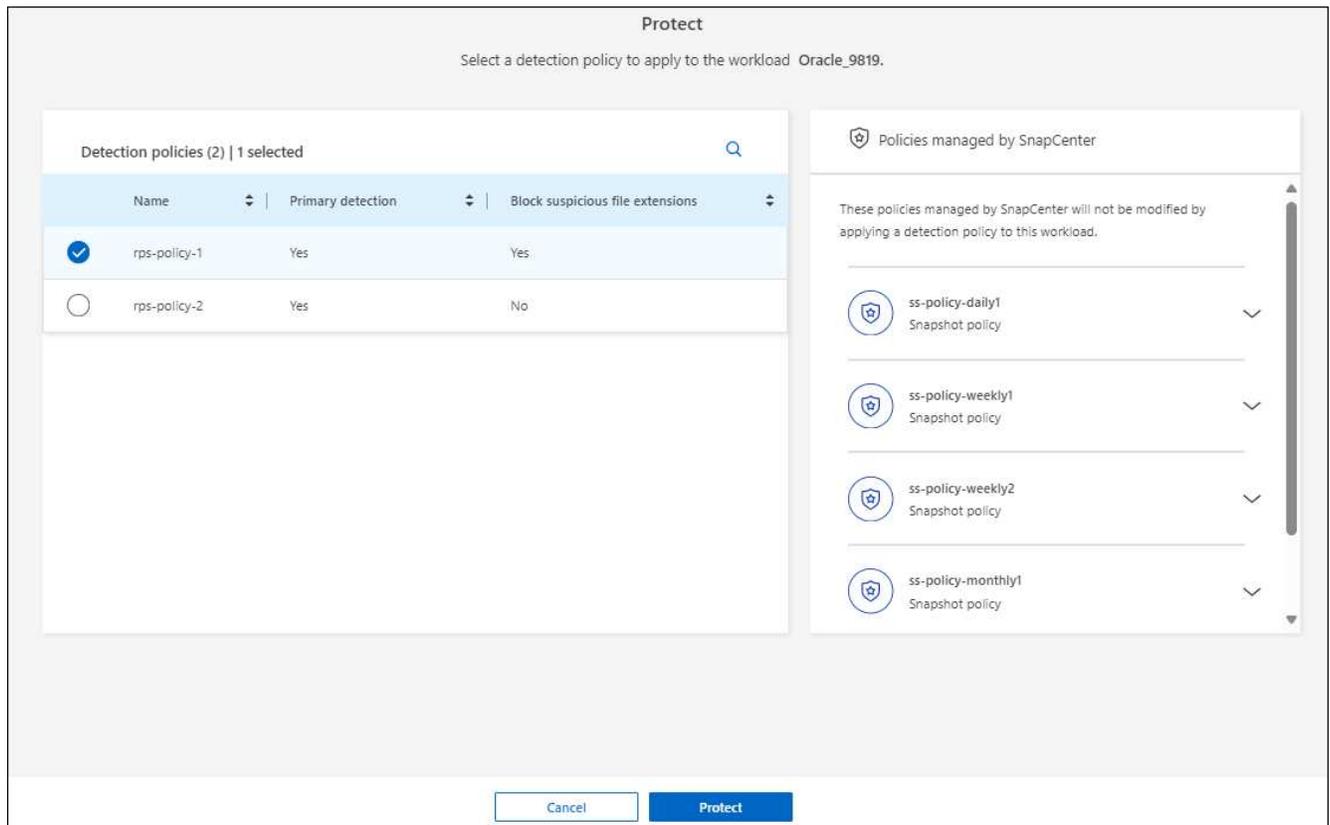
The screenshot displays the SnapCenter console interface. At the top, there are three summary cards: 'At risk' (16 items, 4 last 7 days), 'Data at risk' (32 GiB), and 'Protected' (7 items, 1 last 7 days, 14 GiB data protected). Below these is a navigation bar with 'Workloads' and 'Protection groups'. The main area shows a table of workloads with columns for Workload, Type, Connector, Importance, Privacy, Protection, Detection, Snapshot, and Backup destination. The table lists several VM file shares and an Oracle database, with their respective protection and detection statuses.

