



Use a proteção contra ransomware do BlueXP

BlueXP ransomware protection

NetApp
December 20, 2024

Índice

- Use a proteção contra ransomware do BlueXP 1
 - Use a proteção contra ransomware do BlueXP 1
 - Visualize rapidamente a integridade da carga de trabalho usando o Dashboard 1
 - Proteja workloads 6
 - Responda a um alerta de ransomware detetado 23
 - Recuperar de um ataque de ransomware (após os incidentes serem neutralizados) 32
 - Transferir relatórios 42

Use a proteção contra ransomware do BlueXP

Use a proteção contra ransomware do BlueXP

Com a proteção contra ransomware do BlueXP , você pode visualizar a integridade do workload e proteger workloads.

- ["Descubra workloads na proteção de ransomware BlueXP "](#).
- ["Visualize a proteção e a integridade do workload no Dashboard"](#).
 - Revise e aja de acordo com as recomendações de proteção contra ransomware.
- ["Proteja workloads"](#):
 - Atribua uma estratégia de proteção contra ransomware aos workloads.
 - Aumentar a proteção das aplicações para evitar futuros ataques de ransomware.
 - Crie, altere ou exclua uma estratégia de proteção.
- ["Responda à detecção de possíveis ataques de ransomware"](#).
- ["Recuperar de um ataque"](#) (depois que os incidentes são neutralizados).
- ["Configure as definições de proteção"](#).

Visualize rapidamente a integridade da carga de trabalho usando o Dashboard

O dashboard de proteção contra ransomware do BlueXP fornece informações gerais sobre a integridade da proteção de seus workloads. Você pode determinar rapidamente cargas de trabalho em risco ou protegidas, identificar cargas de trabalho afetadas por um incidente ou em recuperação e avaliar a extensão da proteção observando quanto storage está protegido ou em risco.

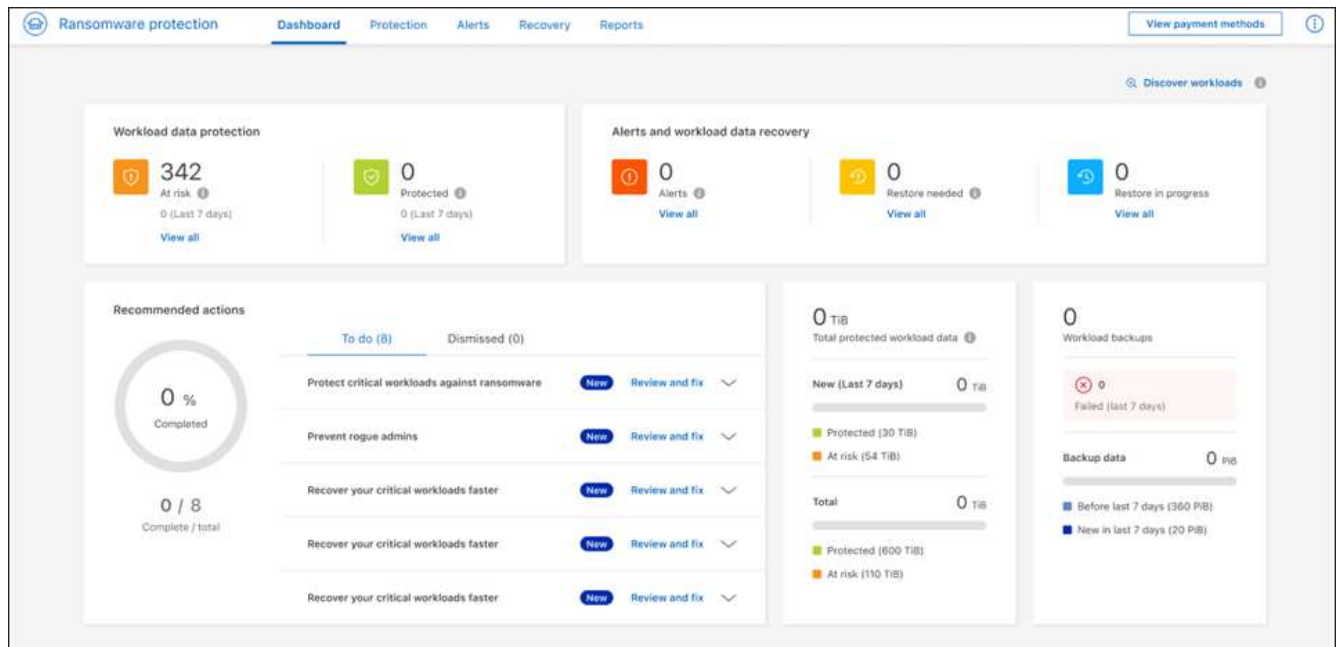
Você também pode usar o Painel para analisar e agir de acordo com as recomendações de proteção, acessar configurações globais, fazer download de relatórios e acessar esta documentação técnica.

Analisar a integridade do workload usando o Dashboard

Passos

1. Na navegação à esquerda do BlueXP , selecione **proteção > proteção contra ransomware**.

Após a descoberta, o Dashboard mostra a integridade da proteção de dados do workload.



2. No Dashboard, você pode executar as seguintes ações em cada um dos painéis:

- **Proteção de dados de carga de trabalho:** Clique em **Exibir tudo** para ver todas as cargas de trabalho que estão em risco ou protegidas na página proteção. As cargas de trabalho estão em risco quando os níveis de proteção não correspondem a uma política de proteção. "[Proteja workloads](#)" Consulte a .



Clique na nota "i" para ver dicas sobre esses dados. Para aumentar o limite de carga de trabalho, clique em **aumentar o limite de carga de trabalho** dentro desta nota eu. Clicar nisso leva você à página de suporte da BlueXP , onde você pode criar um ticket de caso.

- **Alertas e recuperação de dados da carga de trabalho:** Clique em **Exibir todos** para ver incidentes ativos que afetaram sua carga de trabalho, estão prontos para recuperação após incidentes serem neutralizados ou estão em recuperação. "[Responda a um alerta detetado](#)" Consulte a .
 - Um incidente é categorizado em um dos seguintes estados:
 - Novo
 - Demitido
 - A não perder
 - Resolvido
 - Um alerta pode ter um dos seguintes Estados:
 - Novo
 - Inativo
 - Uma carga de trabalho pode ter um dos seguintes status de restauração:
 - Restauração necessária
 - Em curso
 - Restaurado
 - Falha

- **Ações recomendadas:** Para aumentar a proteção, revise cada recomendação e clique em **Revisão e correção**.

["Revise as recomendações de proteção no Dashboard"](#)Consulte ou ["Proteja workloads"](#).

Todas as recomendações que foram adicionadas desde a última visita ao Dashboard são indicadas com "novo" por pelo menos 24 horas. As ações são listadas na ordem de prioridade com as mais importantes no topo. Você pode analisar e agir de acordo com cada um ou descartá-lo.

O número total de ações não inclui ações descartadas.

- **Dados de carga de trabalho:** Monitore alterações na cobertura de proteção nos últimos 7 dias.
- **Backups de carga de trabalho:** Monitore alterações nos backups de carga de trabalho criados pelo serviço que falharam ou foram concluídos com sucesso nos últimos 7 dias.

Revise as recomendações de proteção no Dashboard

A proteção contra ransomware do BlueXP avalia a proteção nos workloads e recomenda ações para aprimorar essa proteção.

Você pode revisar uma recomendação e agir sobre ela, o que altera o status da recomendação para concluir. Ou, se você quiser agir sobre isso mais tarde, você pode descartá-lo. Rejeitar uma ação move a recomendação para uma lista de ações descartadas, que você pode revisar mais tarde.

Aqui está uma amostra das recomendações que o serviço oferece.

Recomendação	Descrição	Como resolver
Adicionar uma política de proteção contra ransomware.	No momento, a carga de trabalho não está protegida.	Atribua uma política à carga de trabalho. "Proteja workloads contra ataques de ransomware" Consulte a .
Conecte-se ao SEIM para relatórios de ameaças.	Envie dados para um sistema de gerenciamento de eventos e segurança (SIEM) para análise e detecção de ameaças.	Insira os detalhes do servidor SIEM/XDR para habilitar a detecção de ameaças. "Configure as definições de proteção" Consulte a .
Habilite a proteção consistente com o workload para aplicações ou VMware.	Essas cargas de trabalho não são gerenciadas pelo software SnapCenter ou pelo plug-in SnapCenter para VMware vSphere.	Para gerenciá-los pelo SnapCenter, habilite a proteção consistente com o workload. "Proteger a carga de trabalho contra ataques de ransomware" Consulte a .
Melhorar a postura de segurança para o ambiente de trabalho	O consultor digital da NetApp identificou pelo menos um risco de segurança alto ou crítico.	Analise todos os riscos de segurança no consultor digital da NetApp. Consulte a "Documentação do Digital Advisor" .

Recomendação	Descrição	Como resolver
Tornar uma política mais forte.	Algumas cargas de trabalho podem não ter proteção suficiente. Fortaleça a proteção das cargas de trabalho com uma política.	Aumente a retenção, adicione backups, aplique backups imutáveis, bloqueie extensões de arquivo suspeitas, habilite a detecção no storage secundário e muito mais. " Proteja workloads contra ataques de ransomware "Consulte a .
Prepare o <backup provider> como destino de backup para fazer backup dos dados de workload.	No momento, a carga de trabalho não tem destinos de backup.	Adicione destinos de backup a essa carga de trabalho para protegê-la. " Configure as definições de proteção "Consulte a .
Proteja workloads de aplicações essenciais ou altamente importantes contra ransomware.	A página proteger exibe workloads da aplicação críticos ou altamente importantes (com base no nível de prioridade atribuído) que não estão protegidos.	Atribua uma política a esses workloads. " Proteja workloads contra ataques de ransomware "Consulte a .
Proteja workloads de compartilhamento de arquivos essenciais ou altamente importantes contra ransomware.	A página proteção exibe cargas de trabalho críticas ou altamente importantes do tipo Compartilhamento de arquivos ou datastore que não estão protegidos.	Atribua uma política a cada um dos workloads. " Proteja workloads contra ataques de ransomware "Consulte a .
Registre o plugin SnapCenter disponível para VMware vSphere (SCV) com o BlueXP	Um workload de VM não é protegido.	Atribua proteção consistente com VM à carga de trabalho da VM habilitando o plug-in SnapCenter para VMware vSphere. " Proteja workloads contra ataques de ransomware "Consulte a .
Registre o servidor SnapCenter disponível com o BlueXP	Uma aplicação não está protegida.	Atribua proteção consistente com aplicativos à carga de trabalho habilitando o servidor SnapCenter. " Proteja workloads contra ataques de ransomware "Consulte a .
Reveja novos alertas.	Existem novos alertas.	Reveja os novos alertas. " Responda a um alerta de ransomware detetado "Consulte a .

Passos

1. Na navegação à esquerda do BlueXP , selecione **proteção > proteção contra ransomware**.
2. No painel ações recomendadas, selecione uma recomendação e selecione **Revisão e correção**.
3. Para ignorar a ação até mais tarde, selecione **Dismiss**.

A recomendação é eliminada da lista to do (tarefas) e aparece na lista descartada.



Mais tarde, você pode alterar um item demitido para um item para fazer. Quando você marca um item concluído ou altera um item rejeitado para uma ação para fazer, o total de ações aumenta em 1.

4. Para rever informações sobre como agir sobre as recomendações, selecione o ícone **informação**.

Exportar dados de proteção para arquivos CSV

Você pode exportar dados e baixar arquivos CSV que mostram detalhes de proteção, alertas e recuperação.

Você pode baixar arquivos CSV de qualquer uma das opções do menu principal:

- **Proteção:** Contém o status e detalhes de todas as cargas de trabalho, incluindo o número total protegido e em risco.
- **Alertas:** Inclui o status e detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação:** Inclui o status e os detalhes de todas as cargas de trabalho que precisam ser restauradas, incluindo o número total de cargas de trabalho marcadas como "Restaurar necessário", "em andamento", "Restaurar falhou" e "restaurado com sucesso".

Se você baixar arquivos CSV da página proteção, Alertas ou recuperação, apenas os dados dessa página serão incluídos no arquivo CSV.


Os arquivos CSV incluem dados para todos os workloads em todos os ambientes de trabalho do BlueXP .

Passos


1. Na navegação à esquerda do BlueXP , selecione **proteção > proteção contra ransomware**.

The screenshot displays the 'Ransomware protection' dashboard. At the top, there are navigation tabs for 'Dashboard', 'Protection', 'Alerts', 'Recovery', and 'Reports'. The main content area is divided into several sections:

- Workload data protection:** Shows 342 items 'At risk' and 0 items 'Protected'.
- Alerts and workload data recovery:** Shows 0 'Alerts', 0 'Restore needed', and 0 'Restore in progress'.
- Recommended actions:** A list of tasks to be completed, such as 'Protect critical workloads against ransomware' and 'Prevent rogue admins', each with a 'Review and fix' button.
- Total protected workload data:** A progress bar showing 0 TiB total, with 0 TiB new in the last 7 days.
- Workload backups:** Shows 0 'Failed' backups in the last 7 days.
- Backup data:** Shows 0 PiB of backup data, with 0 PiB before last 7 days and 0 PiB new in last 7 days.

