Documentação de proteção contra ransomware da BlueXP

BlueXP ransomware protection

NetApp
December 20, 2024

Índice

Documentação de proteção contra ransomware da BlueXP

Notas de lançamento

Novidades na proteção contra ransomware do BlueXP

Saiba o que há de novo na proteção contra ransomware do BlueXP .

16 de dezembro de 2024

Detecte um comportamento anômalo do usuário usando a segurança de workloads de storage do Data Infrastructure Insights

Com esta versão, você pode usar a segurança de workload de storage do Data Infrastructure Insights para detectar um comportamento incomum dos usuários em seus workloads de storage. Esse recurso ajuda você a identificar possíveis ameaças à segurança e bloquear usuários potencialmente maliciosos para proteger seus dados.

Para obter detalhes, "Responda a um alerta de ransomware detetado" consulte .

Antes de usar a segurança de workload de storage para detectar comportamento anômalo do usuário, você precisa configurar a opção usando a opção **Configurações** de proteção contra ransomware da BlueXP .

Consulte a "Configurar as configurações de proteção contra ransomware do BlueXP ".

Selecione workloads para descobrir e proteger

Com esta versão, agora você pode fazer o seguinte:

- Em cada conetor, selecione os ambientes de trabalho onde você deseja descobrir cargas de trabalho. Você pode se beneficiar desse recurso se quiser proteger cargas de trabalho específicas em seu ambiente e não em outros.
- Durante a descoberta do workload, é possível habilitar a detecção automática de workloads por conector. Esse recurso permite selecionar as cargas de trabalho que você deseja proteger.
- Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente.

Consulte a "Localizar workloads".

7 de novembro de 2024

Ativar a classificação de dados e procurar informações de identificação pessoal (PII)

Com essa versão, você pode habilitar a classificação do BlueXP , um componente essencial da família BlueXP , para verificar e classificar dados em seus workloads de compartilhamento de arquivos. A classificação de dados ajuda a identificar se os seus dados incluem informações pessoais ou privadas, o que pode aumentar os riscos de segurança. Esse processo também afeta a importância da carga de trabalho e ajuda a garantir que você esteja protegendo as cargas de trabalho com o nível certo de proteção.

A verificação de dados PII na proteção contra ransomware do BlueXP geralmente 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.

Consulte a "Configurar as configurações de proteção contra ransomware do BlueXP ".

Para iniciar a digitalização, na página proteção, clique em **Identify exposure** (identificar exposição à privacidade) na coluna Privacy exposure (exposição à privacidade).

"Procure dados confidenciais pessoalmente identificáveis com a classificação BlueXP ".

Integração SIEM com o Microsoft Sentinel

Agora você pode enviar dados para o seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e deteção de ameaças usando o Microsoft Sentinel. Anteriormente, você poderia selecionar o AWS Security Hub ou o Splunk Cloud como seu SIEM.

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

Teste gratuito agora 30 dias

Com esse lançamento, novas implantações de proteção contra ransomware do BlueXP agora têm 30 dias para uma avaliação gratuita. Anteriormente, a proteção contra ransomware da BlueXP forneceu 90 dias como uma avaliação gratuita. Se você já está no teste gratuito de 90 dias, essa oferta continua por 90 dias.

Restaure a carga de trabalho do aplicativo no nível do arquivo para o Podman

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode ver uma lista de ficheiros que podem ter sido afetados por um ataque e identificar os que pretende restaurar. Anteriormente, se os conetores BlueXP em uma organização (anteriormente uma conta) estavam usando o Podman, esse recurso foi desativado. Agora está habilitado para Podman. Você pode permitir que a proteção contra ransomware do BlueXP escolha os arquivos a serem restaurados, você pode carregar um arquivo CSV que lista todos os arquivos afetados por um alerta ou você pode identificar manualmente quais arquivos deseja restaurar.

"Saiba mais sobre como recuperar de um ataque de ransomware".

30 de setembro de 2024

Agrupamento personalizado de workloads de compartilhamento de arquivos

Com essa versão, agora você pode agrupar compartilhamentos de arquivos em grupos para facilitar a proteção do data Estate. O serviço pode proteger todos os volumes de um grupo ao mesmo tempo. Anteriormente, você precisava proteger cada volume separadamente.

"Saiba mais sobre como agrupar cargas de trabalho de compartilhamento de arquivos em estratégias de proteção contra ransomware".

2 de setembro de 2024

Avaliação de riscos de segurança do Digital Advisor

A proteção contra ransomware da BlueXP agora reúne informações sobre riscos de segurança altos e críticos relacionados a um cluster do consultor digital da NetApp. Se algum risco for encontrado, a proteção contra ransomware do BlueXP fornece uma recomendação no painel **ações recomendadas** do Painel: "Corrigir uma vulnerabilidade de segurança conhecida no cluster <name>." A partir da recomendação no Dashboard, clicar em **Review and FIX** sugere rever o Digital Advisor e um artigo CVE (Common Vulnerability & Exposure) para resolver o risco de segurança. Se houver vários riscos de segurança, revise as informações no Digital Advisor.

Consulte a "Documentação do Digital Advisor".

Faça backup do Google Cloud Platform

Com essa versão, você pode definir um destino de backup para um bucket do Google Cloud Platform. Anteriormente, você poderia adicionar destinos de backup apenas ao NetApp StorageGRID, Amazon Web Services e Microsoft Azure.

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

Suporte para o Google Cloud Platform

O serviço agora oferece suporte ao Cloud Volumes ONTAP para proteção de storage. Anteriormente, o serviço suportava apenas o Cloud Volumes ONTAP para Amazon Web Services e o Microsoft Azure, juntamente com nas no local.

"Saiba mais sobre a proteção contra ransomware da BlueXP e fontes de dados compatíveis, destinos de backup e ambientes de trabalho".

Controles de acesso baseados em função

Agora é possível limitar o acesso a atividades específicas com o controle de acesso baseado em funções (RBAC). A proteção contra ransomware do BlueXP usa duas funções do BlueXP : Administrador de conta do BlueXP e administrador não-conta (visualizador).

Para obter detalhes sobre as ações que cada função pode executar, "Controles de acesso baseados em função Privileges" consulte .

5 de agosto de 2024

Detecção de ameaças com o Splunk Cloud

Você pode enviar dados automaticamente para o seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e deteção de ameaças. Com versões anteriores, você pode selecionar apenas o AWS Security Hub como seu SIEM. Com essa versão, você pode selecionar o AWS Security Hub ou o Splunk Cloud como seu SIEM.

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

1 de julho de 2024

Traga sua própria licença (BYOL)

Com esta versão, você pode usar uma licença BYOL, que é um arquivo de licença NetApp (NLF) que você obtém de seu representante de vendas da NetApp

"Saiba mais sobre como configurar o licenciamento".

Restaure o workload do aplicativo no nível do arquivo

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode ver uma lista de ficheiros que podem ter sido afetados por um ataque e identificar os que pretende restaurar. Você pode permitir que a proteção contra ransomware do BlueXP escolha os arquivos a serem restaurados, você pode carregar um arquivo CSV que lista todos os arquivos afetados por um alerta ou você pode identificar

manualmente quais arquivos deseja restaurar.

> Com esta versão, se todos os conetores BlueXP em uma conta não estiverem usando Podman, o recurso de restauração de arquivo único será ativado. Caso contrário, ele será desativado para essa conta.

"Saiba mais sobre como recuperar de um ataque de ransomware".

Faça o download de uma lista de arquivos afetados

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode aceder à página Alertas para transferir uma lista de ficheiros afetados num ficheiro CSV e, em seguida, utilizar a página recuperação para carregar o ficheiro CSV.

"Saiba mais sobre como baixar arquivos afetados antes de restaurar um aplicativo".

Eliminar plano de proteçãoão

Com essa versão, agora você pode excluir uma estratégia de proteção contra ransomware.

"Saiba mais sobre como proteger cargas de trabalho e gerenciar estratégias de proteção contra ransomware".

10 de junho de 2024

Bloqueio de cópias snapshot no storage primário

Isso permite bloquear as cópias Snapshot no storage primário para que elas não possam ser modificadas ou excluídas por um determinado período, mesmo que um ataque de ransomware gerencie seu caminho até o destino do storage de backup.

"Saiba mais sobre como proteger cargas de trabalho e ativar o bloqueio de backup em uma estratégia de proteção contra ransomware".