Workload	Type	Connector	Importance	Privacy	Protection	Detection	Snapshot	Backup dest.			
Win_datastore_usess	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransomwa... netapp-backup-vs...	Edit protection	
Win_datastore_usess	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Learning mode	rps-policy-all	BlueXP ransomwa... netapp-backup-vs...	Edit protection	
Win_datastore_usess	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usess	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usess	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_201_1	VM file share	onprem-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Oracle_8821	Oracle	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransomwa... netapp-backup-vs...	Edit protection	

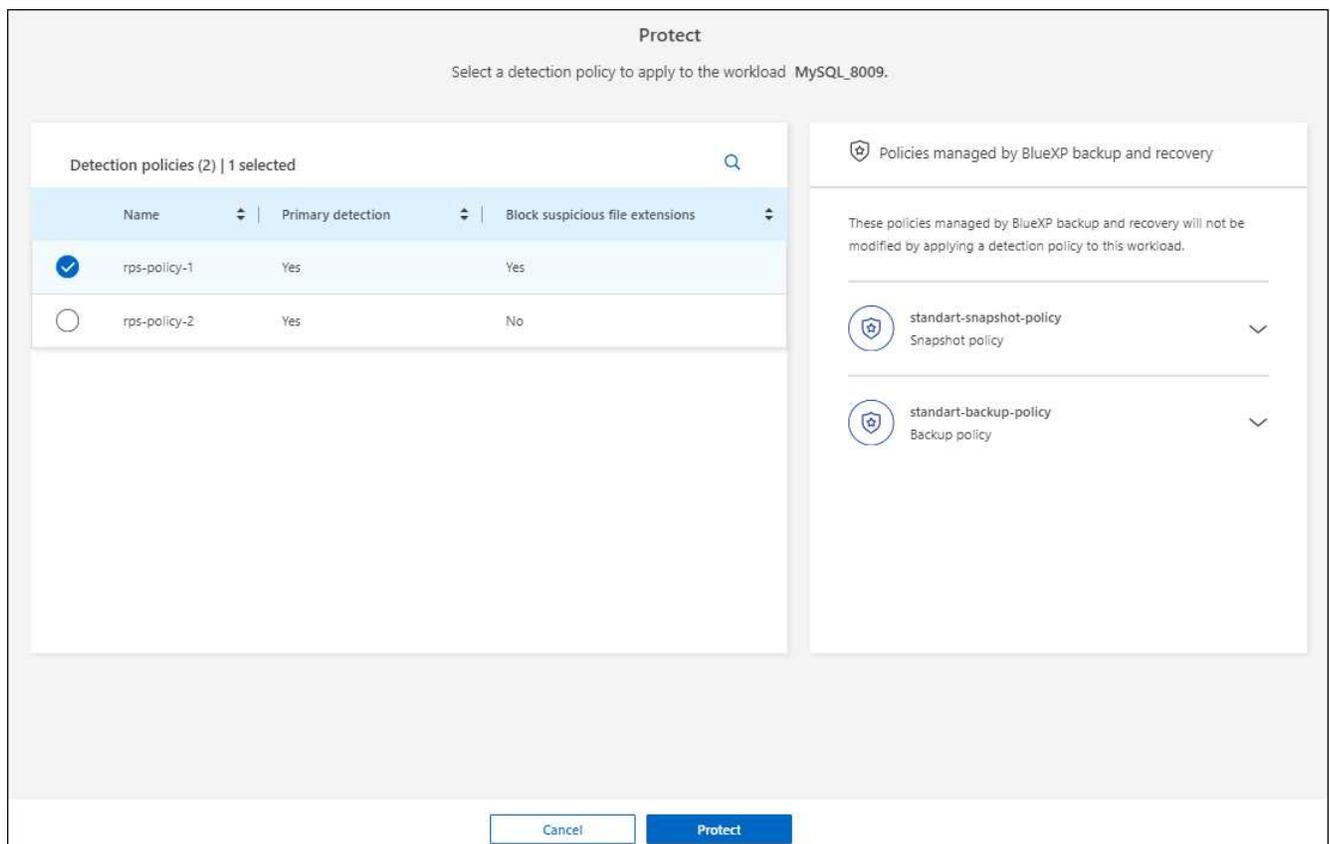
2. Na página proteção, selecione uma carga de trabalho e selecione **proteger**.