2. Na página, selecione a opção **Atualizar**  no canto superior direito para atualizar os dados que aparecerão nos arquivos.


3. Execute um dos seguintes procedimentos:

- Na página, selecione a opção *Download*  .
 - No menu proteção contra ransomware do BlueXP , selecione **relatórios**.
4. Se você selecionou a opção **relatórios**, selecione um dos arquivos nomeados pré-configurados e selecione **Download (CSV)** ou **Download (JSON)**.

Accesse a documentação técnica

Você pode acessar esta documentação técnica a partir de docs.NetApp.com ou dentro do serviço de proteção contra ransomware BlueXP .

Passos

1. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.
2.
No Dashboard, selecione a opção vertical *actions*  .
3. Selecione uma destas opções:
 - **Novidades** para visualizar informações sobre os recursos nas versões atuais ou anteriores nas Notas de versão.
 - **Documentação** para visualizar a página inicial da documentação de proteção contra ransomware do BlueXP e esta documentação.

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**.

Workload	Type	Connector	Importance	Privacy e...	Protection...	Protection...	Detection...	Detection...	Snapshot...	Backup desti...	
Win_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
Win_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
Win_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_usas	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_201_3	VM file share	onprem-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Oracle_S&T	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
Importante 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

Nível de política	Snapshot	Frequência	Retenção (dias)	nº de cópias snapshot	Número máximo total de cópias snapshot
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.

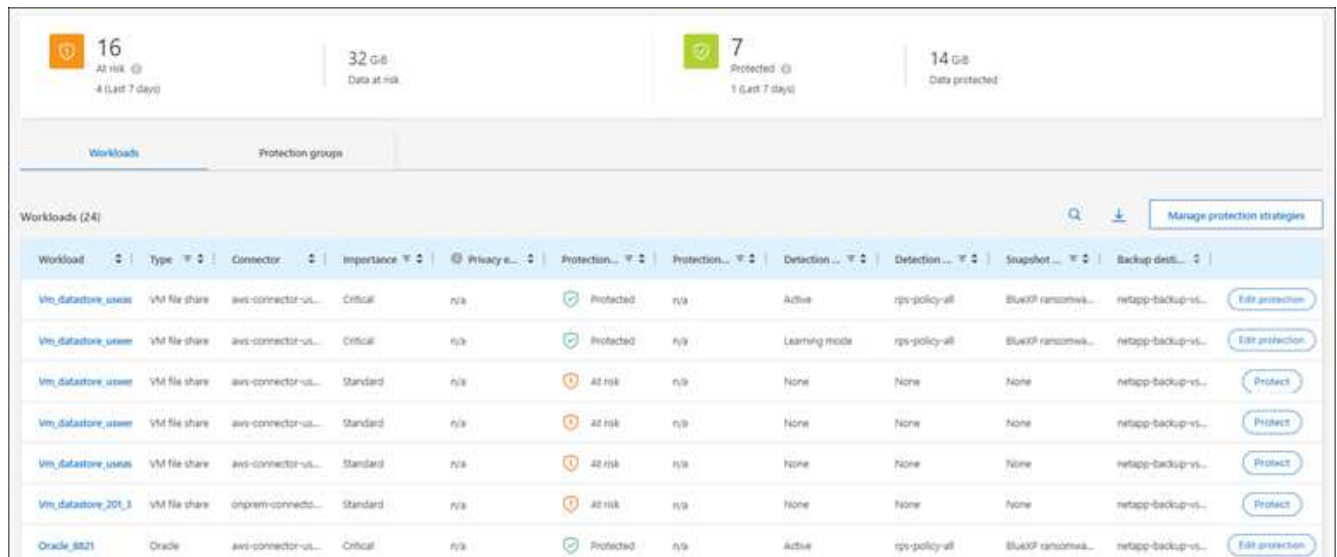
Criar uma estratégia de proteção contra ransomware (se você não tiver políticas de snapshot ou backup)

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**.



The screenshot displays the NetApp BlueXP ransomware protection dashboard. 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' tabs. The main area shows a table of 24 workloads with columns for Workload, Type, Connector, Importance, Privacy, Protection, Detection, Snapshot, and Backup. The table lists various VM file shares and Oracle databases, with their current protection status (e.g., Protected, At risk) and associated policies.

Workload	Type	Connector	Importance	Privacy	Protection	Detection	Snapshot	Backup	Action		
vm_datastore_usas	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransomwa... netapp-backup-vs...	Edit protection	
vm_datastore_usam	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Learning mode	rps-policy-all	BlueXP ransomwa... netapp-backup-vs...	Edit protection	
vm_datastore_usam	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
vm_datastore_usam	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-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Oracle_8521	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 **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

Detection policy: rps-policy-primary ▼

Snapshot policy: important-ss-policy ▼

Backup policy: None ▼

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**.

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

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 the workload Oracle_9819.

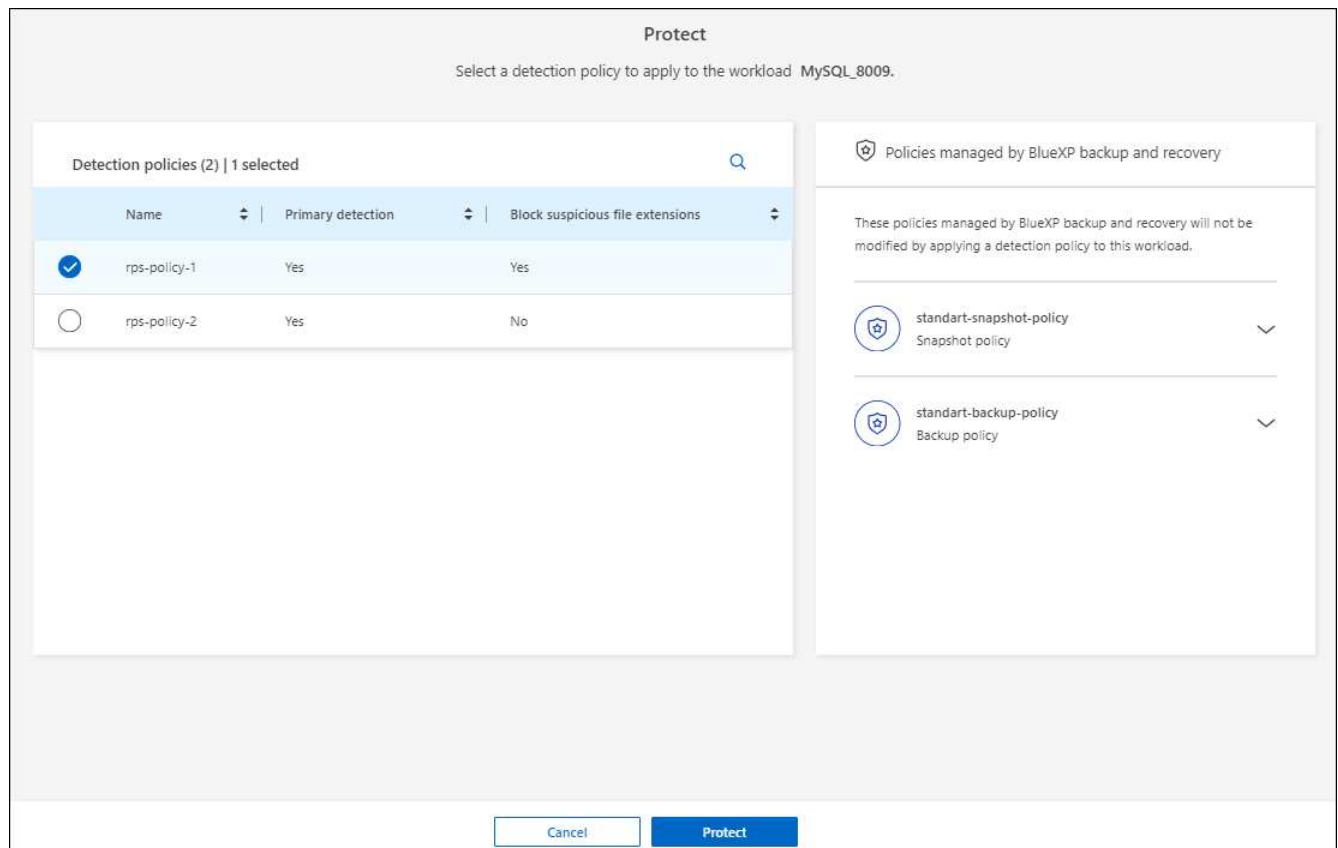
Name	Primary detection	Block suspicious file extensions
<input checked="" type="radio"/> rps-policy-1	Yes	Yes
<input type="radio"/> rps-policy-2	Yes	No

Policies managed by SnapCenter

These policies managed by SnapCenter will not be modified by applying a detection policy to this workload.

- ss-policy-daily1
Snapshot policy
- ss-policy-weekly1
Snapshot policy
- ss-policy-weekly2
Snapshot policy
- ss-policy-monthly1
Snapshot policy

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**.
4. Para aplicar uma política de detecção 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

Agupar 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**.

The screenshot displays the 'Workloads' section of the BlueXP ransomware protection 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) with 'Data protected' (14 GiB). Below these are tabs for 'Workloads' and 'Protection groups'. The main area shows a table of 24 workloads with columns for Workload, Type, Connector, Importance, Privacy, Protection status, Protection policy, Detection policy, Detection strategy, Snapshot, and Backup destination. Each row includes an 'Edit protection' button.

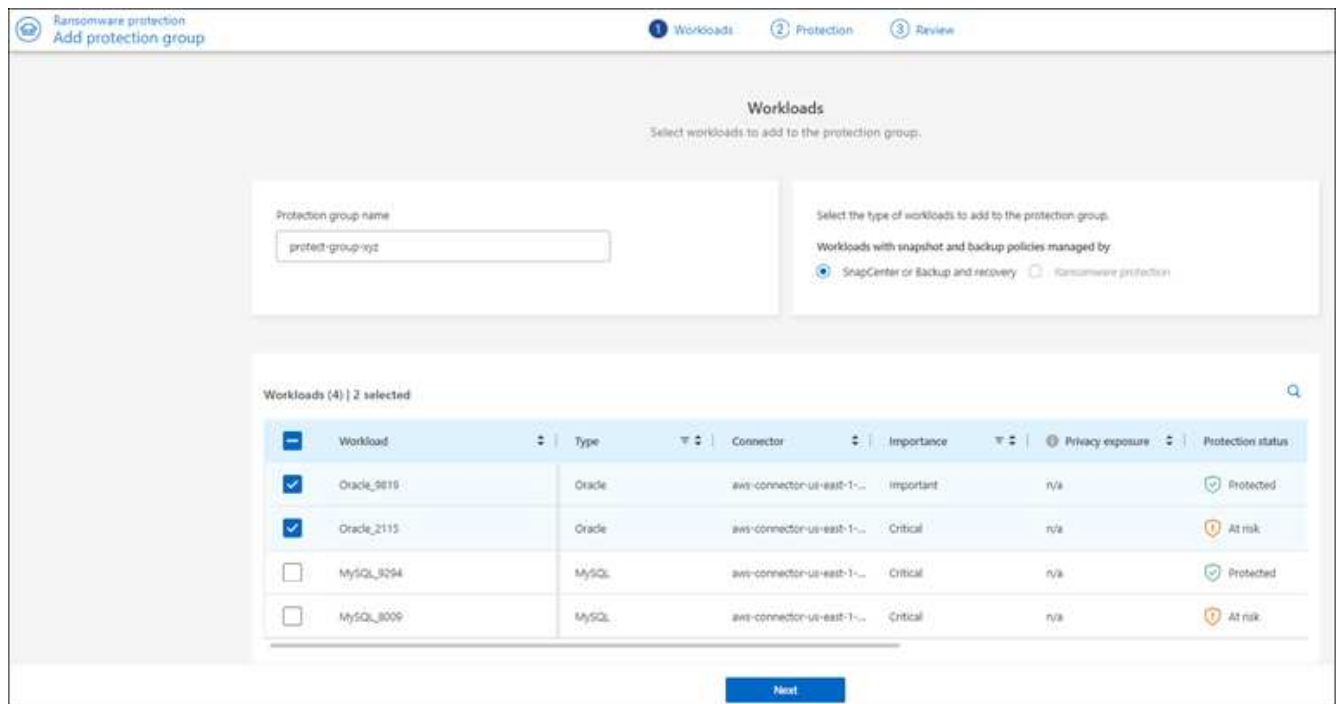
Workload	Type	Connector	Importance	Privacy	Protection	Protection	Detection	Detection	Snapshot	Backup dest.	
Win_datastore_usaes	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransomwa...	netapp-backup-us...	Edit protection
Win_datastore_usaes	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Learning mode	rps-policy-all	BlueXP ransomwa...	netapp-backup-us...	Edit protection
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-us...	Protect
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-us...	Protect
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-us...	Protect
Win_datastore_20T_1	VM file share	onprem-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-us...	Protect
Oracle_B&Z1	Oracle	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rps-policy-all	BlueXP ransomwa...	netapp-backup-us...	Edit protection

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

The screenshot displays the 'Protection groups' section of the BlueXP ransomware protection 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) with 'Data protected' (14 GiB). Below these are tabs for 'Workloads' and 'Protection groups'. The main area shows a table of 1 protection group with columns for Protection group, Detection policy, Snapshot and backup policies, Protection status, Protected count, and Backup destination. An 'Add' button is visible in the top right.