Suporte para Cloud Volumes ONTAP para Microsoft Azure

Esta versão oferece suporte ao Cloud Volumes ONTAP para Microsoft Azure como um ambiente de trabalho, além do Cloud Volumes ONTAP para AWS e do ONTAP nas local.

"Início rápido para Cloud Volumes ONTAP no Azure"

"Saiba mais sobre a proteção contra ransomware BlueXP ".

Microsoft Azure adicionado como destino de backup

Agora você pode adicionar o Microsoft Azure como um destino de backup junto com a AWS e o NetApp StorageGRID.

"Saiba mais sobre como configurar as configurações de proteção".

14 de maio de 2024

Atualizações de licenciamento

Você pode se inscrever para uma avaliação gratuita de 90 dias. Em breve, você poderá comprar uma assinatura paga conforme o uso com o mercado de Serviços Web da Amazon ou trazer sua própria licença do NetApp.

"Saiba mais sobre como configurar o licenciamento".

Protocolo CIFS

O serviço agora é compatível com ONTAP e Cloud Volumes ONTAP no local em ambientes de trabalho da AWS usando protocolos NFS e CIFS. A versão anterior era compatível apenas com o protocolo NFS.

Detalhes do workload

Esta versão agora fornece mais detalhes nas informações de carga de trabalho das páginas proteção e outras para uma avaliação melhorada da proteção da carga de trabalho. Nos detalhes do workload, você pode revisar a política atribuída no momento e revisar os destinos de backup configurados.

"Saiba mais sobre como visualizar os detalhes da carga de trabalho nas páginas proteção".

Proteção e recuperação consistentes com aplicações e VM

Agora, você pode executar proteção consistente com aplicações com o software NetApp SnapCenter e a proteção consistente com VM com o plug-in SnapCenter para VMware vSphere, obtendo um estado inativo e consistente para evitar a perda de dados em potencial mais tarde se a recuperação for necessária. Se a recuperação for necessária, você poderá restaurar o aplicativo ou a VM de volta para qualquer um dos estados disponíveis anteriormente.

"Saiba mais sobre como proteger cargas de trabalho".

Estratégias de proteção contra ransomware

Se as políticas Snapshot ou Backup não existirem no workload, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas neste serviço:

- Política do Snapshot
- Política de backup
- Política de deteção

"Saiba mais sobre como proteger cargas de trabalho".

Detecção de ameaças

Ativar deteção de ameaças agora está disponível usando um sistema de gerenciamento de eventos e segurança de terceiros (SIEM). O Dashboard agora mostra uma nova recomendação para "habilitar a deteção de ameaças", que pode ser configurada na página Configurações.

"Saiba mais sobre como configurar as opções de Configurações".

Ignorar alertas falsos positivos

Na guia Alertas, agora você pode descartar falsos positivos ou decidir recuperar seus dados imediatamente.

"Saiba mais sobre como responder a um alerta de ransomware".

Estado de deteção

Novos status de detecção aparecem na página proteção mostrando o status da detecção de ransomware aplicada à carga de trabalho.

"Saiba mais sobre como proteger cargas de trabalho e visualizar status de proteção".

Faça o download de arquivos CSV

Você pode baixar arquivos CSV* nas páginas proteção, Alertas e recuperação.

"Saiba mais sobre como baixar arquivos CSV do Painel de Controle e outras páginas".

Link de documentação

O link Exibir documentação agora está incluído na interface do usuário. Você pode acessar esta documentação a partir da opção Dashboard vertical **actions***  **. Selecione *Novidades** para visualizar detalhes nas Notas de versão ou **Documentação** para visualizar a página inicial da documentação de proteção contra ransomware do BlueXP .

Backup e recuperação do BlueXP

O serviço de backup e recuperação do BlueXP já não precisa estar habilitado no ambiente de trabalho. "pré-requisitos"Consulte . O serviço de proteção contra ransomware do BlueXP ajuda a configurar um destino de backup por meio da opção Configurações. "Configure as definições"Consulte .

Opção de definições

Agora você pode configurar destinos de backup nas Configurações de proteção contra ransomware do BlueXP .

"Saiba mais sobre como configurar as opções de Configurações".

5 de março de 2024

Gestão da política de proteção

Além de usar políticas predefinidas, agora você pode criar políticas. "Saiba mais sobre como gerenciar políticas".

Imutabilidade no armazenamento secundário (DataLock)

Agora você pode tornar o backup imutável no storage secundário usando a tecnologia NetApp DataLock no armazenamento de objetos. "Saiba mais sobre como criar políticas de proteção".

Backup automático para NetApp StorageGRID

Além de usar a AWS, agora você pode escolher o StorageGRID como destino de backup. "Saiba mais sobre como configurar destinos de backup".

Recursos adicionais para investigar possíveis ataques

Agora você pode ver mais detalhes forenses para investigar o potencial ataque detetado. "Saiba mais sobre como responder a um alerta de ransomware detetado".

Processo de recuperação

O processo de recuperação foi aprimorado. Agora, você pode recuperar volume por volume ou todos os volumes para um workload. "Saiba mais sobre como recuperar de um ataque de ransomware (após os incidentes terem sido neutralizados)".

"Saiba mais sobre a proteção contra ransomware BlueXP ".

6 de outubro de 2023

O serviço de proteção contra ransomware da BlueXP é uma solução SaaS para proteger dados, detectar possíveis ataques e recuperar dados de um ataque de ransomware.

Para a versão de visualização, o serviço protege workloads baseados em aplicações de Oracle, MySQL, armazenamentos de dados de VM e compartilhamentos de arquivos no storage nas local, bem como o Cloud Volumes ONTAP na AWS (usando o protocolo NFS) em organizações da BlueXP individualmente e faz o backup dos dados no storage de nuvem da Amazon Web Services.

O serviço de proteção contra ransomware da BlueXP fornece uso completo de várias tecnologias NetApp para que seu administrador de segurança ou engenheiro de operações de segurança de dados possam atingir as seguintes metas:

- Visualizar rapidamente a proteção contra ransomware em todos os seus workloads.
- Tenha insights sobre as recomendações de proteção de ransomware
- Melhorar a postura de proteção com base nas recomendações de proteção contra ransomware da BlueXP .
- Atribua políticas de proteção contra ransomware para proteger seus principais workloads e dados de alto risco contra ataques de ransomware.
- Monitore a integridade dos workloads contra ataques de ransomware em busca de anomalias de dados.
- Avalie rapidamente o impactos de incidentes de ransomware em sua carga de trabalho.
- Recupere de incidentes de ransomware de forma inteligente, restaurando os dados e garantindo que a reinfeção dos dados armazenados não ocorra.

"Saiba mais sobre a proteção contra ransomware BlueXP ".

Comece agora

Saiba mais sobre a proteção contra ransomware BlueXP

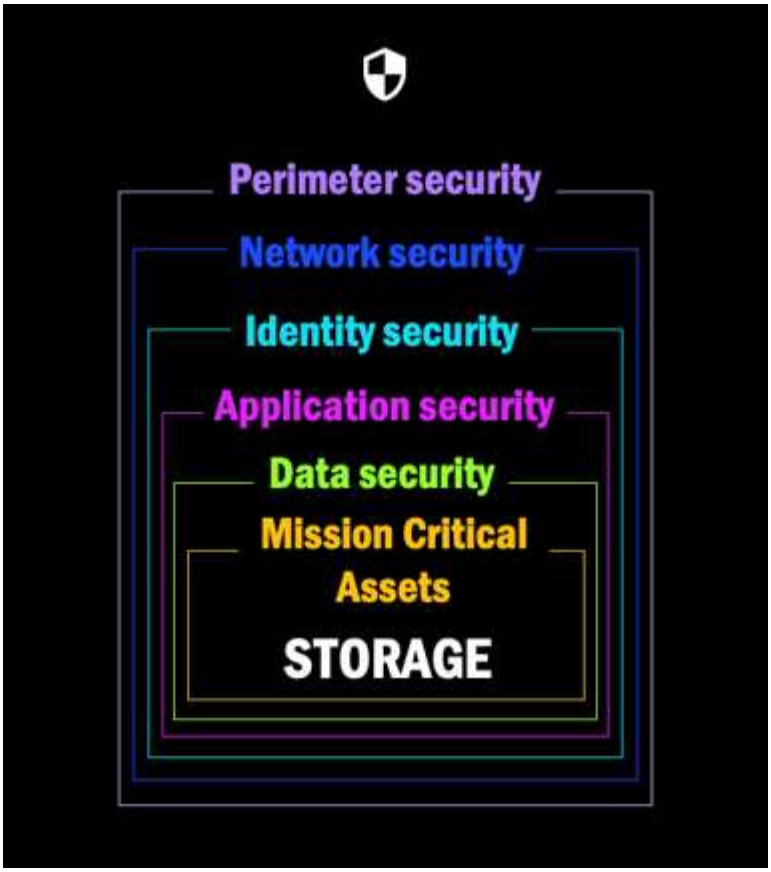
Os ataques de ransomware podem bloquear o acesso aos seus dados e os invasores podem pedir resgate em troca da liberação de dados ou descriptografia. De acordo com a IDC, não é incomum que as vítimas de ransomware sofram vários ataques de ransomware. O ataque pode interromper o acesso aos dados entre um dia e várias semanas.