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:



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



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

- Para aplicar uma política de detecção além das políticas de instantâneos e backup gerenciadas em outro lugar, selecione a política de detecção.
- Selecione **Protect**.
- Na página de proteção, revise a coluna Política de detecção para ver a diretiva de detecção atribuída. Além disso, a coluna de 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

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

Compartilhe arquivos de grupo para facilitar a proteção

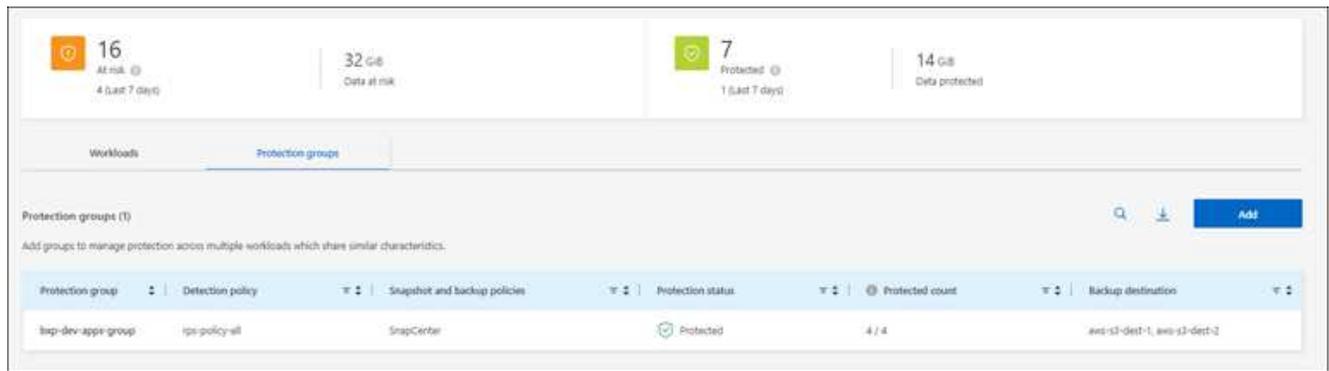
Agrupar compartilhamentos de arquivos facilita a proteção de seu data estate. O serviço pode proteger todos os volumes em um grupo ao mesmo tempo em vez de proteger cada volume separadamente.