Protection group	Detection policy	Snapshot and backup policies	Protection status	Protected count	Backup destination
isp-dev-apps group	rps-policy-all	SnapCenter	Protected	4 / 4	aws-s3-dest-1, aws-s3-dest-2

3. Selecione **Adicionar**.

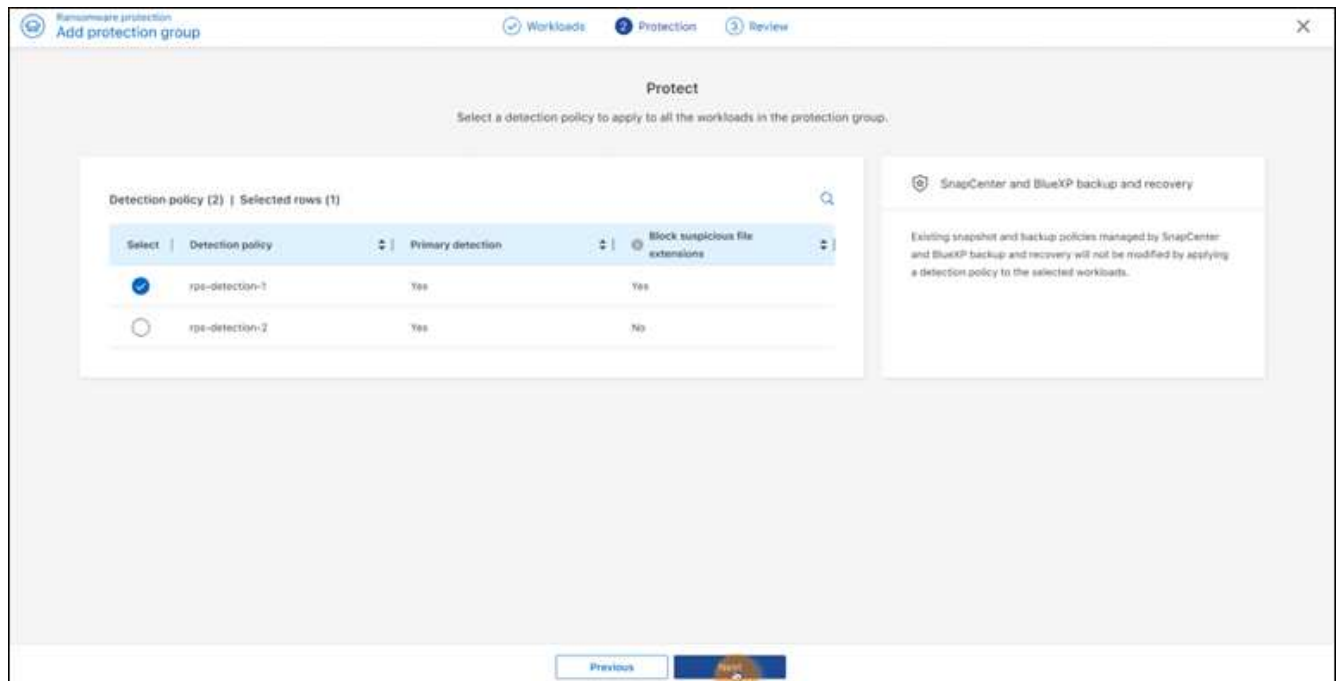


4. Introduza um nome para o grupo de proteção.
5. Execute um dos seguintes passos:
 - a. Se você já tiver políticas de proteção em vigor, selecione se deseja agrupar cargas de trabalho com base no gerenciamento dessas mesmas:
 - Proteção contra ransomware da BlueXP
 - Backup e recuperação do SnapCenter 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**.



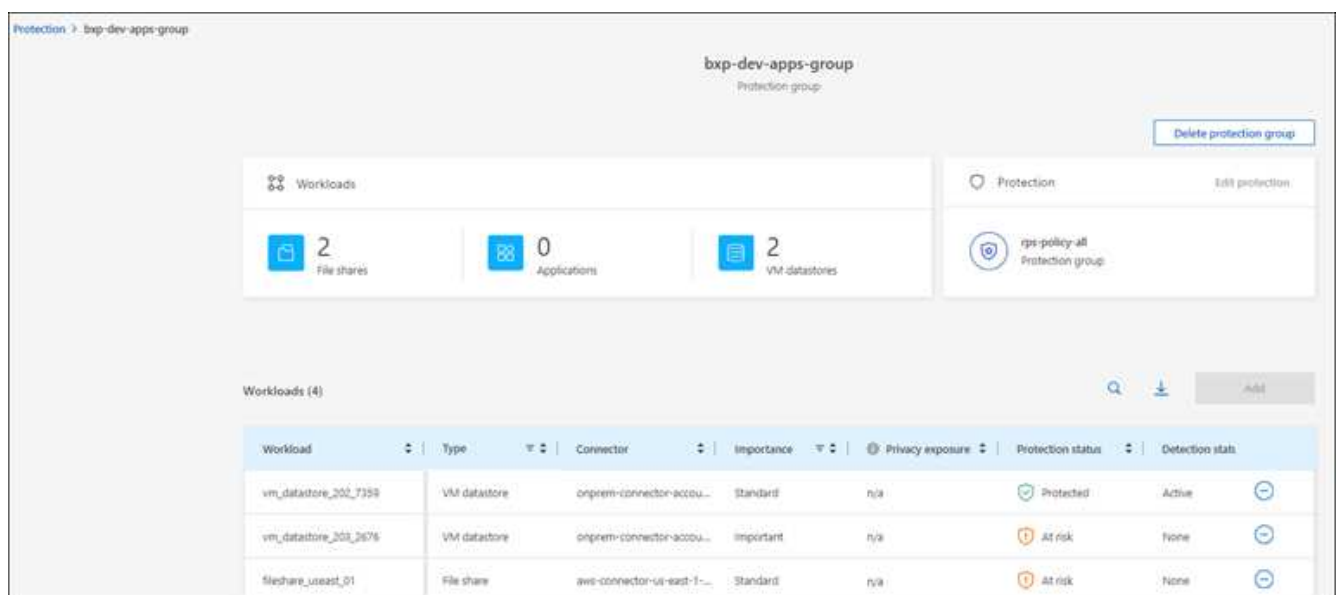
8. Selecione a política que governará a proteção para este grupo.
9. Selecione **seguinte**.
10. Reveja as seleções para o grupo de proteção.
11. Selecione **Adicionar**.

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.



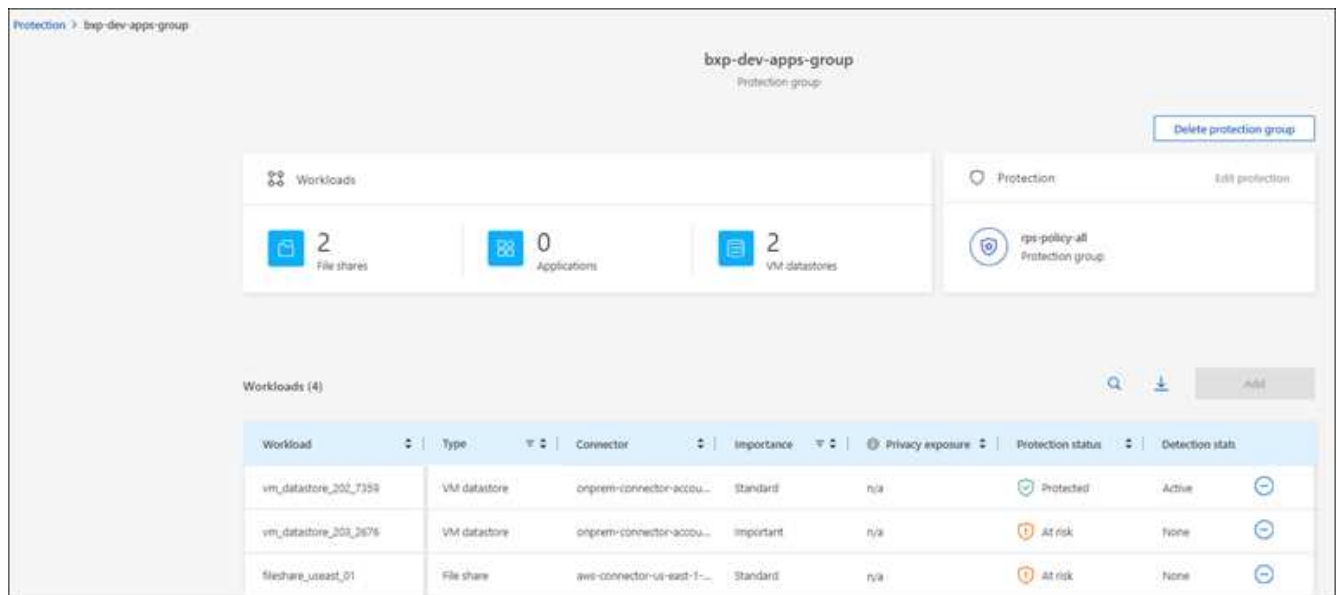
4. Na página do grupo de proteção selecionado, selecione a carga de trabalho que deseja remover do grupo e selecione a opção *ações*...
5. No menu ações, selecione **Remover carga de trabalho**.
6. Confirme se deseja remover a carga de trabalho e selecione **Remover**.

Elimine o grupo de proteção

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.



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.

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_us-east_02	File share	aws-connector...	Critical	High	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_us-west_01	File share	aws-connector...	Standard	Medium	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_us-east_03	File share	aws-connector...	Standard	Identify exposure	At risk	n/a	None	None	None	netapp-backup...	Protect
Fileshare_us-west_02_...	File share	aws-connector...	Critical	Identify exposure	Protected	n/a	Learning mode	rps-policy-all	BlueXP ransom...	netapp-backup...	Edit protection
Fileshare_us-east_01	File share	aws-connector...	Standard	Identify exposure	At risk	n/a	None	None	None	n/a	Protect
Gcp_ha_volt_7496	File share	aws-gcp-conne...	Critical	Identify exposure	At risk	n/a	None	None	None	n/a	Protect
Vm_datastore_us-east...	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.

Workload	Type	Location	Importance	Privacy exposure	Protection status	Detection status	Action
oracle-app-01	Oracle	host.name.com	Critical	n/a	At risk	n/a	Protect
fileshare_uswest_03_0192	File share	host.name.com	Critical	Medium	At risk	n/a	Protect
oracle-app-02	Oracle	host.name.com	Important	n/a	At risk	n/a	Protect
fileshare_uswest_02_3223	File share	host.name.com	Critical	High	Protected	Active	Edit protection
fileshare_uswest_01_3847	File share	host.name.com	Standard	Identify exposure	Protected	Error	Edit protection
fileshare_uswest_04_1231	File share	host.name.com	Critical	Identify exposure	Protected	Active	Edit protection

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

fileshare_uswest_02_3223

- Critical Importance**
- Protected** Protection status
- Active** Detection status
- 1 Alerts** View alerts
- Restore needed** Recovery View recovery

High Privacy exposure **Preview** **Investigate**

Total PII 10.3k identifiers in 368 files

Types of PII Identifiers

- Credit cards: 8.1k in 250 files
- Contacts: 2k in 168 files
- Passwords: 293 in 100 files
- Data subjects: 0 in 368 files

Protection **Edit protection**

Protection group: finance-apps View
Ransomware protection strategy: rps-strategy-critical

- rps-detection-1 Detection policy
- rps-snapshots-xyz Snapshot policy
- rps-backup-xyz

File share

Location: scspa2536184001.rtp.openenlab.netapp.com
SnapCenter server: 10.100.100.100

Storage

Volume: volume1
Field: Value
Field: Value
Field: Value

Copies (82)

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
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"](#)

Responda a um alerta de ransomware detetado

Se a proteção contra ransomware do BlueXP detectar um possível ataque, um alerta será exibido no Painel de proteção contra ransomware do BlueXP e nas notificações do BlueXP , no canto superior direito, indicando um possível ataque de ransomware. O serviço também inicia imediatamente a obtenção de uma cópia snapshot. Neste ponto, você deve olhar para o risco potencial na guia **Alertas** de proteção contra ransomware BlueXP .