A proteção contra ransomware da BlueXP é um serviço que protege seus dados contra ransomware. O serviço protege workloads baseados em aplicações de Oracle, MySQL, armazenamentos de dados de VM e compartilhamentos de arquivos no storage nas local (usando os protocolos NFS e CIFS), bem como o Cloud Volumes ONTAP para Amazon Web Services, Cloud Volumes ONTAP para Google Cloud e Cloud Volumes ONTAP para Microsoft Azure em organizações BlueXP . O serviço faz backup dos dados para o Amazon Web Services, o Google Cloud, o storage de nuvem Microsoft Azure e o NetApp StorageGRID.

Proteção contra ransomware na camada de dados

Sua postura de segurança normalmente abrange várias camadas de defesa para proteger contra uma variedade de ameaças cibernéticas.

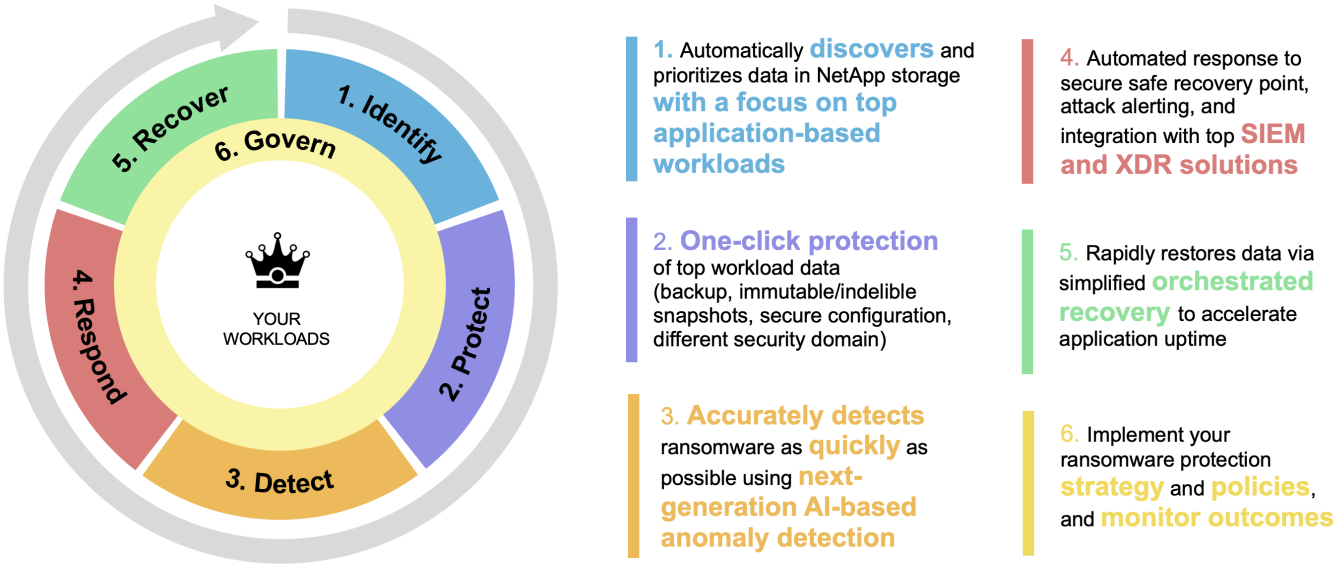
- * Camada externa*: Esta é a sua primeira linha de defesa usando firewalls, sistemas de deteção de intrusão e redes privadas virtuais para proteger os limites da rede.
- **Segurança de rede**: Esta camada baseia-se na base com segmentação de rede, monitoramento de tráfego e criptografia.
- **Segurança de identidade**: Usa métodos de autenticação, controles de acesso e gerenciamento de identidade para garantir que somente usuários autorizados possam acessar recursos confidenciais.
- **Segurança de aplicativos**: Protege aplicativos de software usando práticas seguras de codificação, testes de segurança e autoproteção de aplicativos em tempo de execução.
- **Segurança de dados**: Protege seus dados com proteção de dados, backups e estratégias de recuperação. A proteção contra ransomware da BlueXP opera nessa camada.



O que você pode fazer com a proteção contra ransomware do BlueXP

O serviço de proteção contra ransomware do BlueXP fornece uso completo de várias tecnologias NetApp para que seu administrador de storage, administrador de segurança de dados ou engenheiro de operações de segurança possam cumprir as seguintes metas:

- **Identifique** todos os workloads gerenciados em NetApp on-premises nas com NFS ou ambientes de trabalho CIFS na BlueXP , em organizações BlueXP , projetos e conetores BlueXP baseados em aplicações, compartilhamento de arquivos ou VMware. Em seguida, o serviço categoriza a prioridade de dados e fornece recomendações para melhorias na proteção de ransomware.
- * Proteja* suas cargas de trabalho habilitando backups, cópias Snapshot e estratégias de proteção contra ransomware em seus dados.
- Nota de rodapé: Embora seja possível que um ataque não seja detetado, nossa pesquisa indica que a tecnologia NetApp resultou em um alto grau de deteção para certos ataques de ransomware baseados em criptografia de arquivos.]
- **Responda** a potenciais ataques de ransomware iniciando automaticamente um instantâneo NetApp ONTAP inviolável que está bloqueado para que a cópia não possa ser excluída acidentalmente ou maliciosamente. Seus dados de backup permanecerão imutáveis e protegidos de ponta a ponta contra ataques de ransomware na origem e no destino.
- **Recupere** suas cargas de trabalho que ajudam a acelerar o tempo de atividade da carga de trabalho orquestrando várias tecnologias NetApp. Você pode optar por recuperar volumes específicos. O serviço fornece recomendações sobre as melhores opções.
- **Governar**: Implemente sua estratégia de proteção contra ransomware e monitore os resultados.



Benefícios de usar a proteção contra ransomware do BlueXP

A proteção contra ransomware da BlueXP oferece os seguintes benefícios:

- Detecta cargas de trabalho e seus cronogramas de snapshot e backup existentes e classifica sua importância relativa.
- Avalia sua postura de proteção contra ransomware e a exibe em um painel fácil de entender.
- Fornece recomendações sobre as próximas etapas com base na análise da postura de descoberta e proteção.
- Aplica recomendações de proteção de dados orientada por IA/ML com acesso a um clique.
- Protege dados nos principais workloads baseados em aplicações, como MySQL, Oracle, VMware datastores e compartilhamentos de arquivos.
- Detecta ataques de ransomware a dados em tempo real no storage primário usando a tecnologia de AI.
- Inicia ações automatizadas em resposta a possíveis ataques detetados, criando cópias Snapshot e iniciando alertas sobre atividades anormais.
- Aplica recuperação selecionada para atender às políticas de RPO. A proteção contra ransomware do BlueXP orquestra a recuperação de incidentes de ransomware usando vários serviços de recuperação do NetApp, incluindo o backup e a recuperação do BlueXP (antigo backup em nuvem) e o SnapCenter.
- Usa o controle de acesso baseado em função (RBAC) para controlar o acesso a recursos e operações do serviço, o que aumenta a segurança.

Custo

O NetApp não cobra pelo uso da versão de avaliação da proteção contra ransomware do BlueXP .

Com o lançamento de outubro de 2024, novas implantações de proteção contra ransomware BlueXP têm 30 dias para uma avaliação gratuita. Anteriormente, a proteção contra ransomware da BlueXP forneceu 90 dias como uma avaliação gratuita. Se você já está no teste gratuito de 90 dias, essa oferta continua por 90 dias.

Se você tiver backup e recuperação do BlueXP e proteção contra ransomware BlueXP , todos os dados

comuns protegidos por ambos os produtos serão cobrados apenas pela proteção contra ransomware do BlueXP .