Passos

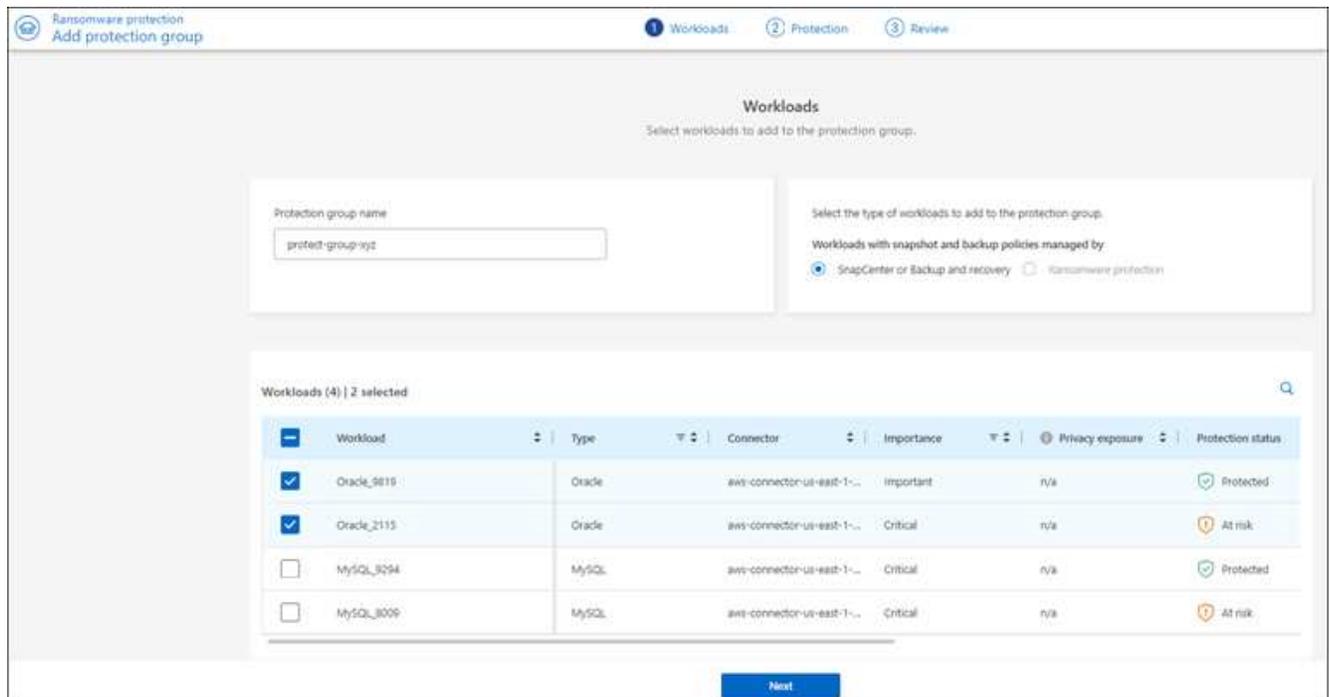
- No menu de proteção contra ransomware BlueXP, selecione **proteção**.

Workload	Type	Connector	Importance	Privacy	Protection	Detection	Snapshot	Backup dest.
Win_datastore_usaix	VM file share	aws-connector-us...	Critical	no	Protected	Active	BlueXP ransomwa...	netapp-backup-us...
Win_datastore_usaxm	VM file share	aws-connector-us...	Critical	no	Protected	Learning mode	BlueXP ransomwa...	netapp-backup-us...
Win_datastore_usaxw	VM file share	aws-connector-us...	Standard	no	At risk	None	None	netapp-backup-us...
Win_datastore_usaxv	VM file share	aws-connector-us...	Standard	no	At risk	None	None	netapp-backup-us...
Win_datastore_201_1	VM file share	onprem-connecto...	Standard	no	At risk	None	None	netapp-backup-us...
Oracle_8821	Oracle	aws-connector-us...	Critical	no	Protected	Active	BlueXP ransomwa...	netapp-backup-us...

- Na página de proteção, selecione a guia **grupos de proteção**.



3. Selecione **Adicionar**.



4. Introduza um nome para o grupo de proteção.

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**.