Você pode ignorar falsos positivos ou decidir recuperar seus dados imediatamente.



Se você decidir ignorar o alerta, o serviço irá aprender esse comportamento e associá-lo a operações normais e não iniciar um alerta sobre tal comportamento novamente.

Para começar a recuperar seus dados, marque o alerta como pronto para recuperação para que seu administrador de armazenamento possa iniciar o processo de recuperação.

Cada alerta pode ter vários incidentes em volumes diferentes com status diferentes, portanto, certifique-se de olhar para todos os incidentes.

O serviço fornece informações chamadas *Evidence* sobre o que causou a emissão do alerta, como o seguinte:

- Extensões de arquivo foram criadas ou alteradas
- A criação de arquivos ocorreu e aumentou em uma porcentagem listada
- A exclusão de arquivos ocorreu e aumentou em uma porcentagem listada

Um alerta é baseado nos seguintes tipos de comportamento:

- **Ataque potencial:** Um alerta ocorre quando o Autonomous ransomware Protection deteta uma nova extensão e a ocorrência é repetida mais de 20 vezes nas últimas 24 horas (comportamento padrão).
- **Aviso:** Um aviso ocorre com base nos seguintes comportamentos:
 - A detecção de uma nova extensão não foi identificada antes e o mesmo comportamento não repete tempos suficientes para declará-la como um ataque.
 - Alta entropia é observada.
 - As operações de leitura/gravação/renomeação/exclusão de arquivos tiveram um aumento de 100% na atividade além da linha de base.

As evidências são baseadas em informações da proteção autônoma contra ransomware no ONTAP. Para obter detalhes, "[Visão geral da proteção autônoma contra ransomware](#)" consulte .

Um alerta pode ter um dos seguintes Estados:

- **Novo**
- **Inativo**

Um incidente de alerta é categorizado em um dos seguintes estados:

- **Novo:** Todos os incidentes são marcados como "novo" quando são identificados pela primeira vez.
- **Demitido:** Se você suspeitar que a atividade não é um ataque de ransomware, você pode alterar o status para "demitido".



Depois de descartar um ataque, você não pode alterar isso de volta. Se você ignorar um workload, todas as cópias Snapshot feitas automaticamente em resposta ao possível ataque de ransomware serão excluídas permanentemente.

- **Dismissing:** O incidente está em processo de desistência.
- **Resolvido:** O incidente foi mitigado.

Ver alertas

Você pode acessar alertas no Painel de proteção contra ransomware do BlueXP ou na guia **Alertas**.

Passos

1. No Painel de proteção contra ransomware do BlueXP , revise o painel Alertas.
2. Selecione **Ver tudo** em um dos Estados.
3. Clique num alerta para rever todos os incidentes em cada volume para cada alerta.
4. Para rever alertas adicionais, clique em **Alerta** no breadcrumbs no canto superior esquerdo.
5. Reveja os alertas na página Alertas.

Ransomware protection Dashboard Protection Alerts Recovery Reports Free trial (90 days)

6 Alerts 12 GiB Impacted data

Automated responses 9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
Alert9314	Fileshare_uswest_02_...	svm_cv...	File share	Active	aws-connector-us-we...	1	2 GiB	8 days ago
Alert8727	Oracle_8821		Oracle	Active	aws-connector-us-ea...	2	2 GiB	8 days ago
Alert9823	Oracle_9819		Oracle	Inactive	aws-connector-us-...	1	2 GiB	8 days ago
Alert3932	Mysql_9294		MySQL	Active	aws-connector-us-ea...	2	2 GiB	8 days ago
Alert7918	Vm_datastore_202_735...		VM datastore	Active	onprem-connec...	1	2 GiB	8 days ago
Alert5319	Vm_datastore_uswest_...		VM file share	Active	aws-connect...	1	2 GiB	8 days ago

6. Continuar:

- [\[Detect anomalous user behavior\]](#).
- [Marque os incidentes de ransomware como prontos para recuperação \(após os incidentes serem neutralizados\)](#).
- [Descarte incidentes que não sejam potenciais ataques](#).

Detectar atividades maliciosas e comportamento anômalo do usuário

Olhando para a guia Alertas, você pode identificar se há atividade maliciosa. Os detalhes que aparecem dependem de como o alerta foi acionado:

- Acionado pelo recurso Autonomous ransomware Protection no ONTAP. Isso detecta atividades maliciosas com base no comportamento dos arquivos no volume.
- Acionado por Data Infrastructure Insights Workload Security. Isso requer uma licença para a segurança de workload do Insights da infraestrutura de dados e que você a habilite na proteção contra ransomware do BlueXP . Esse recurso detecta um comportamento anômalo do usuário nos workloads de storage e permite que você bloqueie acesso adicional a esse usuário.

Para ativar a segurança de cargas de trabalho na proteção contra ransomware do BlueXP , vá para a página **Configurações** e selecione a opção **conexão de segurança de carga de trabalho**.

Para obter uma visão geral do Data Infrastructure Insights Workload Security, consulte "[Sobre o Workload Security](#)"



Se você não tiver uma licença para segurança de workload de infraestrutura de dados e não a ativar na proteção contra ransomware do BlueXP , não verá as informações anômalas de comportamento do usuário.

Quando ocorre atividade maliciosa, um alerta é gerado e um instantâneo automatizado é obtido.

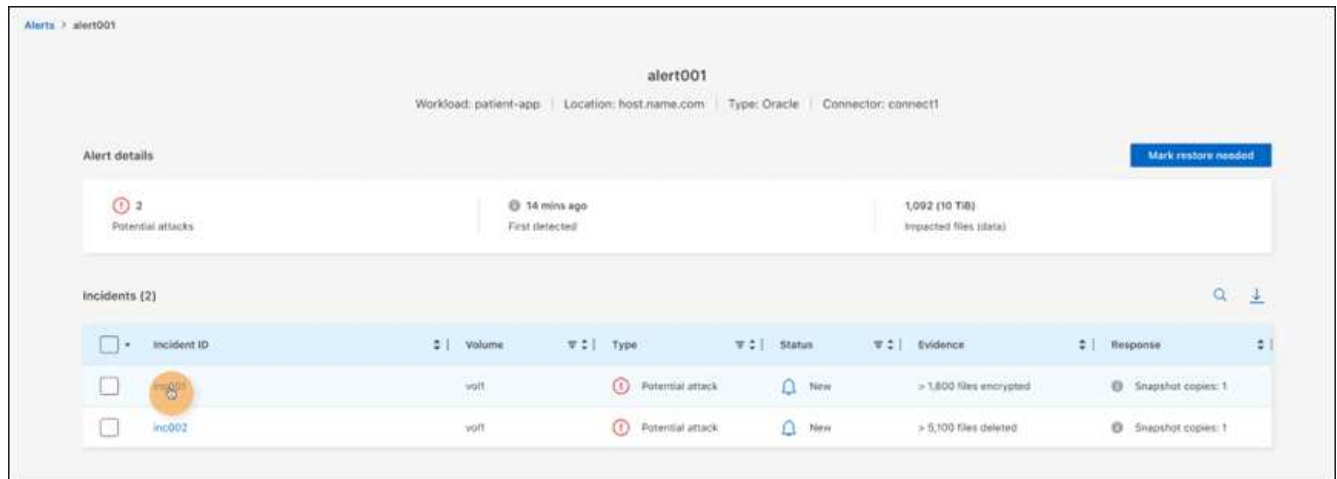
Visualizar apenas atividades maliciosas do Autonomous ransomware Protection

Quando o Autonomous ransomware Protection aciona um alerta na proteção contra ransomware do BlueXP , você pode visualizar os seguintes detalhes:

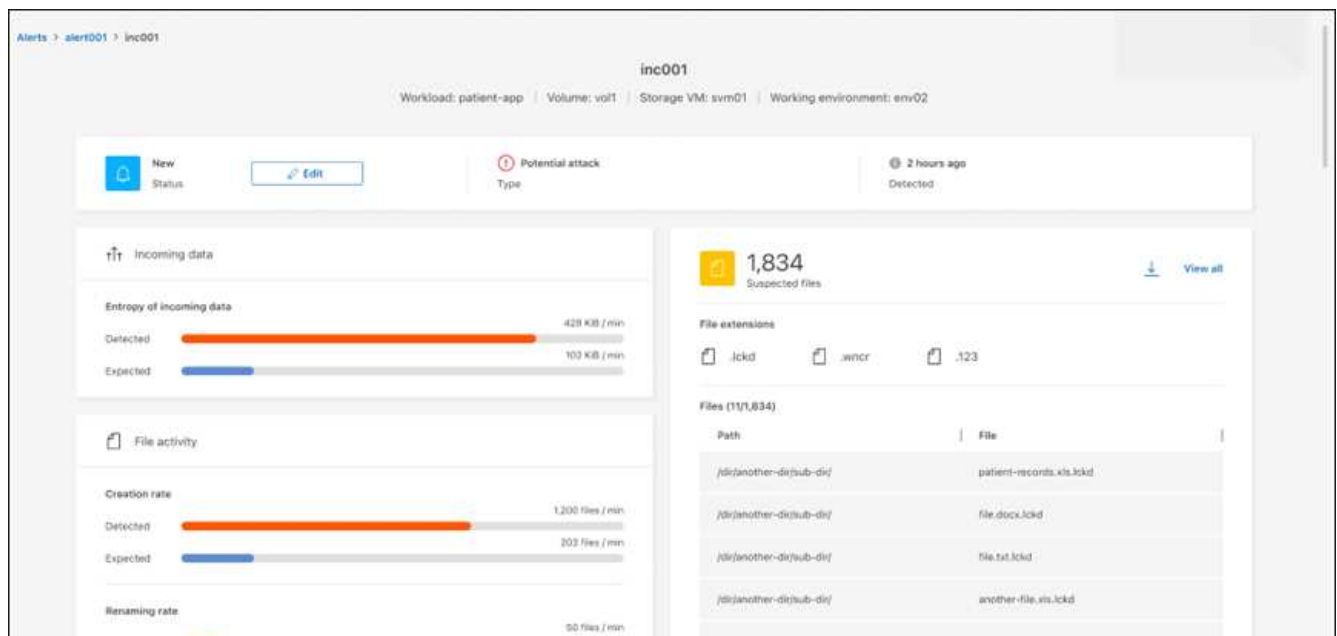
- Entropia de dados de entrada
- Taxa de criação esperada de novos arquivos em comparação com a taxa detetada
- Taxa de exclusão esperada de arquivos em comparação com a taxa detetada
- Taxa de renomeação esperada dos arquivos em comparação com a taxa detetada

Passos

1. No menu de proteção contra ransomware BlueXP , seleccione **Alertas**.
2. Seleccione um alerta.
3. Reveja os incidentes no alerta.



4. Seleccione um incidente para rever os detalhes do incidente.



Veja um comportamento anômalo do usuário no Data Infrastructure Insights Workload Security

Quando a segurança de workload aciona um alerta na proteção de ransomware do BlueXP , você pode visualizar o usuário suspeito, bloquear o usuário e investigar a atividade do usuário diretamente no sistema de segurança de workloads da infraestrutura de dados.



Esses recursos são além dos detalhes disponíveis no Just Autonomous ransomware Protection.

Antes de começar

Essa opção requer uma licença para segurança de workload do Insights da infraestrutura de dados e sua ativação na proteção contra ransomware do BlueXP .

Para habilitar a segurança de workloads na proteção contra ransomware do BlueXP , faça o seguinte:

1. Vá para a página **Configurações**.
2. Selecione a opção **conexão de segurança de carga de trabalho**.

Para obter detalhes, "[Configurar as configurações de proteção contra ransomware do BlueXP](#)" consulte .