Depois de comprar uma licença ou uma assinatura do PayGo, qualquer workload que tenha uma política de detecção de ransomware (proteção autônoma contra ransomware) habilitada (descoberta ou definida pela proteção contra ransomware do BlueXP) e pelo menos uma política de snapshot ou backup, a proteção contra ransomware do BlueXP classifica-a como "protegida" e conta com relação à capacidade adquirida ou à assinatura do PayGo. Se uma carga de trabalho for descoberta sem uma diretiva de deteção (ARP), mesmo que tenha políticas de backup ou snapshot, ela será classificada como "em risco" e *não* conta em relação à capacidade adquirida.

Workloads protegidos contam com a capacidade adquirida ou com a assinatura após o término do período de teste de 90 dias. A proteção contra ransomware da BlueXP é cobrada por GB pelos dados associados a workloads protegidos antes de serem eficientes.

Licenciamento

Com a proteção contra ransomware do BlueXP , você pode usar diferentes planos de licenciamento, incluindo uma avaliação gratuita, uma assinatura paga conforme o uso em breve ou trazer sua própria licença.

O serviço de proteção contra ransomware do BlueXP requer uma licença do NetApp ONTAP One.

A licença de proteção contra ransomware da BlueXP não inclui produtos NetApp adicionais. A proteção contra ransomware do BlueXP pode usar o backup e a recuperação do BlueXP mesmo que você não tenha uma licença para ele.

Para detectar comportamento anômalo do usuário, a proteção contra ransomware do BlueXP usa a proteção autônoma contra ransomware do NetApp, um modelo de aprendizado de máquina (ML) no ONTAP que deteta atividade de arquivos maliciosos. Esse modelo está incluído na licença de proteção contra ransomware da BlueXP . Você também pode usar a Segurança de carga de trabalho do Insights da infraestrutura de dados (anteriormente Cloud Insights) (licença necessária) para investigar o comportamento do usuário e bloquear usuários específicos de atividades adicionais.

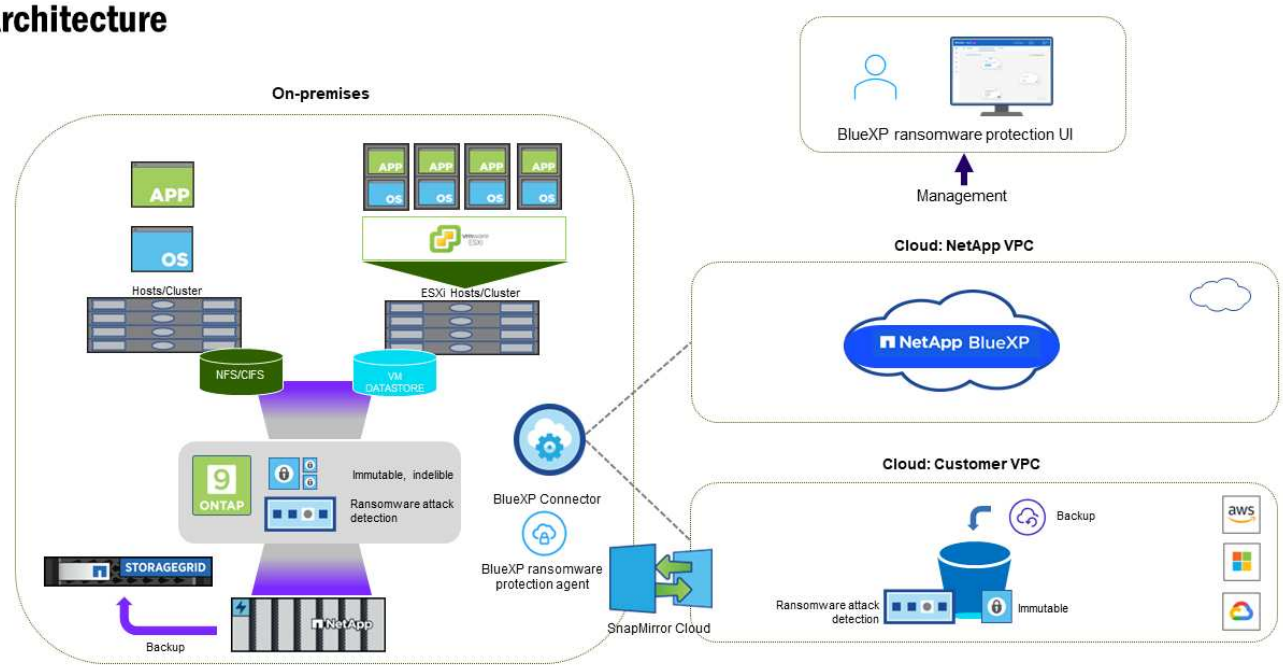
Para obter detalhes, "Configure o licenciamento"consulte .

Como a proteção contra ransomware do BlueXP funciona

Em um alto nível, a proteção contra ransomware do BlueXP funciona assim.

A proteção contra ransomware do BlueXP usa backup e recuperação do BlueXP para descobrir e definir políticas de snapshot e backup para workloads de compartilhamento de arquivos, e o SnapCenter ou SnapCenter para VMware para descobrir e definir políticas de snapshot e backup para workloads de aplicação e VM. Além disso, a proteção contra ransomware do BlueXP usa backup e recuperação do BlueXP e o SnapCenter / SnapCenter para VMware para executar recuperação consistente com arquivos e workloads.

Architecture



Recurso	Descrição
IDENTIFIQUE	• Encontra todos os dados nas (protocolos NFS e CIFS) e Cloud Volumes ONTAP no local conectados à BlueXP . • Identifica os dados dos clientes das APIs de serviço ONTAP e SnapCenter e os associa a cargas de trabalho. Saiba mais sobre "ONTAP" e "Software SnapCenter". • Detecta o nível de proteção atual de cada volume de cópias NetApp Snapshot e políticas de backup, bem como quaisquer recursos de detecção on-box. Em seguida, o serviço associa essa postura de proteção às cargas de trabalho usando backup e recuperação do BlueXP , serviços ONTAP e tecnologias NetApp, como proteção autônoma contra ransomware, FPolicy, políticas de backup e políticas de snapshot. Saiba mais sobre "Proteção autônoma contra ransomware" e "Backup e recuperação do BlueXP", e "Política de ONTAP". • Atribui uma prioridade de negócios a cada workload com base nos níveis de proteção descobertos automaticamente e recomenda políticas de proteção para cargas de trabalho com base em sua prioridade de negócios. A prioridade do workload é baseada nas frequências do Snapshot já aplicadas a cada volume associado à carga de trabalho.
* PROTEGER*	• Monitore workloads ativamente e orquestra o uso de backup e recuperação do BlueXP , SnapCenter e APIs do ONTAP aplicando políticas em cada um dos workloads identificados.

Recurso	Descrição
DETECTAR	• Detecta possíveis ataques com um modelo integrado de aprendizado de máquina (ML) que deteta atividade e criptografia potencialmente anômalas. • Fornece detecção de camada dupla que começa com a deteção de possíveis ataques de ransomware no storage primário e a resposta a atividades anormais. Basta fazer cópias Snapshot automatizadas adicionais para criar os pontos de restauração de dados mais próximos. O serviço oferece a capacidade de se aprofundar para identificar possíveis ataques com maior precisão sem afetar o desempenho dos workloads primários. • Determina os arquivos e mapas suspeitos específicos que atacam as cargas de trabalho associadas, usando as tecnologias ONTAP, Autonomous ransomware Protection, Data Infrastructure Insights (anteriormente Cloud Insights) e FPolicy.
RESPONDER	• Mostra dados relevantes, como atividade de arquivo, atividade de usuário e entropia, para ajudá-lo a concluir revisões forenses sobre o ataque. • Inicia cópias snapshot rápidas usando tecnologias e produtos da NetApp, como ONTAP, proteção autônoma contra ransomware e FPolicy.
RECUPERAR	• Determina o melhor Snapshot ou backup e recomenda o melhor ponto de recuperação real (RPA) usando tecnologias e serviços de backup e recuperação do BlueXP , ONTAP, proteção autônoma contra ransomware e FPolicy. • Orquestra a recuperação de workloads, incluindo VMs, compartilhamentos de arquivos e bancos de dados com consistência de aplicação.
GOVERNAR	• Atribui as estratégias de proteção contra ransomware • Ajuda a monitorar os resultados.