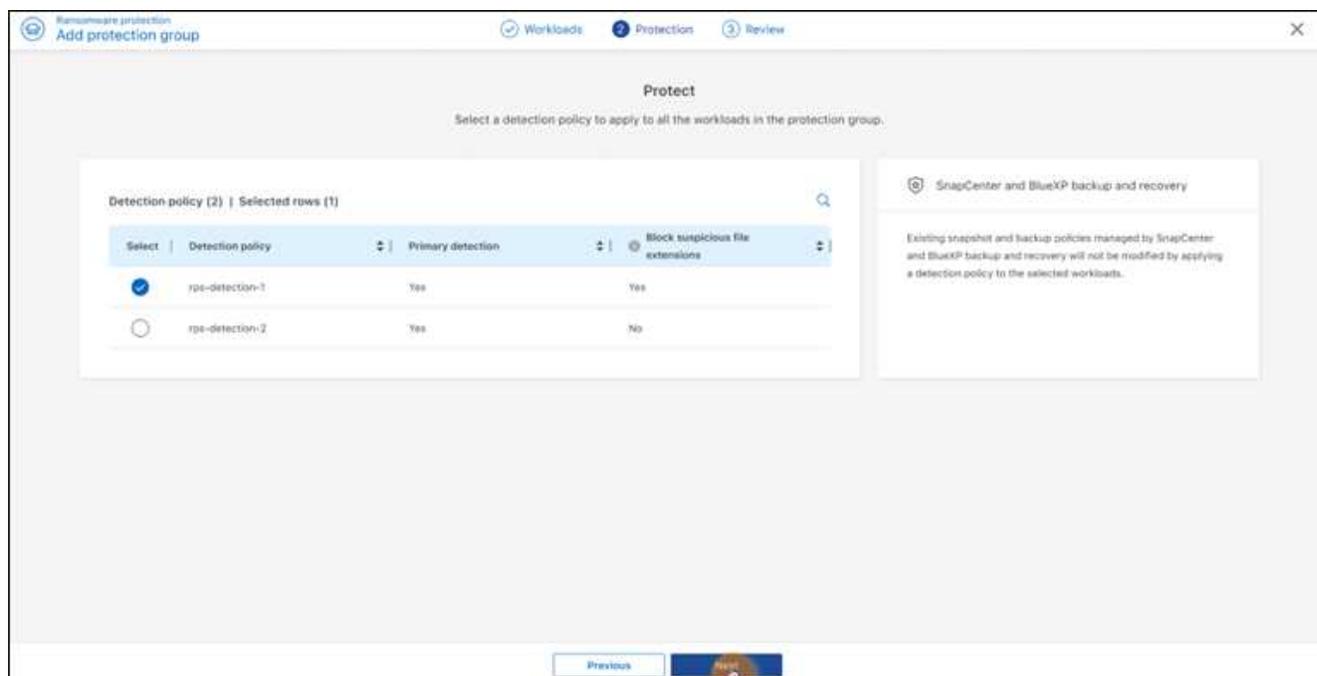
ii. Se o workload escolhido tiver volumes em vários ambientes de trabalho, selecione o destino do backup para os vários ambientes de trabalho para que eles possam ser copiados para a nuvem.

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**.