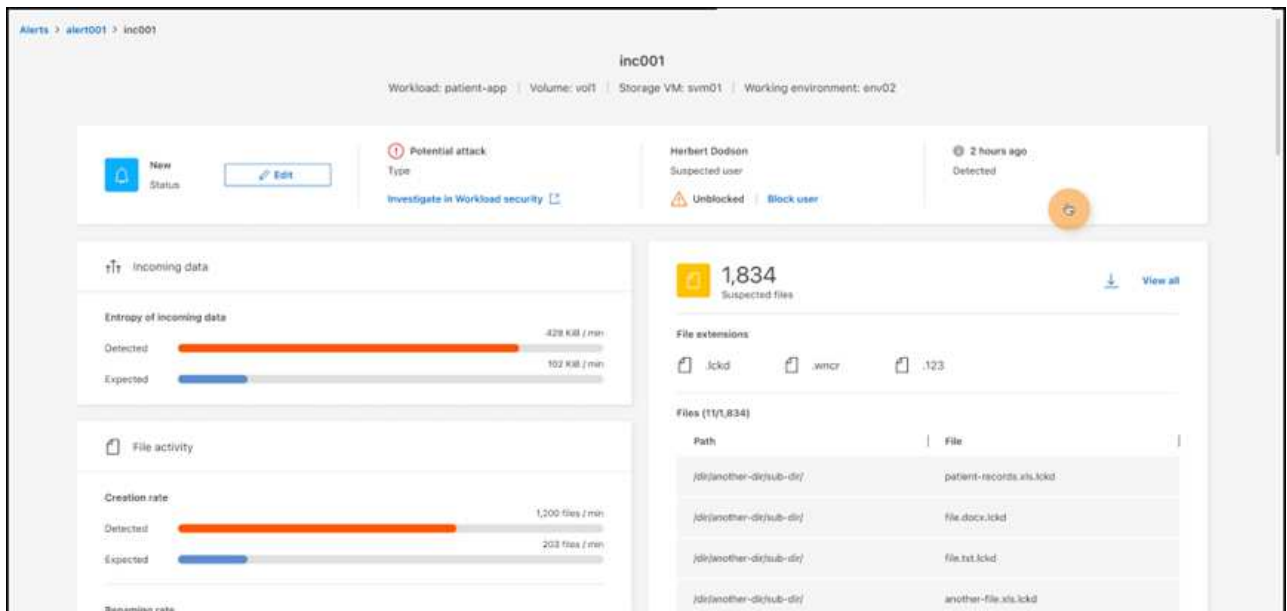
Passos

1. No menu de proteção contra ransomware BlueXP , selecione **Alertas**.
2. Selecione um alerta.
3. Reveja os incidentes no alerta.

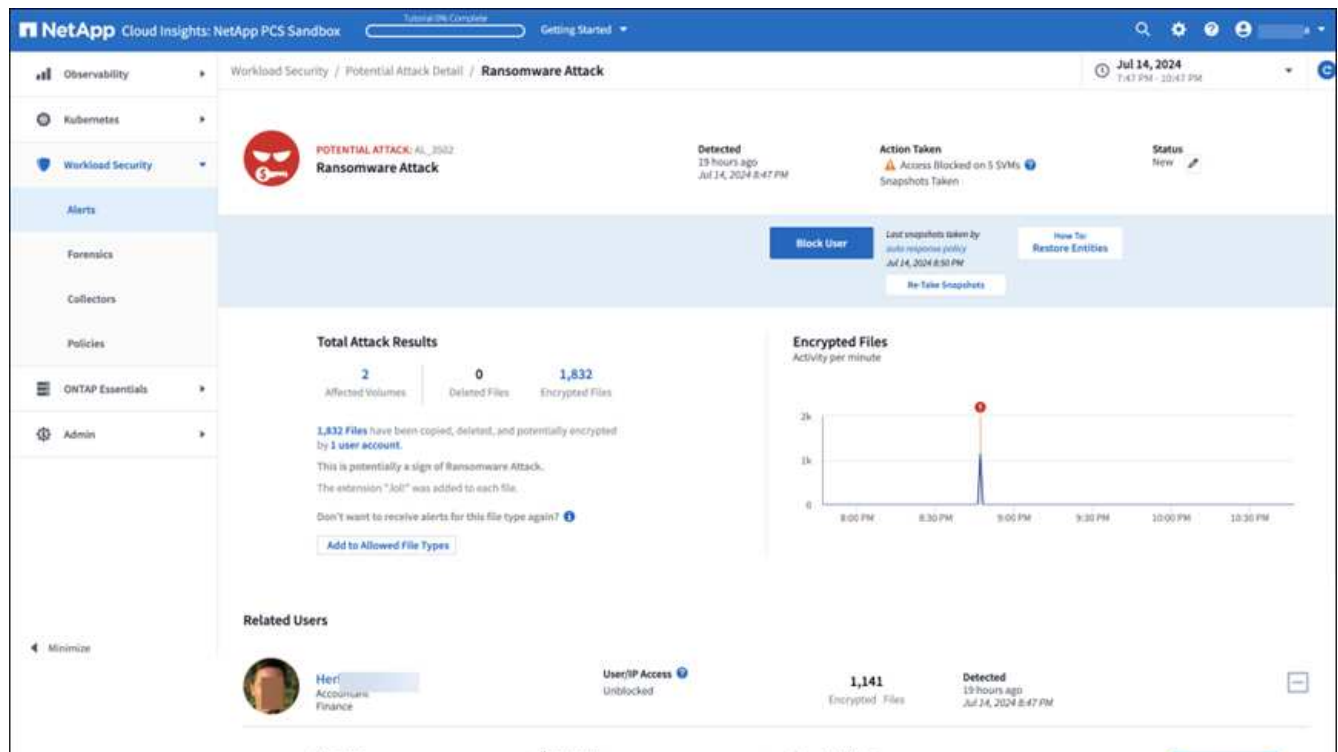
The screenshot displays the 'Alerts' page for 'alert001'. At the top, it shows metadata: Workload: patient-app, Location: host.name.com, Type: Oracle, and Connector: connect1. A blue button 'Mark restore needed' is visible. The 'Alert details' section includes: 2 Potential attacks, a link to 'Investigate in Workload security', a suspected user 'Herbert Dodson', a status of 'Unblocked' with a 'Block user' option, and a detection time of '14 mins ago'. It also notes '1,092 (10 TiB) Impacted files (data)'. Below this is a table of 'Incidents (2)'. The table has columns for Incident ID, Volume, Type, Status, Evidence, and Response.

Incident ID	Volume	Type	Status	Evidence	Response
inc001	vol1	Potential attack	New	> 1,800 files encrypted	Snapshot copies: 1
inc002	vol1	Potential attack	New	> 5,100 files deleted	Snapshot copies: 1

4. Para bloquear um usuário suspeito de acesso adicional em seu ambiente monitorado pelo BlueXP , selecione o link **Bloquear usuário**.
5. PESQUISE o alerta ou um incidente no alerta:
 - a. Para pesquisar o alerta ainda mais no Data Infrastructure Insights Workload Security, selecione o link **Investigate in Workload Security**.
 - b. Selecione um incidente para rever os detalhes do incidente.



O Data Infrastructure Insights Workload Security é aberto em uma nova guia.

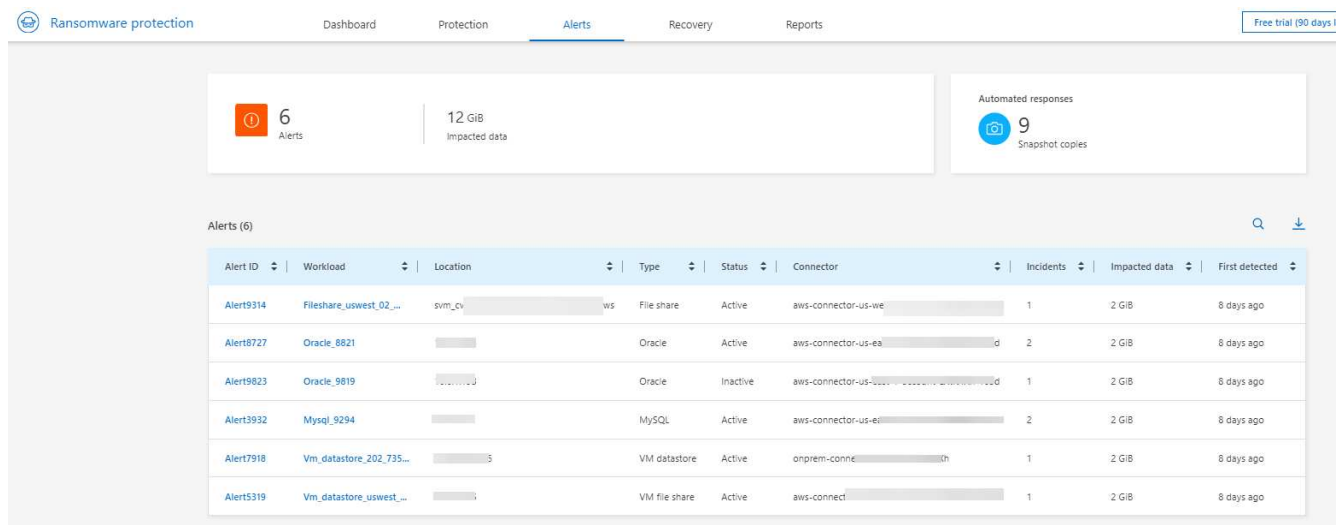


Marque os incidentes de ransomware como prontos para recuperação (após os incidentes serem neutralizados)

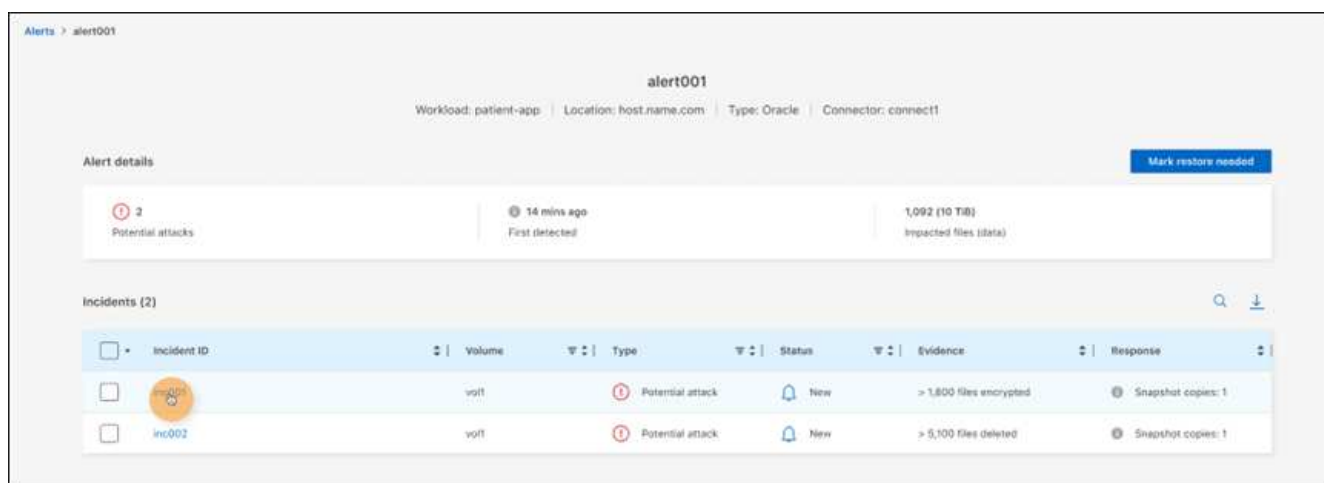
Depois de atenuar o ataque e estar pronto para recuperar cargas de trabalho, você deve se comunicar com sua equipe de administração de storage que os dados estão prontos para recuperação para que possam iniciar o processo de recuperação.

Passos

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



2. Na página Alertas, selecione o alerta.
3. Reveja os incidentes no alerta.



4. Se você determinar que os incidentes estão prontos para recuperação, selecione **Marcar restauração necessária**.
5. Confirme a ação e selecione **Marcar restauração necessária**.
6. Para iniciar a recuperação da carga de trabalho, selecione a carga de trabalho **Recover** na mensagem ou selecione a guia **Recovery**.

Resultado

Depois que o alerta é marcado para restauração, o alerta passa da guia Alertas para a guia recuperação.

Descarte incidentes que não sejam potenciais ataques

Depois de analisar incidentes, você precisa determinar se os incidentes são potenciais ataques. Se não, eles podem ser demitidos.

Você pode ignorar falsos positivos ou decidir recuperar seus dados imediatamente. Se você decidir ignorar o alerta, o serviço irá aprender esse comportamento e associá-lo a operações normais e não iniciar um alerta sobre tal comportamento novamente.

Se você ignorar um workload, todas as cópias Snapshot feitas automaticamente em resposta ao possível

ataque de ransomware serão excluídas permanentemente.



Se você ignorar um alerta, não poderá alterar esse status de volta para qualquer outro status e não poderá desfazer essa alteração.