Destinos de backup compatíveis, ambientes de trabalho e fontes de dados de workload

Use a proteção contra ransomware do BlueXP para ver a resiliência dos dados a um ataque cibernético contra os seguintes tipos de destinos de backup, ambientes de trabalho e fontes de dados de workload:

Os destinos de backup são suportados

- Amazon Web Services (AWS) S3
- Google Cloud Platform
- Microsoft Azure Blob
- NetApp StorageGRID

Ambientes de trabalho suportados

- ONTAP nas no local (usando protocolos NFS e CIFS) com ONTAP versão 9.11.1 e posterior
- Cloud Volumes ONTAP 9.11.1 ou posterior para AWS (usando protocolos NFS e CIFS)
- Cloud Volumes ONTAP 9.11.1 ou posterior para Google Cloud Platform (usando protocolos NFS e CIFS)
- Cloud Volumes ONTAP 9.12.1 ou superior para Microsoft Azure (usando protocolos NFS e CIFS)

Não há suporte para os seguintes itens: Volumes FlexGroup, versões do ONTAP anteriores a 9.11.1, volumes iSCSI, volumes de ponto de montagem, volumes de caminho de montagem, volumes offline e volumes DP (proteção de dados).

Fontes de dados de carga de trabalho suportadas

O serviço protege os seguintes workloads baseados na aplicação em volumes de dados primários:

- Compartilhamentos de arquivo do NetApp
- Armazenamentos de dados VMware
- Bancos de dados (MySQL e Oracle)
- Mais em breve

Além disso, se você estiver usando o SnapCenter ou o SnapCenter para VMware, todos os workloads compatíveis com esses produtos também serão identificados na proteção contra ransomware do BlueXP . A proteção contra ransomware da BlueXP pode protegê-los e recuperá-los de maneira consistente com os workloads.

Termos que podem ajudá-lo com proteção contra ransomware

Você pode se beneficiar ao compreender alguma terminologia relacionada à proteção contra ransomware.

- **Proteção**: Proteção na proteção contra ransomware BlueXP significa garantir que snapshots e backups imutáveis ocorram regularmente para um domínio de segurança diferente usando políticas de proteção.
- **Carga de trabalho**: Uma carga de trabalho na proteção contra ransomware do BlueXP pode incluir bancos de dados MySQL ou Oracle, datastores VMware ou compartilhamentos de arquivos.

Pré-requisitos de proteção contra ransomware da BlueXP

Comece a usar a proteção contra ransomware do BlueXP verificando a prontidão do seu ambiente operacional, login, acesso à rede e navegador da Web.

Para usar a proteção contra ransomware do BlueXP , você precisará desses pré-requisitos.

Em BlueXP

- Uma conta de usuário do BlueXP com o administrador da organização Privileges para descobrir recursos.
- Organização do BlueXP com pelo menos um conector BlueXP ativo que se conecta a clusters ONTAP locais ou que se conecta ao Cloud Volumes ONTAP na AWS ou no Azure.
- O conetor BlueXP tem de ter o `cloudmanager-ransomware-protection` recipiente num estado ativo.
- Pelo menos um ambiente de trabalho do BlueXP com um cluster ONTAP no local do NetApp ou Cloud volume ONTAP na AWS ou Azure (usando protocolos nas ou CIFS).
  - Os clusters ONTAP ou Cloud volume ONTAP com ONTAP os versão 9.11.1 ou superior são compatíveis.
  - Se os clusters do ONTAP no local ou o Cloud volume ONTAP na AWS ou na nuvem do Azure ainda não estiverem integrados no BlueXP , você precisará de um BlueXP Connector.

```
https://docs.netapp.com/us-en/bluexp-setup-admin/concept-
connectors.html["Saiba como configurar um conetor BlueXP "]Consulte e
https://docs.netapp.com/us-en/cloud-manager-setup-admin/reference-
checklist-cm.html["Requisitos padrão do BlueXP"^].
```

Se você tiver vários conetores BlueXP em uma única organização do BlueXP , o serviço de proteção contra ransomware da BlueXP verificará os recursos do ONTAP em todos os conetores além daquele que está selecionado atualmente na IU do BlueXP .

Em ONTAP 9.11,1 e posterior

- Uma licença do ONTAP One é ativada na instância do ONTAP no local.
- Uma licença para a proteção autônoma contra ransomware do NetApp, usada pela proteção contra ransomware do BlueXP , habilitada na instância do ONTAP local, dependendo da versão do ONTAP que você estiver usando. Consulte a "Visão geral da proteção autônoma contra ransomware".

  O lançamento geral da proteção contra ransomware do BlueXP , ao contrário da versão prévia, inclui uma licença para a tecnologia NetApp Autonomous ransomware Protection. "Visão geral da proteção autônoma contra ransomware"Consulte para obter detalhes.

  Para obter mais detalhes sobre o licenciamento, "Saiba mais sobre a proteção contra ransomware BlueXP "consulte .

- Para aplicar configurações de proteção (como habilitar a proteção Autônoma contra ransomware e outras), a proteção contra ransomware do BlueXP precisa de permissões de administrador no cluster do ONTAP. O cluster do ONTAP deve ter sido integrado somente usando as credenciais de usuário do administrador do cluster do ONTAP.
- Se o cluster do ONTAP já estiver integrado no BlueXP usando credenciais de usuário não administrativas, as permissões de usuário que não sejam administrativas devem ser atualizadas com as permissões necessárias fazendo login no cluster do ONTAP, descrito nesta página.

Para backups de dados

- Uma conta no NetApp StorageGRID, AWS S3 ou Azure Blob para destinos de backup e o conjunto de permissões de acesso.

  Consulte "Lista de permissões AWS, Azure ou S3" para obter mais informações.

- O serviço de backup e recuperação do BlueXP não precisa ser ativado no ambiente de trabalho.

  O serviço de proteção contra ransomware do BlueXP ajuda a configurar um destino de backup por meio da opção Configurações. "Configure as definições"Consulte .

Atualizar permissões de usuário que não sejam administradores em um ambiente de trabalho do ONTAP

Se você precisar atualizar permissões de usuário que não sejam administradores para um ambiente de trabalho específico, execute estas etapas.

1. Faça login no BlueXP e procure o ambiente de trabalho que precisa de suas permissões de usuário do ONTAP atualizadas.
2. Clique duas vezes no ambiente de trabalho para ver os detalhes.
3. Clique em **Exibir informações adicionais** que mostram o nome de usuário.
4. Faça login na CLI do cluster do ONTAP usando o usuário admin.
5. Exibir as funções existentes para esse usuário. Introduza:

```
security login show -user-or-group-name <username>
```

6. Altere a função para o utilizador. Introduza:

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. Retorne à IU de proteção contra ransomware do BlueXP para usá-la.

Início rápido para proteção contra ransomware BlueXP

Aqui está uma visão geral das etapas necessárias para começar a usar a proteção contra ransomware BlueXP . Os links em cada etapa levam você a uma página que fornece mais detalhes.

Reveja os pré-requisitos

"Certifique-se de que seu ambiente atenda a esses requisitos".

Configure o serviço de proteção contra ransomware

- "Prepare o NetApp StorageGRID, Amazon Web Services ou Microsoft Azure como destino de backup".
- "Configure um conetor no BlueXP".
- "Configurar destinos de cópia de segurança".
- "Opcionalmente, ative a deteção de ameaças".
- "Descubra workloads em BlueXP ".

O que se segue?

Depois de configurar o serviço, aqui está o que você pode fazer a seguir.

- "Ver a integridade da proteção de workload no Dashboard".
- "Proteja workloads".
- "Responda à detecção de possíveis ataques de ransomware".

- "Recuperar de um ataque (após os incidentes serem neutralizados)".

Configurar a proteção contra ransomware do BlueXP

Para usar a proteção contra ransomware do BlueXP , execute algumas etapas para configurá-la.

Antes de começar, revise "pré-requisitos" para garantir que seu ambiente esteja pronto.

Prepare o destino da cópia de segurança

Prepare um dos seguintes destinos de backup:

- NetApp StorageGRID
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Depois de configurar as opções no próprio destino de backup, você o configurará posteriormente como um destino de backup no serviço de proteção contra ransomware BlueXP . Para obter detalhes sobre como configurar o destino de backup na proteção contra ransomware do BlueXP , "Configurar destinos de cópia de segurança"consulte .

Prepare o StorageGRID para se tornar um destino de backup

Se pretender utilizar o StorageGRID como destino da cópia de segurança, consulte "Documentação do StorageGRID" para obter detalhes sobre o StorageGRID.

Prepare a AWS para se tornar um destino de backup

- Configure uma conta na AWS.
- Configure "Permissões da AWS" na AWS.