8. Selecione a política que governará a proteção para este grupo.

9. Selecione **seguinte**.

10. Reveja as seleções para o grupo de proteção.

11. Selecione **Adicionar**.

Remover workloads de um grupo

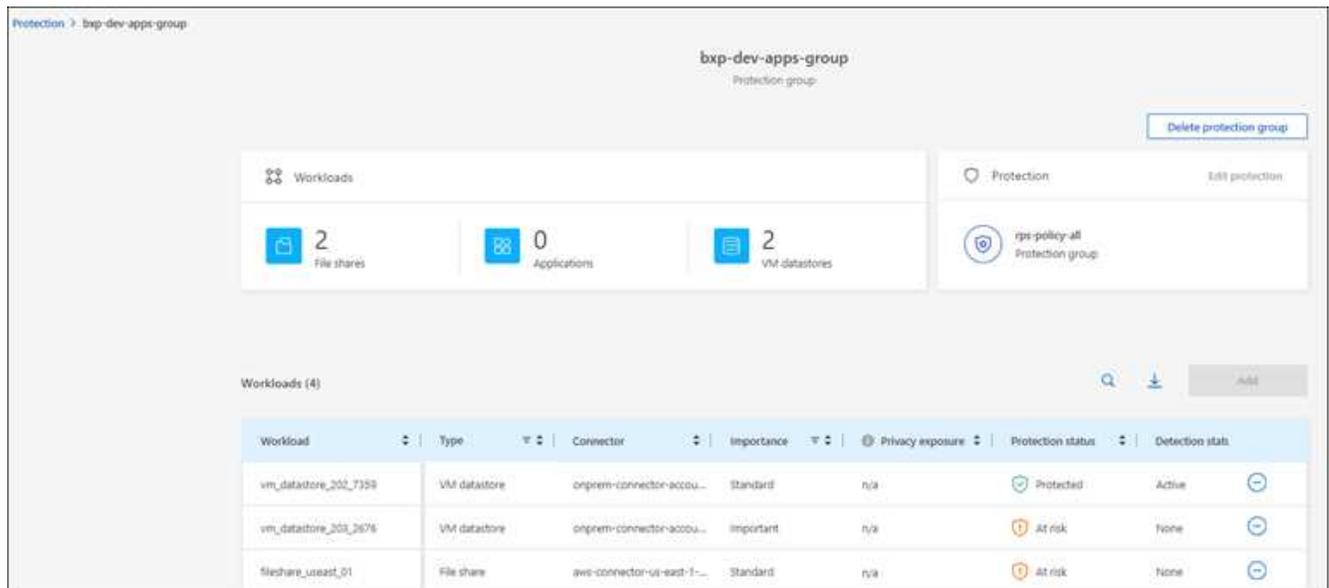
Mais tarde, talvez seja necessário remover cargas de trabalho de um grupo existente.

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.



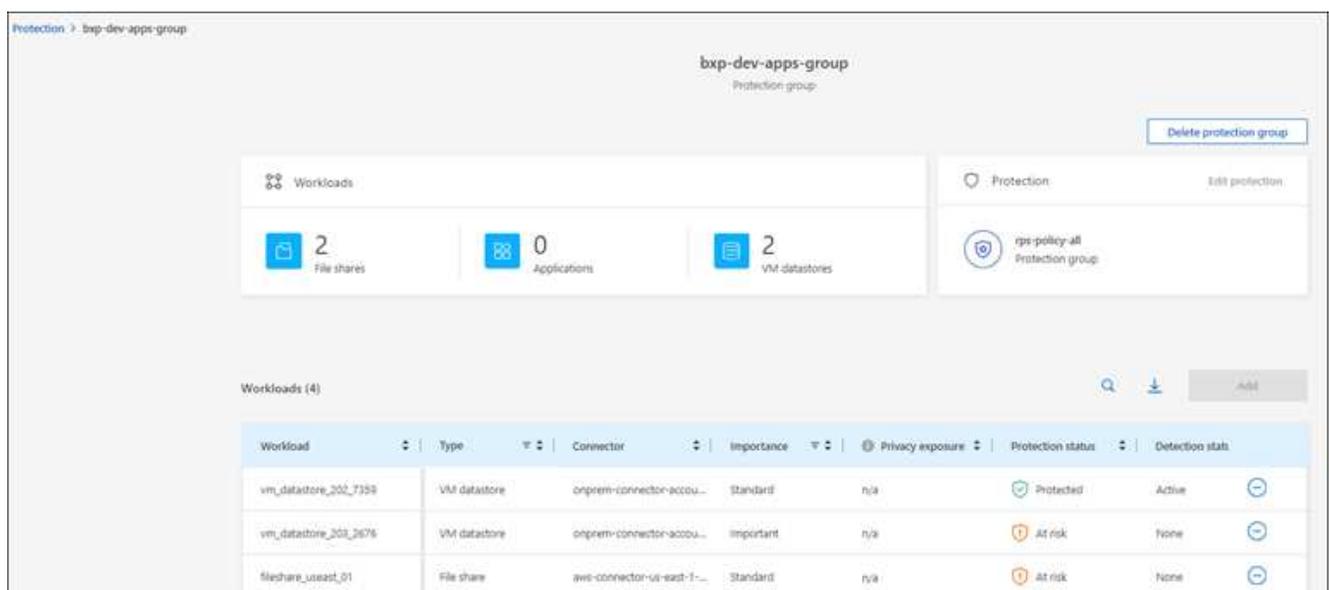
- Na página do grupo de proteção selecionado, selecione a carga de trabalho que deseja remover do grupo e selecione a opção *ações*...
- No menu ações, selecione **Remover carga de trabalho**.
- Confirme se deseja remover a carga de trabalho e selecione **Remover**.