Passos

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

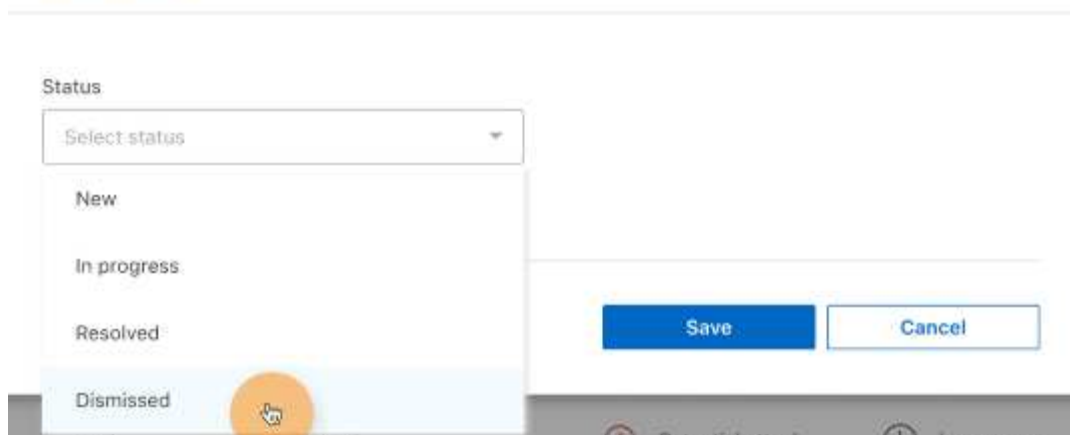
Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
Alert9314	Fileshare_uswest_02...	svm_cv...	File share	Active	aws-connector-us-we...	1	2 GiB	8 days ago
Alert8727	Oracle_8821		Oracle	Active	aws-connector-us-ea...	2	2 GiB	8 days ago
Alert9823	Oracle_9819		Oracle	Inactive	aws-connector-us-e...	1	2 GiB	8 days ago
Alert3932	Mysql_9294		MySQL	Active	aws-connector-us-e...	2	2 GiB	8 days ago
Alert7918	Vm_datastore_202_735...		VM datastore	Active	onprem-conne...	1	2 GiB	8 days ago
Alert5319	Vm_datastore_uswest_...		VM file share	Active	aws-connect...	1	2 GiB	8 days ago

2. Na página Alertas, selecione o alerta.

Incident ID	Volume	SVM	Working environ...	Type	Status	First detected	Evidence	Automated respon...
Inci1234	oracle	svm...	cvoa...	Potential attack	New	8 days ago	4 new extensions detect...	1 Snapshot copy

3. Selecione um ou mais incidentes. Ou selecione todos os incidentes selecionando a caixa ID do Incidente no canto superior esquerdo da tabela.
4. Se você determinar que o incidente não é uma ameaça, ignore-o como um falso positivo:
 - Selecione o incidente.
 - Selecione o botão **Editar status** acima da tabela.

Edit status



5. Na caixa Editar status, selecione o status "**demitido**".

São exibidas informações adicionais sobre o workload e quais cópias Snapshot serão excluídas.

6. Selecione **Guardar**.

O status sobre o incidente ou incidentes muda para "demitido".

Exibir uma lista de arquivos afetados

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, pode ver uma lista de ficheiros afetados. Pode aceder à página Alertas para transferir uma lista de ficheiros afetados. Em seguida, use a página recuperação para carregar a lista e escolher quais arquivos restaurar.

Passos

Use a página Alertas para recuperar a lista de arquivos afetados.



Se um volume tiver vários alertas, talvez seja necessário fazer o download da lista CSV de arquivos afetados para cada alerta.

1. No menu de proteção contra ransomware BlueXP , selecione **Alertas**.
2. Na página Alertas, classifique os resultados por workload para mostrar os alertas da carga de trabalho do aplicativo que você deseja restaurar.
3. Na lista de alertas para essa carga de trabalho, selecione um alerta.
4. Para esse alerta, selecione um único incidente.

The screenshot shows the BlueXP interface for an incident labeled 'inc1234'. At the top, it indicates 'Workload: Oracle_9819', 'Volume: orac...', 'SVM: svm...', and 'Working environment: cvo...'. The main area is divided into several sections:

- Status:** 'New Status' and 'Potential attack Type'.
- Incoming data:** Shows 'Entropy of incoming data' with 'Detected' as 'Not determined (learning in progress)' and 'Expected' as '26820 KiB / min'.
- File activity:** Shows 'Creation rate' with 'Detected' as 'Not determined (learning in progress)' and 'Expected' as '65 files / min'. It also shows 'Renaming rate' as 'Not determined (learning in progress)'.
- Impacted files (70):** A list of files with a search and download icon. The list includes:
 - New file extensions (4): .omg, .lck, .pck, .xyz
 - Suspect file extensions (4): .lck, .omg, .pck, .xyz
 - Impacted files list:
 - /Top_Dir_1/Sub_Dir_11/test_file_5007.1.omg
 - /Top_Dir_1/Sub_Dir_11/test_file_12372.2.lck
 - /Top_Dir_1/Sub_Dir_11/test_file_5007.1.lck

5. Para esse incidente, selecione o ícone de download e faça o download da lista de arquivos afetados no formato CSV.

Recuperar de um ataque de ransomware (após os incidentes serem neutralizados)

Depois que os workloads forem marcados como "Restauração necessária", a proteção contra ransomware da BlueXP recomenda um ponto de recuperação real (RPA) e orquestra o fluxo de trabalho para uma recuperação resistente a falhas.

- Se a aplicação ou VM for gerenciada pelo SnapCenter, a proteção contra ransomware do BlueXP restaura o aplicativo ou a VM de volta ao estado anterior e à última transação usando o processo consistente com aplicativos ou consistente com VMs. A restauração consistente com a aplicação ou VM adiciona aos dados no volume quaisquer dados que não os tenham transformado em storage, por exemplo, dados no cache ou em uma operação de e/S.
- Se o aplicativo ou VM for *não* gerenciado pelo SnapCenter e for gerenciado pelo backup e recuperação do BlueXP ou pela proteção contra ransomware do BlueXP, a proteção contra ransomware do BlueXP executará uma restauração consistente com falhas, onde todos os dados que estavam no volume no mesmo ponto de tempo serão restaurados, por exemplo, se o sistema falhar.

É possível restaurar o workload selecionando todos os volumes, volumes específicos ou arquivos específicos.



A recuperação do workload pode afetar os workloads em execução. Você deve coordenar os processos de recuperação com as partes interessadas apropriadas.

Uma carga de trabalho pode ter um dos seguintes status de restauração:

- **Restore needed:** A carga de trabalho precisa ser restaurada.
- **Em andamento:** A operação de restauração está em andamento.
- **Restaurado:** A carga de trabalho foi restaurada.

- **Falhou:** O processo de restauração da carga de trabalho não pôde ser concluído.

Veja os workloads que estão prontos para serem restaurados

Revise as cargas de trabalho que estão no status de recuperação "Restaurar necessário".

Passos

1. Execute um dos seguintes procedimentos:
 - No Painel, revise os totais "Restaurar necessário" no painel Alertas e selecione **Exibir tudo**.
 - No menu, selecione **recuperação**.
2. Revise as informações da carga de trabalho na página **recuperação**.

Workload	Location	Type	Connector	Managed by	Recovery status	Progress	Importance	Total data	Action
Mysql_9294	10.0.1.10	MySQL	aws-connector-us-east-1-...	None	Restore needed	n/a	Critical	2 GiB	Restore
Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-...	None	Restore needed	n/a	Critical	2 GiB	Restore
Fileshare_uswest_02_...	svm_cvoawswest01rpsde...	File share	aws-connector-us-west-1-...	None	Restore needed	n/a	Critical	2 GiB	Restore
Vm_datastore_202_735...	10.195.52.126	VM datastore	onprem-connector-accou...	SnapCenter for VMware	Restore needed	n/a	Standard	2 GiB	Restore
Vm_datastore_uswest_...	10.0.1.215	VM datastore	aws-connector-us-west-1-...	None	Restored	100%	Critical	2 GiB	Restore

Restaure um workload gerenciado pelo SnapCenter

Com a proteção contra ransomware do BlueXP , o administrador de storage pode determinar a melhor maneira de restaurar workloads a partir do ponto de restauração recomendado ou do ponto de restauração preferido.

O estado da aplicação muda se necessário para a restauração. O aplicativo será restaurado para o seu estado anterior a partir de arquivos de controle, se eles forem incluídos no backup. Após a conclusão da restauração, o aplicativo será aberto no modo LEITURA-GRAVAÇÃO.

Passos

1. No menu de proteção contra ransomware BlueXP , selecione **recuperação**.
2. Revise as informações da carga de trabalho na página **recuperação**.
3. Selecione uma carga de trabalho que esteja no estado "Restaurar necessário".
4. Para restaurar, selecione **Restaurar**.
5. **Restaurar escopo:** Consistente com aplicativos (ou para SnapCenter para VMs, o escopo de restauração é "por VM")
6. **Fonte:** Selecione a seta para baixo ao lado de fonte para ver os detalhes. Selecione o ponto de restauração que deseja usar para restaurar os dados.



A proteção contra ransomware do BlueXP identifica o melhor ponto de restauração como o backup mais recente pouco antes do incidente e mostra uma indicação "recomendada".

7. **Destino:** Selecione a seta para baixo ao lado de destino para ver os detalhes.
 - a. Selecione o local original ou alternativo.
 - b. Selecione o ambiente de trabalho.
 - c. Selecione a VM de armazenamento.
8. Se o destino original não tiver espaço suficiente para restaurar a carga de trabalho, será exibida uma linha de "armazenamento temporário". Você pode selecionar o armazenamento temporário para restaurar os dados da carga de trabalho. Os dados restaurados serão copiados do armazenamento temporário para o local original. Clique na seta **para baixo** na linha de armazenamento temporário e defina o cluster de destino, a VM de armazenamento e o nível local.
9. **Localização da quarentena:** Opcionalmente, selecione onde deseja armazenar dados potencialmente infetados antes de iniciar o processo de restauração para análise posterior após a recuperação.
10. Selecione **Guardar**.
11. Selecione **seguinte**.
12. Reveja as suas seleções.
13. Selecione **Restaurar**.
14. No menu superior, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Restaure um workload não gerenciado pelo SnapCenter

Com a proteção contra ransomware do BlueXP, o administrador de storage pode determinar a melhor maneira de restaurar workloads a partir do ponto de restauração recomendado ou do ponto de restauração preferido.

O administrador de armazenamento de segurança pode recuperar dados em diferentes níveis:

- Recuperação de todos os volumes
- Recupere uma aplicação no nível do volume ou no nível do ficheiro e da pasta.
- Recupere um compartilhamento de arquivos no nível de volume, diretório ou arquivo/pasta.
- Recupere de um datastore em um nível de VM.

O processo difere ligeiramente dependendo do tipo de carga de trabalho.

Passos

1. No menu de proteção contra ransomware BlueXP, selecione **recuperação**.
2. Revise as informações da carga de trabalho na página **recuperação**.
3. Selecione uma carga de trabalho que esteja no estado "Restaurar necessário".
4. Para restaurar, selecione **Restaurar**.
5. **Restore Scope:** Selecione o tipo de restauração que deseja concluir:
 - Todos os volumes
 - Por volume

- Por arquivo: Você pode especificar uma pasta ou arquivos únicos para restaurar.

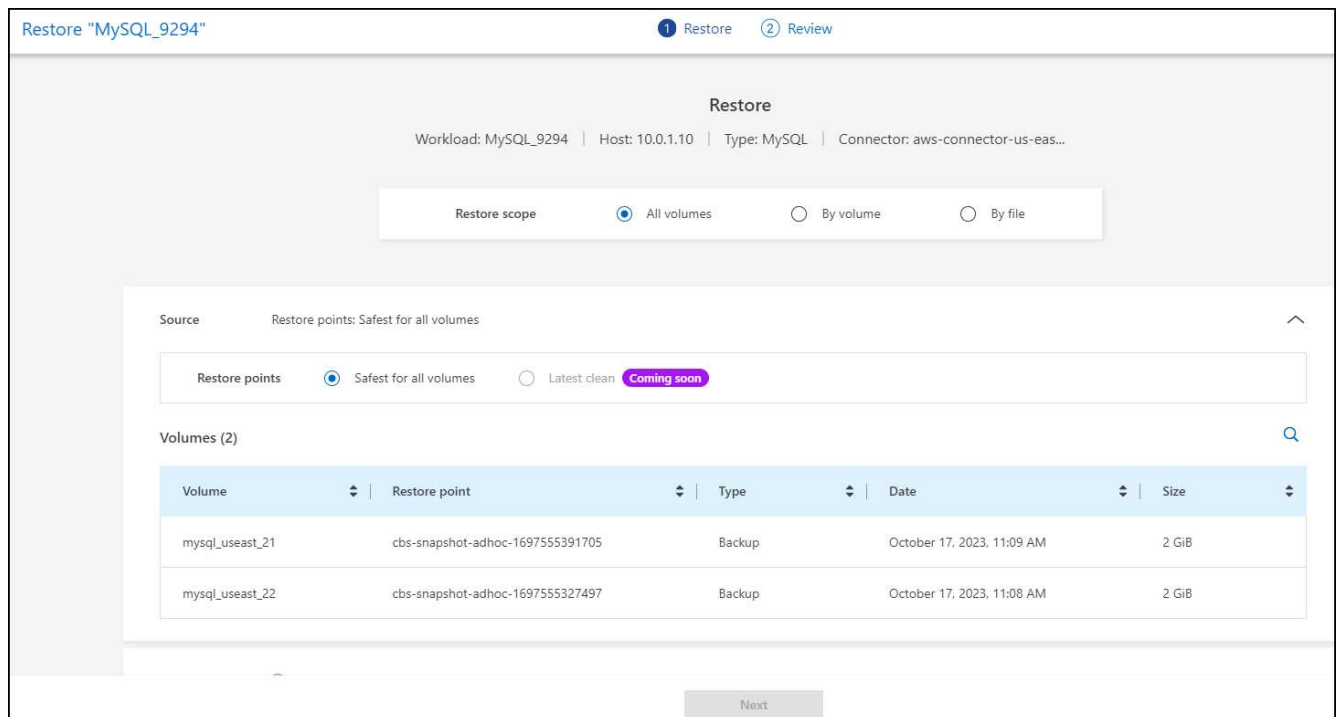


Pode selecionar até 100 ficheiros ou uma única pasta.