Para obter detalhes sobre como gerenciar seu storage da AWS no BlueXP , "Gerencie seus buckets do Amazon S3" consulte .

Prepare o Azure para se tornar um destino de backup

- Configure uma conta no Azure.
- Configurar "Permissões do Azure" no Azure.

Para obter detalhes sobre como gerenciar seu storage Azure no BlueXP , "Gerencie suas contas de storage do Azure" consulte .

Configure o BlueXP

A próxima etapa é configurar o BlueXP e o serviço de proteção contra ransomware BlueXP .

Revisão "Requisitos padrão do BlueXP".

Crie um conetor no BlueXP

Deve contactar o seu representante de vendas da NetApp para experimentar ou utilizar este serviço. Em seguida, ao usar o BlueXP Connector, ele incluirá as funcionalidades apropriadas para o serviço de proteção contra ransomware.

Para criar um conetor no BlueXP antes de usar o serviço, consulte a documentação do BlueXP que descreve "Como criar um conetor BlueXP"o .

> Se você tiver vários conetores BlueXP , o serviço verificará os dados em todos os conetores além daquele que aparece atualmente na IU do BlueXP . Este serviço descobre todos os projetos e todos os conetores associados a esta organização.

Acesse a proteção contra ransomware do BlueXP

Você usa o NetApp BlueXP para fazer login no serviço de proteção contra ransomware da BlueXP .

A proteção contra ransomware do BlueXP usa o controle de acesso baseado em funções (RBAC) para controlar o acesso que cada usuário tem a ações específicas. Para obter detalhes sobre as ações que cada função pode executar, "Privileges de controle de acesso baseado em funções de proteção contra ransomware da BlueXP "consulte .

Para fazer login no BlueXP , você pode usar as credenciais do site de suporte da NetApp ou se inscrever para fazer login na nuvem do NetApp usando seu e-mail e uma senha. "Saiba mais sobre como fazer login".

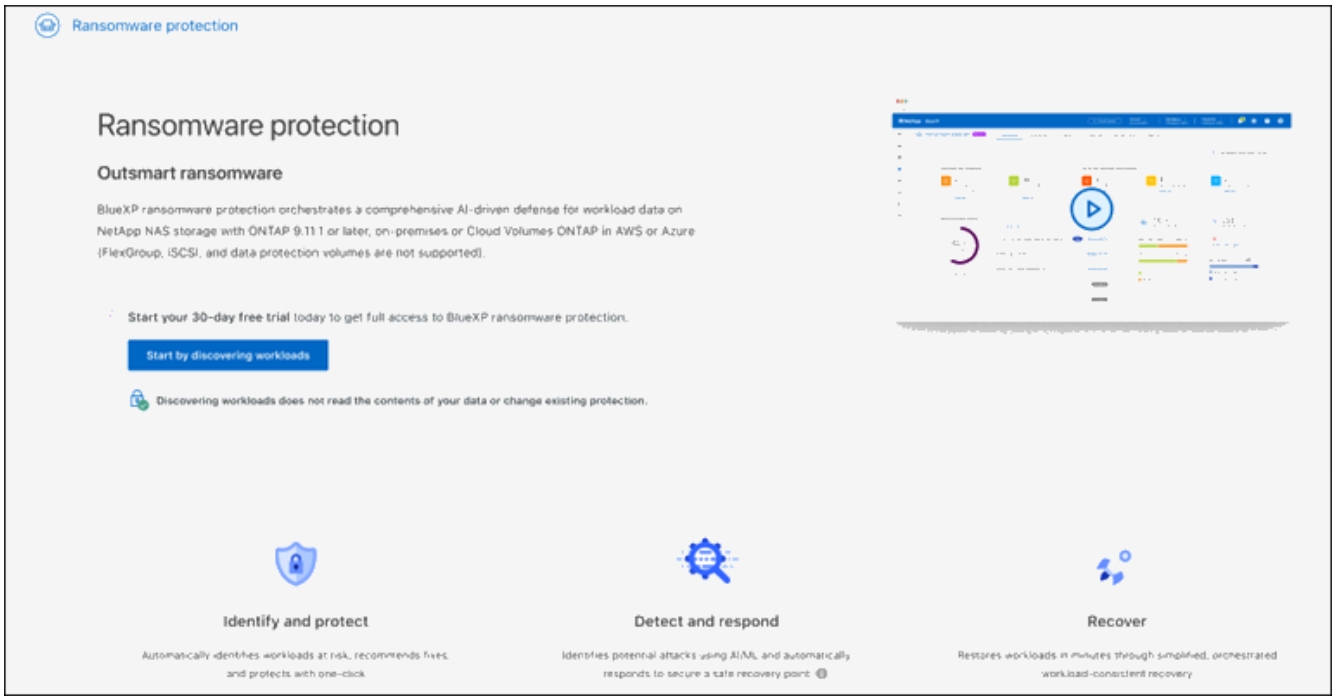
Passos

1. Abra um navegador da Web e vá para o "Consola BlueXP".

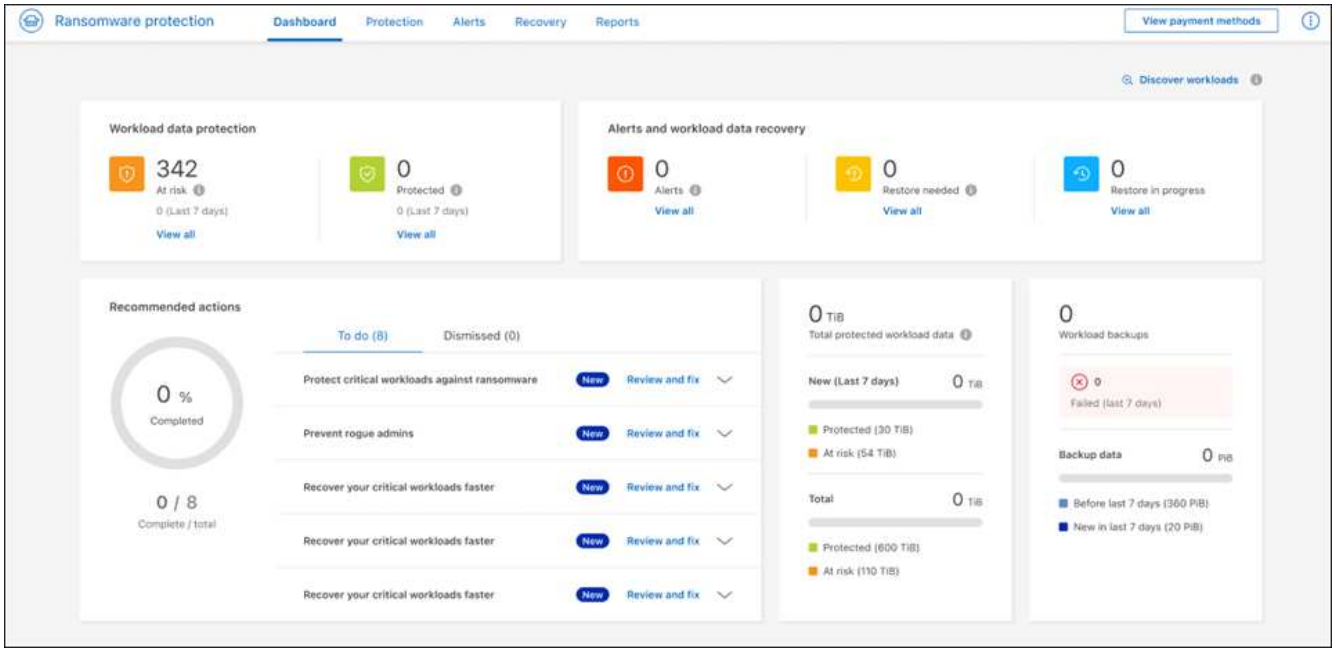
   É apresentada a página de início de sessão do NetApp BlueXP .

2. Inicie sessão no BlueXP .
3. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.

   Se esta for a primeira vez que fizer login neste serviço, a página de destino será exibida.



Caso contrário, o Dashboard de proteção contra ransomware do BlueXP será exibido.



Se você não tiver um conetor BlueXP ou não for o único para este serviço, talvez seja necessário entrar em Contato com o suporte da NetApp.

4. Se você ainda não fez isso, selecione a opção **descobrir cargas de trabalho**.

   "Localizar workloads"Consulte a .

Configure o licenciamento para a proteção contra ransomware BlueXP

Com a proteção contra ransomware do BlueXP , você pode usar diferentes planos de licenciamento.