Elimine o grupo de proteção

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

Passos

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



- 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.

Ransomware protection strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads	
rpi-strategy-critical	critical-si-policy	critical-bu-policy	rpe-policy-all	3	▼ ***
rpi-strategy-important	important-si-policy	important-bu-policy	rpe-policy-all	5	▼ ***
rpi-strategy-standard	standard-si-policy	standard-bu-policy	rpe-policy-all	0	▼ ***
RPS strategy 4	standard-si-policy-344	standard-bu-policy-344	rpe-policy-all	0	▼ ***

3. 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.

Passos

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.

Passos

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.

Workload	Type	Connec...	Import...	Privacy expos...	Protecti...	Protecti...	Detecti...	Detecti...	Snapsh...	Backup...	
Fileshare_useast_02	File share	aws-connector...	Critical	High	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_useast_01	File share	aws-connector...	Standard	Medium	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_useast_03	File share	aws-connector...	Standard	Identify exposure	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_useast_02_...	File share	aws-connector...	Critical	Identify exposure	Protected	n/a	Learning mode	rps-policy-all	BlueXP ransom...	netapp-backup...	Edit protection
Fileshare_useast_01	File share	aws-connector...	Standard	Identify exposure	At risk	n/a	None	None	None	n/a	Protect
Gcp_ha_voht_7496	File share	ran-gcp-conne...	Critical	Identify exposure	At risk	n/a	None	None	None	n/a	Protect
Vm_datastore_useast_...	Vm file share	aws-connector...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransom...	netapp-backup...	Edit protection

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

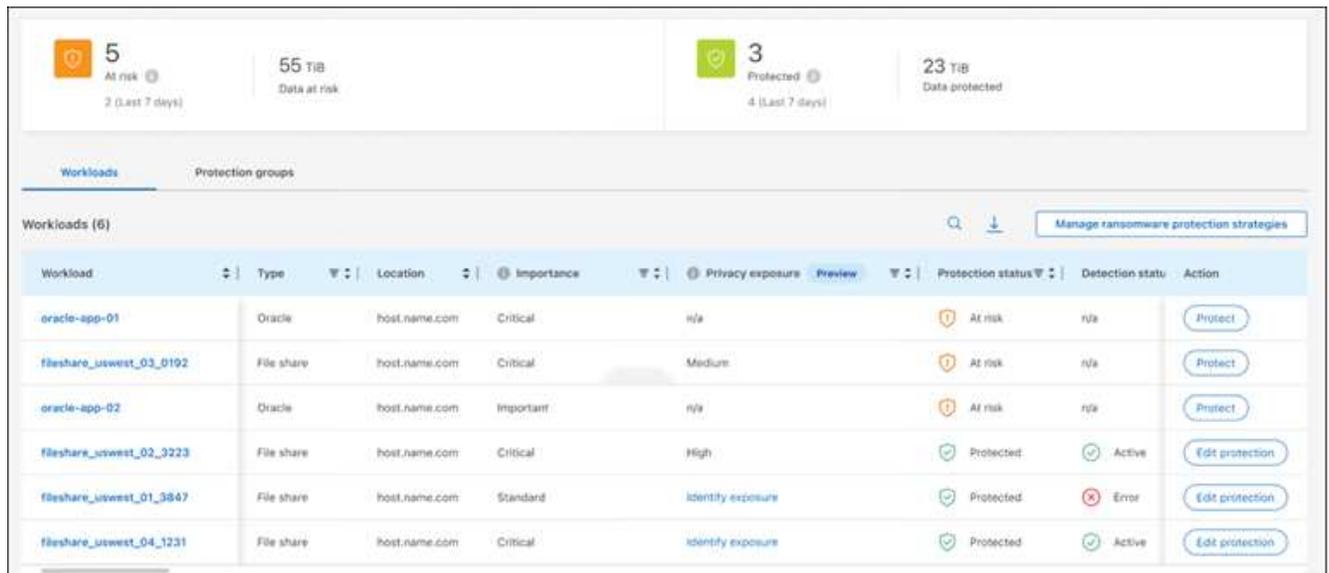
Após a classificação do BlueXP verificar informações de identificação pessoal (PII), você pode olhar para o risco de dados PII.