6. Continue com um dos procedimentos a seguir, dependendo se você escolheu o aplicativo, o volume ou o arquivo.

Restaurar todos os volumes

1. No menu de proteção contra ransomware BlueXP , selecione **recuperação**.
2. Selecione uma carga de trabalho que esteja no estado "Restaurar necessário".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no âmbito Restaurar, selecione **todos os volumes**.



5. **Fonte:** Selecione a seta para baixo ao lado de fonte para ver os detalhes.
 - a. Selecione o ponto de restauração que deseja usar para restaurar os dados.



A proteção contra ransomware do BlueXP identifica o melhor ponto de restauração como o backup mais recente imediatamente antes do incidente e mostra uma indicação "mais seguro para todos os volumes". Isso significa que todos os volumes serão restaurados para uma cópia antes do primeiro ataque ao primeiro volume detetado.

6. **Destino:** Selecione a seta para baixo ao lado de destino para ver os detalhes.
 - a. Selecione o ambiente de trabalho.
 - b. Selecione a VM de armazenamento.
 - c. Selecione o agregado.
 - d. Altere o prefixo de volume que será prepended para todos os novos volumes.

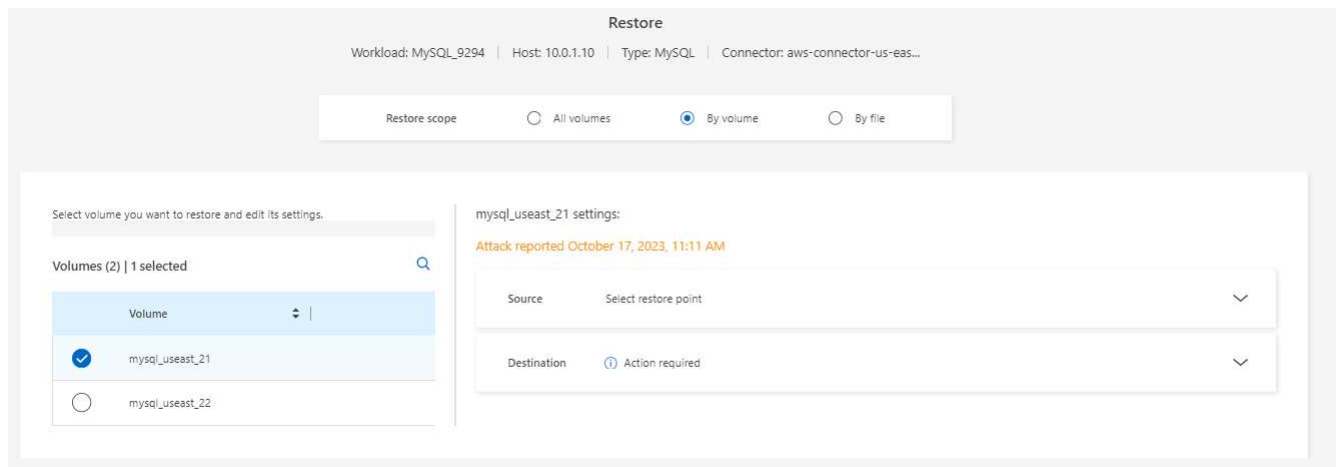


O novo nome do volume aparece como prefixo, nome do volume original, nome da cópia de segurança e data da cópia de segurança.

7. **Localização da quarentena:** Opcionalmente, selecione onde deseja armazenar dados potencialmente infectados antes de iniciar o processo de restauração para análise posterior após a recuperação.
8. Selecione **Guardar**.
9. Selecione **seguinte**.
10. Reveja as suas seleções.
11. Selecione **Restaurar**.
12. No menu superior, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Restaurar um workload de aplicação no nível de volume

1. No menu de proteção contra ransomware BlueXP , selecione **recuperação**.
2. Selecione uma carga de trabalho de aplicativo que esteja no estado "Restaurar necessário".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no âmbito Restaurar, selecione **por volume**.



5. Na lista de volumes, selecione o volume que deseja restaurar.
6. **Fonte:** Selecione a seta para baixo ao lado de fonte para ver os detalhes.
 - a. Selecione o ponto de restauração que deseja usar para restaurar os dados.



A proteção contra ransomware do BlueXP identifica o melhor ponto de restauração como o backup mais recente pouco antes do incidente e mostra uma indicação "recomendada".

7. **Destino:** Selecione a seta para baixo ao lado de destino para ver os detalhes.
 - a. Selecione o ambiente de trabalho.
 - b. Selecione a VM de armazenamento.
 - c. Selecione o agregado.
 - d. Reveja o novo nome do volume.



O novo nome do volume aparece como o nome do volume original, o nome da cópia de segurança e a data da cópia de segurança.

8. **Localização da quarentena:** Opcionalmente, selecione onde deseja armazenar dados potencialmente infectados antes de iniciar o processo de restauração para análise posterior após a recuperação.
9. Selecione **Guardar**.
10. Selecione **seguinte**.
11. Reveja as suas seleções.
12. Selecione **Restaurar**.
13. No menu superior, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Restaure um workload de aplicação no nível do arquivo

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, pode ver uma lista de ficheiros afetados. Pode aceder à página Alertas para transferir uma lista de ficheiros afetados. Em seguida, use a página recuperação para carregar a lista e escolher quais arquivos restaurar.

É possível restaurar um workload de aplicação no nível do arquivo para o mesmo ambiente de trabalho ou diferente.

Etapas para obter a lista de arquivos afetados

Use a página Alertas para recuperar a lista de arquivos afetados.



Se um volume tiver vários alertas, você precisará baixar a lista CSV de arquivos afetados para cada alerta.

1. No menu de proteção contra ransomware BlueXP , selecione **Alertas**.
2. Na página Alertas, classifique os resultados por workload para mostrar os alertas da carga de trabalho do aplicativo que você deseja restaurar.
3. Na lista de alertas para essa carga de trabalho, selecione um alerta.
4. Para esse alerta, selecione um único incidente.

5. Para ver a lista completa de arquivos, selecione **clique aqui** na parte superior do painel arquivos afetados.
6. Para esse incidente, selecione o ícone de download e faça o download da lista de arquivos afetados no formato CSV.

Passos para restaurar esses arquivos

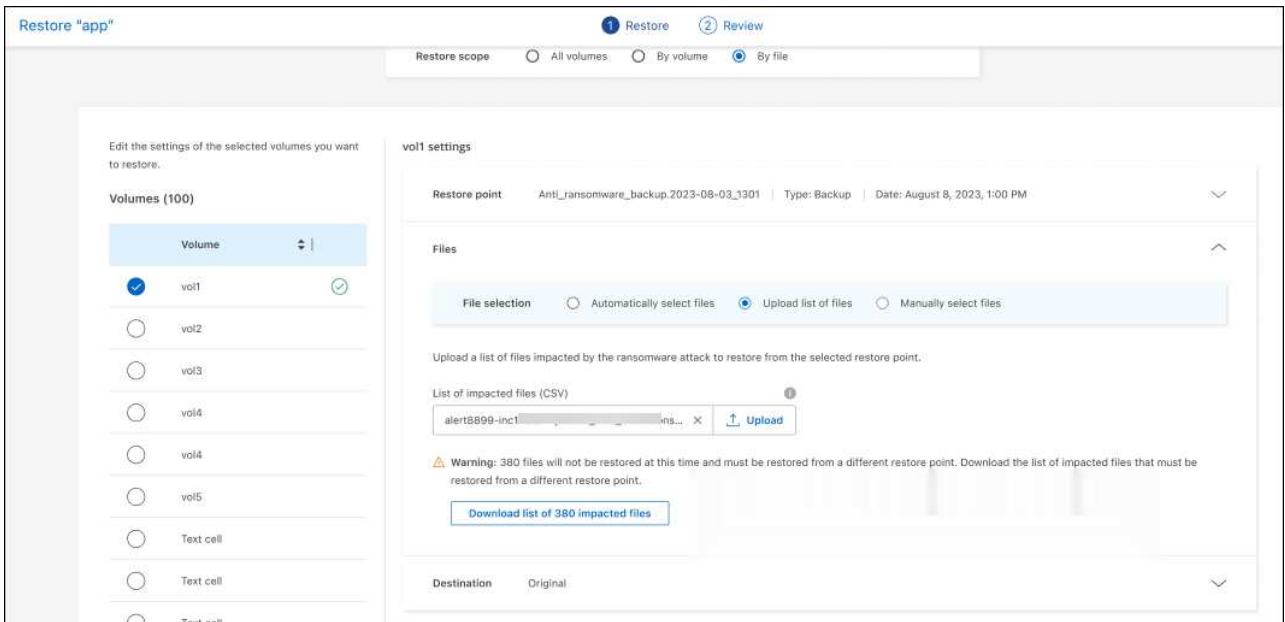
1. No menu de proteção contra ransomware BlueXP, selecione **recuperação**.
2. Selecione uma carga de trabalho de aplicativo que esteja no estado "Restaurar necessário".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no âmbito Restaurar, selecione **por ficheiro**.
5. Na lista de volumes, selecione o volume que contém os ficheiros que pretende restaurar.
6. **Ponto de restauração:** Selecione a seta para baixo ao lado de **ponto de restauração** para ver os detalhes. Selecione o ponto de restauração que deseja usar para restaurar os dados.



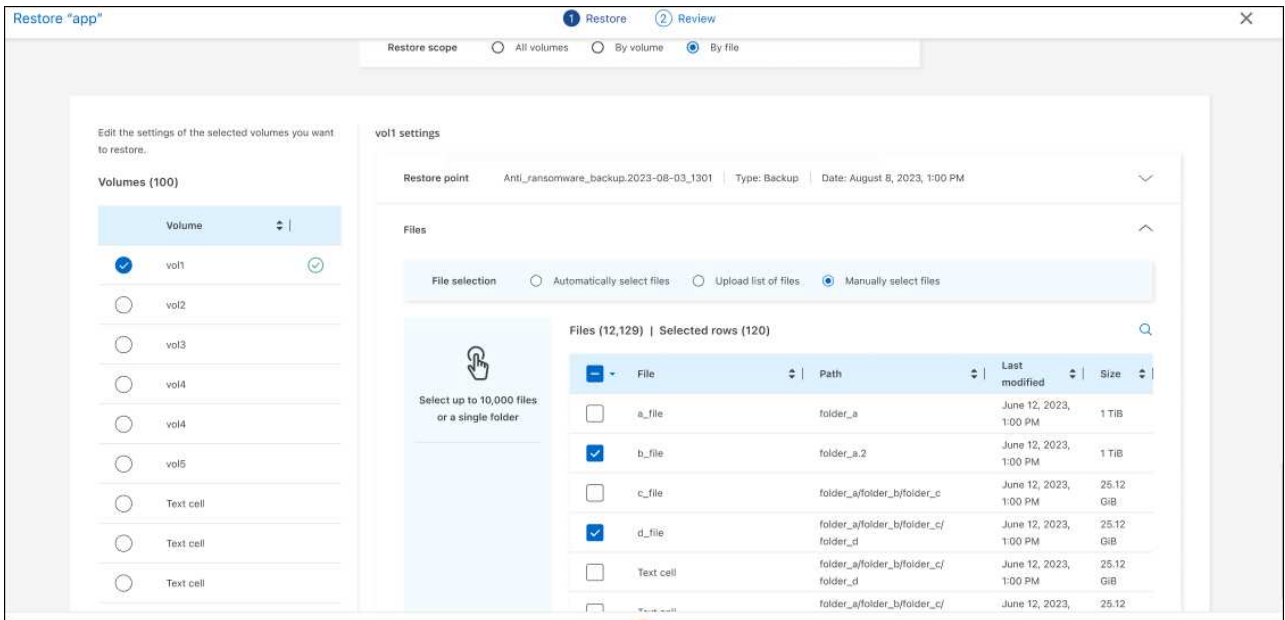
A coluna motivo no painel pontos de restauração mostra o motivo do instantâneo ou do backup como "resposta programada" ou "resposta automatizada a incidentes de ransomware".