Você pode usar os seguintes tipos de licença:

- Inscreva-se para uma avaliação gratuita de 30 dias.
- Compre uma assinatura PAYGO (pay-as-you-go) com o Amazon Web Services (AWS) Marketplace, o Google Cloud Marketplace ou o Azure Marketplace (em breve).
- Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém de seu representante de vendas da NetApp Você pode usar o número de série da licença para ativar o BYOL na carteira digital BlueXP .

Depois de configurar seu BYOL ou comprar uma assinatura PAYGO, você pode ver a licença na guia carteira digital BlueXP **licenças de serviço de dados** ou a assinatura ativa na guia carteira digital BlueXP **assinaturas**.

Após o término da avaliação gratuita ou a licença ou assinatura expirar, você ainda poderá fazer o seguinte no serviço:

- Visualizar workloads e integridade do workload.
- Exclua qualquer recurso, como uma política.
- Execute todas as operações agendadas que foram criadas durante o período de teste ou sob a licença.

Outras considerações de licença

A licença de proteção contra ransomware da BlueXP não inclui produtos NetApp adicionais. A proteção contra ransomware do BlueXP pode usar o backup e a recuperação do BlueXP mesmo que você não tenha uma licença para ele.

Se você tiver backup e recuperação do BlueXP e proteção contra ransomware BlueXP , todos os dados comuns protegidos por ambos os produtos serão cobrados apenas pela proteção contra ransomware do BlueXP .

Você pode visualizar um comportamento anômalo do usuário com o 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 . Para obter uma visão geral do Data Infrastuture 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.

Experimente-o usando um teste gratuito de 30 dias

Você pode experimentar a proteção contra ransomware do BlueXP usando uma avaliação gratuita de 30 dias. Você deve ser um administrador da Organização BlueXP para iniciar a avaliação gratuita.

Com o lançamento de outubro de 2024, novas implantações de proteção contra ransomware BlueXP agora têm 30 dias para uma avaliação gratuita. Anteriormente, a proteção contra ransomware da BlueXP forneceu 90 dias como uma avaliação gratuita. Se você já está no teste gratuito de 90 dias, essa oferta continua por 90 dias.

Não são aplicados limites de capacidade durante o teste.

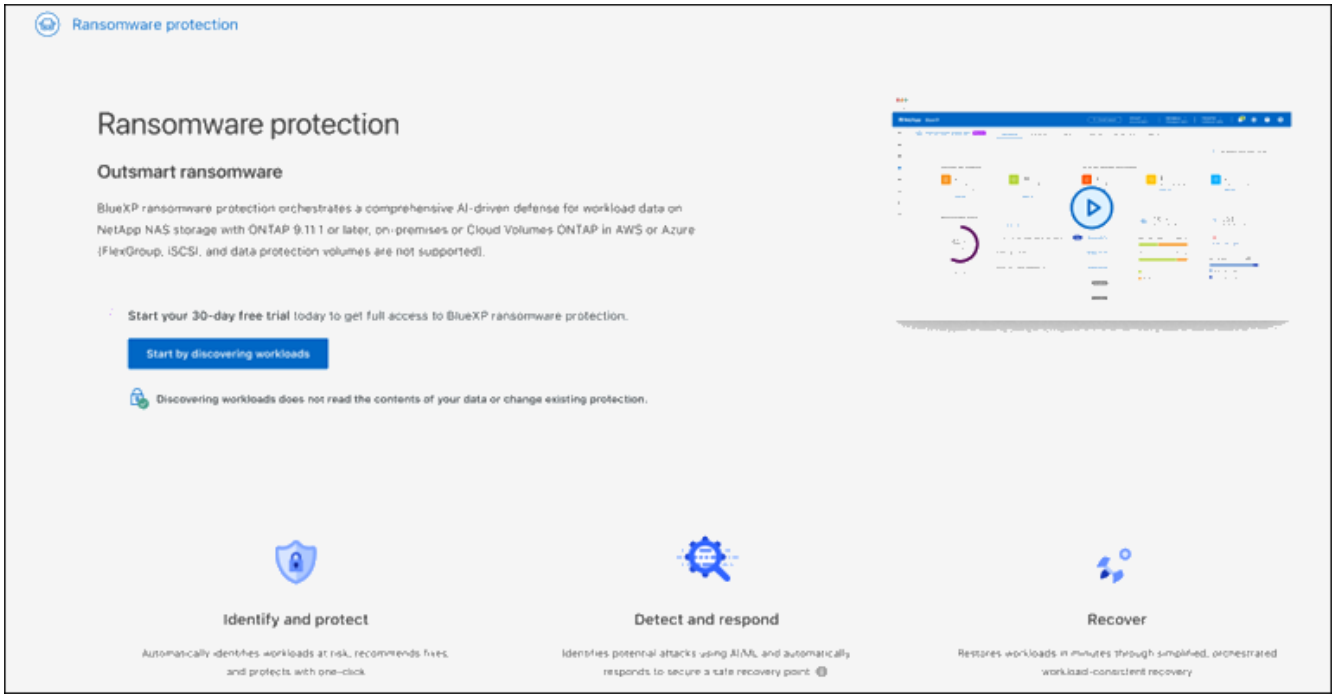
Você pode obter uma licença ou assinar a qualquer momento e você não será cobrado até que o teste de 30 dias termine. Para continuar após o teste de 30 dias, você precisará comprar uma licença BYOL ou uma assinatura PAYGO.

Durante o teste, você tem funcionalidade completa.

Passos

1. Aceder ao "Consola BlueXP".
2. Inicie sessão no BlueXP .
3. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.

   Se esta for a primeira vez que fizer login neste serviço, a página de destino será exibida.



4. Se você ainda não adicionou um conetor para outros serviços, adicione um.

   Para adicionar um conetor, "Saiba mais sobre conetores" consulte a .

5. Depois de configurar um conetor, na página inicial da proteção contra ransomware do BlueXP , o botão para adicionar um conetor muda a um botão para descobrir cargas de trabalho. Selecione **Comece descobrindo cargas de trabalho**.
6. Para rever as informações de avaliação gratuita, selecione a opção pendente no canto superior direito.

Após o término da avaliação, obtenha uma assinatura ou licença

Após o término da avaliação gratuita, você pode se inscrever em um dos marketplaces ou comprar uma

licença da NetApp.

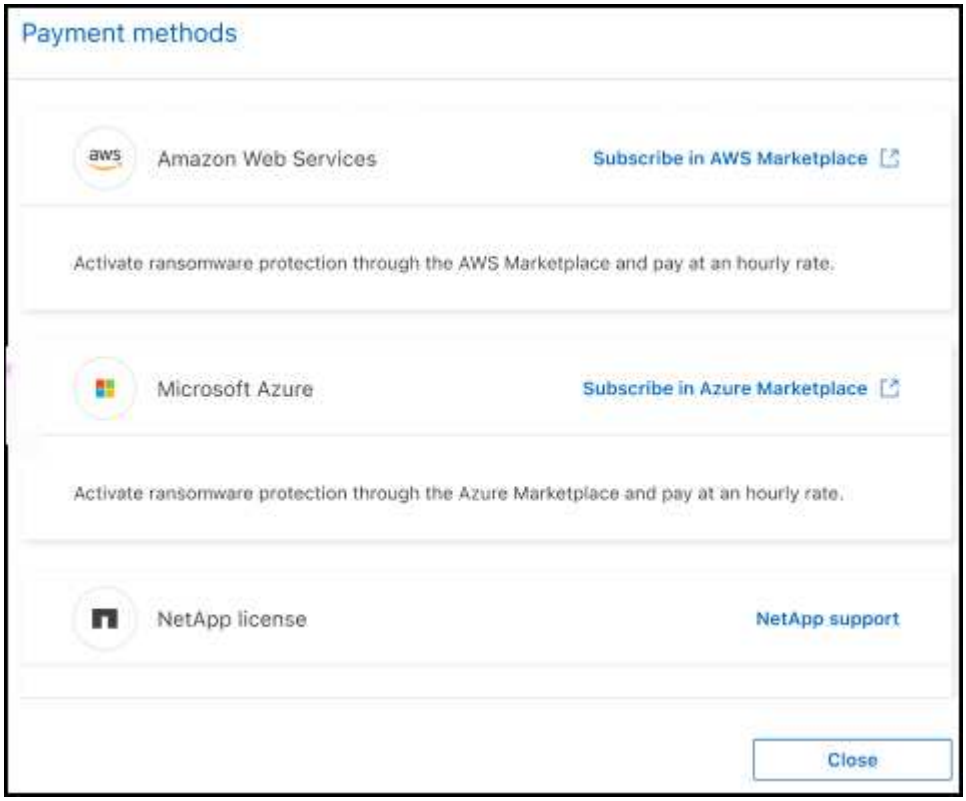
Inscreva-se no AWS Marketplace Inscreva-se através do Microsoft Azure Marketplace Inscreva-se no Google Cloud Marketplace Traga sua própria licença (BYOL)

Inscreva-se no AWS Marketplace

Este procedimento fornece uma visão geral de alto nível de como se inscrever diretamente no AWS Marketplace.