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

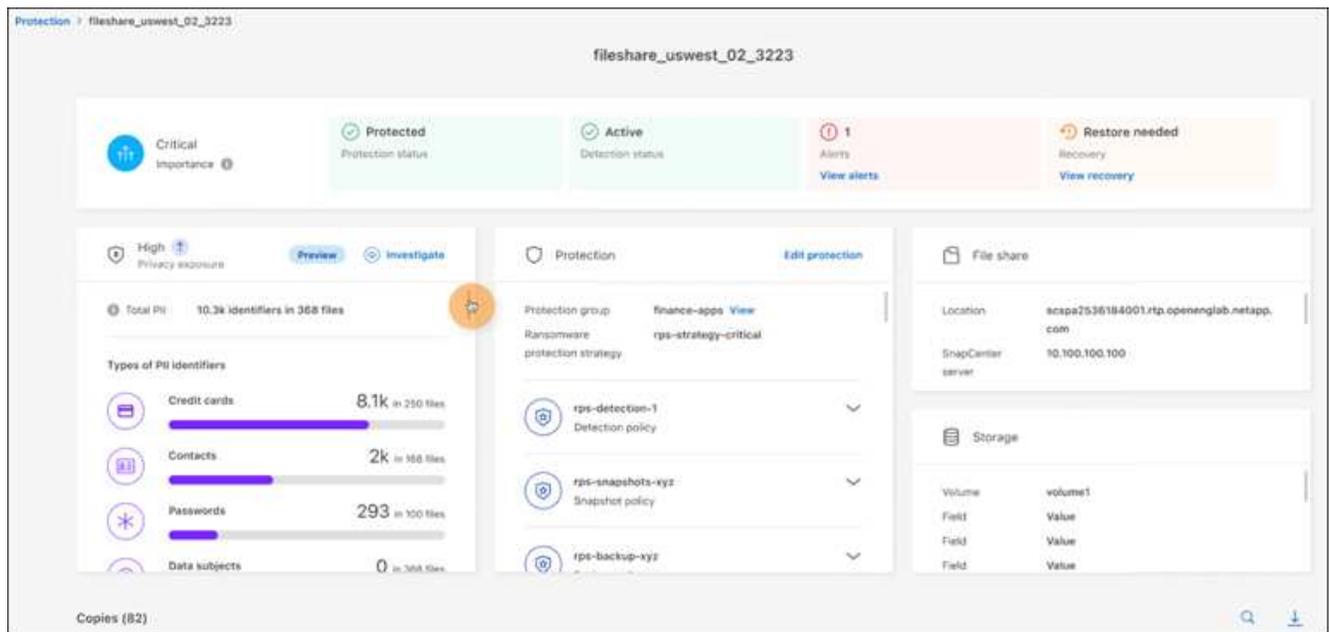
- **High:** Mais de 70% dos arquivos têm PII
- **Médio:** Maior que 30% e menos de 70% dos arquivos têm PII
- *** Baixo *:** Maior que 0 e menos de 30% dos arquivos têm PII

Passos

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.



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



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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO 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 DESTES SOFTWARES, 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.