7. Ficheiros:

- * **Selecione automaticamente arquivos*:** Deixe a proteção contra ransomware BlueXP selecionar os arquivos a serem restaurados.
- * **Carregar lista de arquivos*:** Carregue um arquivo CSV que contém a lista de arquivos afetados que você obteve da página Alertas ou que você tem. Você pode restaurar até 10.000 arquivos de cada vez.



- * Seleção manualmente arquivos*: Seleção até 10.000 arquivos ou uma única pasta para restaurar.



Se nenhum arquivo não puder ser restaurado usando o ponto de restauração selecionado, uma mensagem será exibida indicando o número de arquivos que não podem ser restaurados e permite que você baixe a lista desses arquivos selecionando **Download list of impacted files**.

8. **Destino:** Selecione a seta para baixo ao lado de destino para ver os detalhes.

- Escolha onde restaurar os dados: Local de origem original ou um local alternativo que você pode especificar.



Enquanto os arquivos originais ou diretório serão substituídos pelos dados restaurados, os nomes originais do arquivo e da pasta permanecerão os mesmos, a menos que você especifique novos nomes.

- b. Selecione o ambiente de trabalho.
- c. Selecione a VM de armazenamento.
- d. Opcionalmente, insira o caminho.



Se você não especificar um caminho para a restauração, os arquivos serão restaurados para um novo volume no diretório de nível superior.

- e. Selecione se pretende que os nomes dos ficheiros ou diretório restaurados sejam os mesmos nomes que a localização atual ou nomes diferentes.
9. **Localização da quarentena:** Opcionalmente, selecione onde deseja armazenar dados potencialmente infetados antes de iniciar o processo de restauração para análise posterior após a recuperação.
10. Selecione **seguinte**.
11. Reveja as suas seleções.
12. Selecione **Restaurar**.
13. No menu superior, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Restaure um compartilhamento de arquivos ou datastore

1. Depois de selecionar um compartilhamento de arquivos ou datastore para restaurar, na página Restaurar, no escopo de restauração, selecione **por volume**.

Restore "fileshare_uswest_02..."

1 Restore 2 Review

Restore scope: All volumes By volume By file

Select volume you want to restore and edit its settings:

Volume (1) | All selected

Volume

fileshare_uswest_02

fileshare_uswest_02 settings:

Attack reported October 17, 2023, 11:05 AM

Source: Select restore point

Destination: Action required

Define the alternate location where this volume will be restored. A new volume will be created in the selected working environment and SVM.

Working environment: Select working environment SVM: Select SVM Aggregate: Select aggregate

New volume name: vol1

Save

Next

2. Na lista de volumes, selecione o volume que deseja restaurar.
3. **Fonte:** Selecione a seta para baixo ao lado de fonte para ver os detalhes.
 - a. Selecione o ponto de restauração que deseja usar para restaurar os dados.



A proteção contra ransomware do BlueXP identifica o melhor ponto de restauração como o backup mais recente pouco antes do incidente e mostra uma indicação "recomendada".

4. **Destino:** Selecione a seta para baixo ao lado de destino para ver os detalhes.

- a. Escolha onde restaurar os dados: Local de origem original ou um local alternativo que você pode especificar.



Enquanto os arquivos originais ou diretório serão substituídos pelos dados restaurados, os nomes originais do arquivo e da pasta permanecerão os mesmos, a menos que você especifique novos nomes.

- b. Selecione o ambiente de trabalho.
- c. Selecione a VM de armazenamento.
- d. Opcionalmente, insira o caminho.



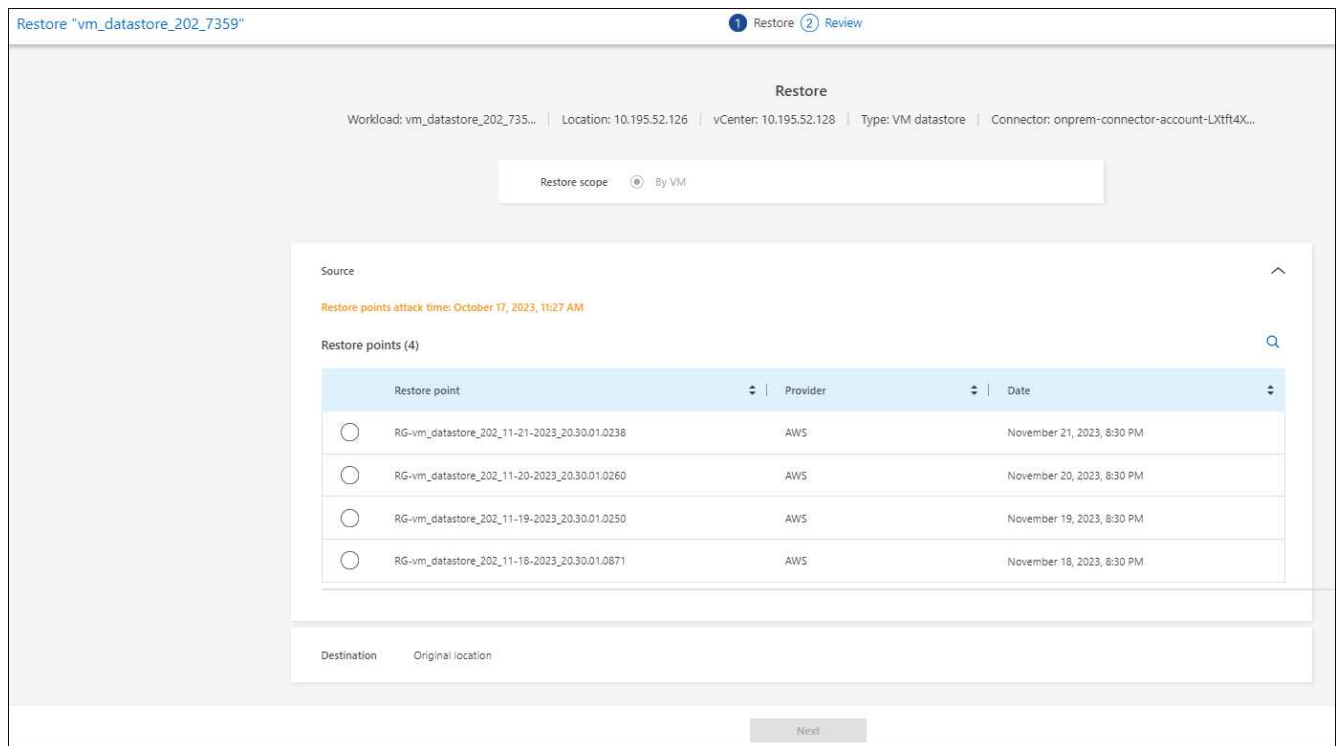
Se você não especificar um caminho para a restauração, os arquivos serão restaurados para um novo volume no diretório de nível superior.

5. Selecione **Guardar**.
6. Reveja as suas seleções.
7. Selecione **Restaurar**.
8. No menu, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Restaure um compartilhamento de arquivo VM no nível da VM

Na página recuperação depois de selecionar uma VM para restaurar, continue com estas etapas.

1. **Fonte:** Selecione a seta para baixo ao lado de fonte para ver os detalhes.



2. Selecione o ponto de restauração que deseja usar para restaurar os dados.
3. **Destino:** Para localização original.
4. Selecione **seguinte**.
5. Reveja as suas seleções.
6. Selecione **Restaurar**.
7. No menu, selecione **recuperação** para revisar a carga de trabalho na página recuperação onde o status da operação se move pelos estados.

Transferir relatórios

Você pode exportar dados de proteção e fazer o download dos arquivos CSV ou JSON que mostram detalhes de proteção, alertas e recuperação.

Antes de baixar os arquivos CSV ou JSON, você deve atualizar os dados, o que também atualiza os dados que aparecerão nos arquivos.

Você pode baixar arquivos de qualquer uma das opções do menu principal:

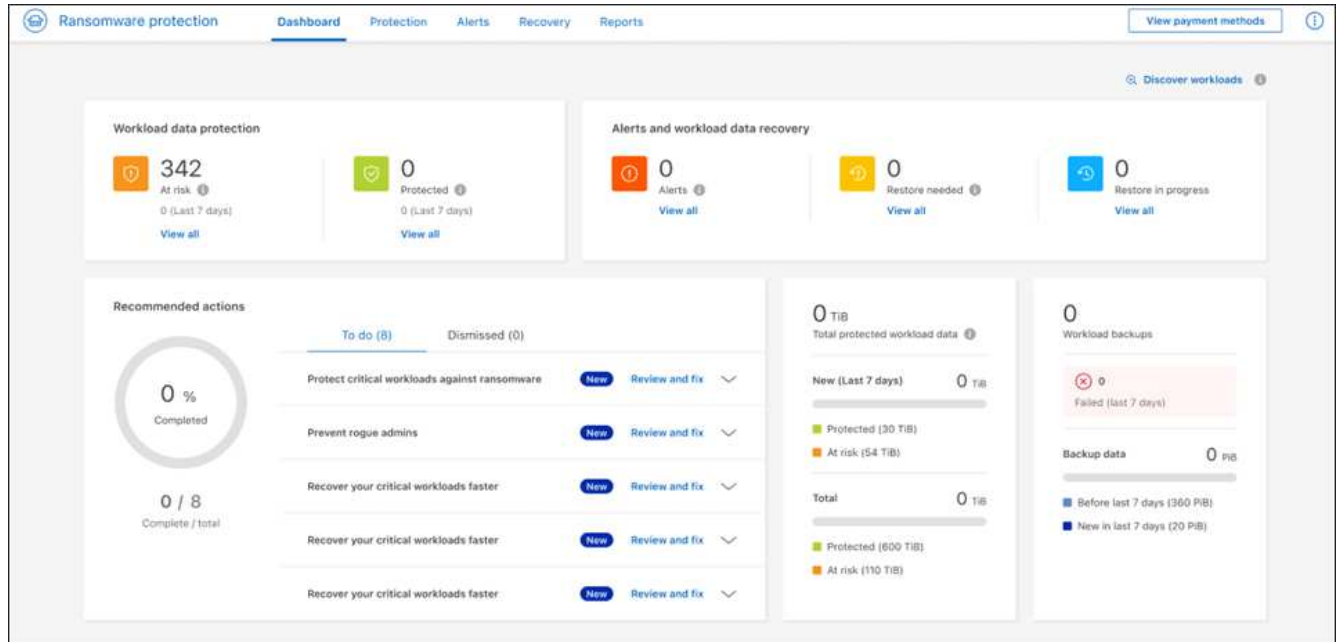
- **Proteção:** Contém o status e detalhes de todas as cargas de trabalho, incluindo o número total protegido e em risco.
- **Alertas:** Inclui o status e detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação:** Inclui o status e os detalhes de todas as cargas de trabalho que precisam ser restauradas, incluindo o número total de cargas de trabalho marcadas como "Restaurar necessário", "em andamento", "Restaurar falhou" e "restaurado com sucesso".
- **Relatórios:** Você pode exportar dados de qualquer uma das páginas e baixar os arquivos.



Se você baixar arquivos CSV da página proteção, Alertas ou recuperação, os dados mostram apenas os dados nessa página.

Os arquivos CSV incluem dados para todos os workloads em todos os ambientes de trabalho do BlueXP .

Passos

1. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.




2. No Painel de instrumentos ou em outra página, selecione a opção **Atualizar**  no canto superior direito para atualizar os dados que aparecerão nos relatórios.
3. Execute um dos seguintes procedimentos:
 - Na página, selecione a opção *Download*  .
 - No menu proteção contra ransomware do BlueXP , selecione **relatórios**.
4. Se você selecionou a opção **relatórios**, selecione um dos nomes de arquivo CSV pré-configurados e selecione **Download (CSV)** ou **Download (JSON)**.

Reports

Review protection status, alerts, and recovery details to monitor and maintain system health.

Ransomware protection details

 Last updated: April 30, 2024, 2:28 PM



Summary

Summary of RPS metrics for all workloads

[Download \(JSON\)](#)



Protection

Tabular details for all workloads that are at risk and protected

[Download \(CSV\)](#)



Alerts

Tabular details for all alerts

[Download \(CSV\)](#)



Recovery

Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored

[Download \(CSV\)](#)

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.