Passos

1. Na proteção contra ransomware do BlueXP , siga um destes procedimentos:
   - Você vê uma mensagem de que o teste gratuito está expirando. Na mensagem, selecione **Exibir métodos de pagamento**.
   - Clique no aviso **avaliação gratuita** no canto superior direito e selecione **Ver métodos de pagamento**.



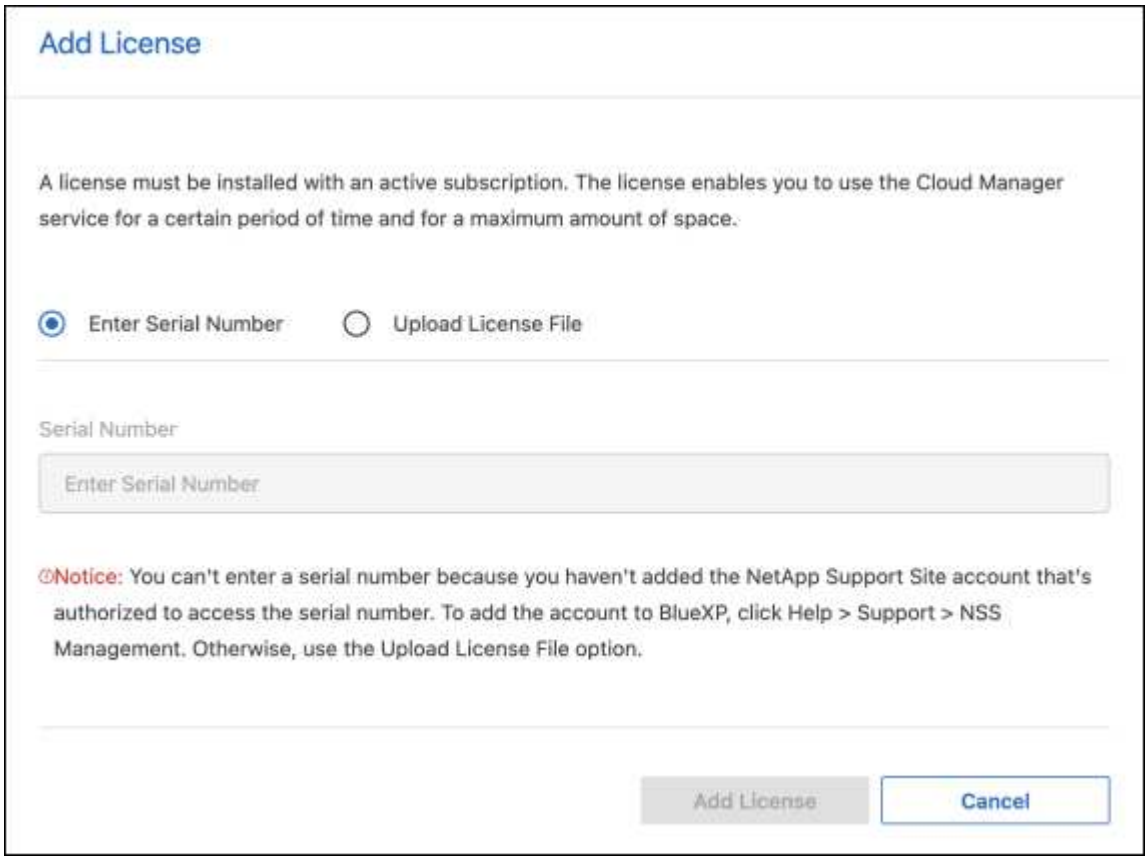
2. Na página métodos de pagamento, selecione **Inscrever-se no AWS Marketplace**.
3. No AWS Marketplace, selecione **Exibir opções de compra**.
4. Use o AWS Marketplace para assinar a proteção contra ransomware do BlueXP .
5. Quando você retorna à proteção contra ransomware do BlueXP , uma mensagem indica que você está inscrito.

> Um e-mail é enviado a você que inclui o número de série da proteção contra ransomware da BlueXP e indica que a proteção contra ransomware da BlueXP está subscrita no AWS Marketplace.

6. Voltar à página métodos de pagamento de proteção contra ransomware BlueXP .

7. Adicione a licença ao BlueXP selecionando **Adicionar licença ao BlueXP** .

   O serviço de carteira digital BlueXP mostra a página Adicionar licença.



8. Na página Adicionar licença na carteira digital BlueXP , selecione **Digite o número de série**, digite o número de série que foi incluído no e-mail enviado a você e selecione **Adicionar licença**.
9. Para ver os detalhes da licença na carteira digital BlueXP , na navegação à esquerda do BlueXP , selecione **Governança** > **carteira digital**.
   - Para ver as informações da subscrição, selecione **Subscrições**.
   - Para ver licenças BYOL, selecione **licenças de serviços de dados**.

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

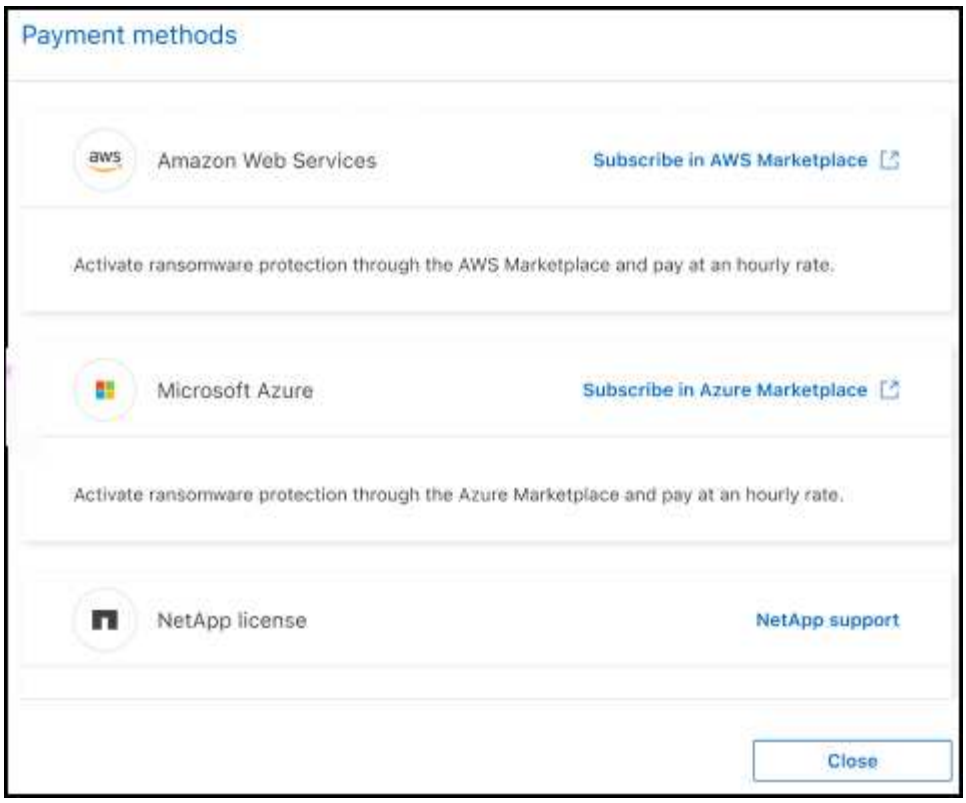
    É apresentada uma mensagem a indicar que foi adicionada uma licença.

Inscreva-se através do Microsoft Azure Marketplace

Este procedimento fornece uma visão geral de alto nível de como se inscrever diretamente no Azure Marketplace.

Passos

1. Na proteção contra ransomware do BlueXP , siga um destes procedimentos:
    - Você vê uma mensagem de que o teste gratuito está expirando. Na mensagem, selecione **Exibir métodos de pagamento**.
    - Clique no aviso **avaliação gratuita** no canto superior direito e selecione **Ver métodos de pagamento**.

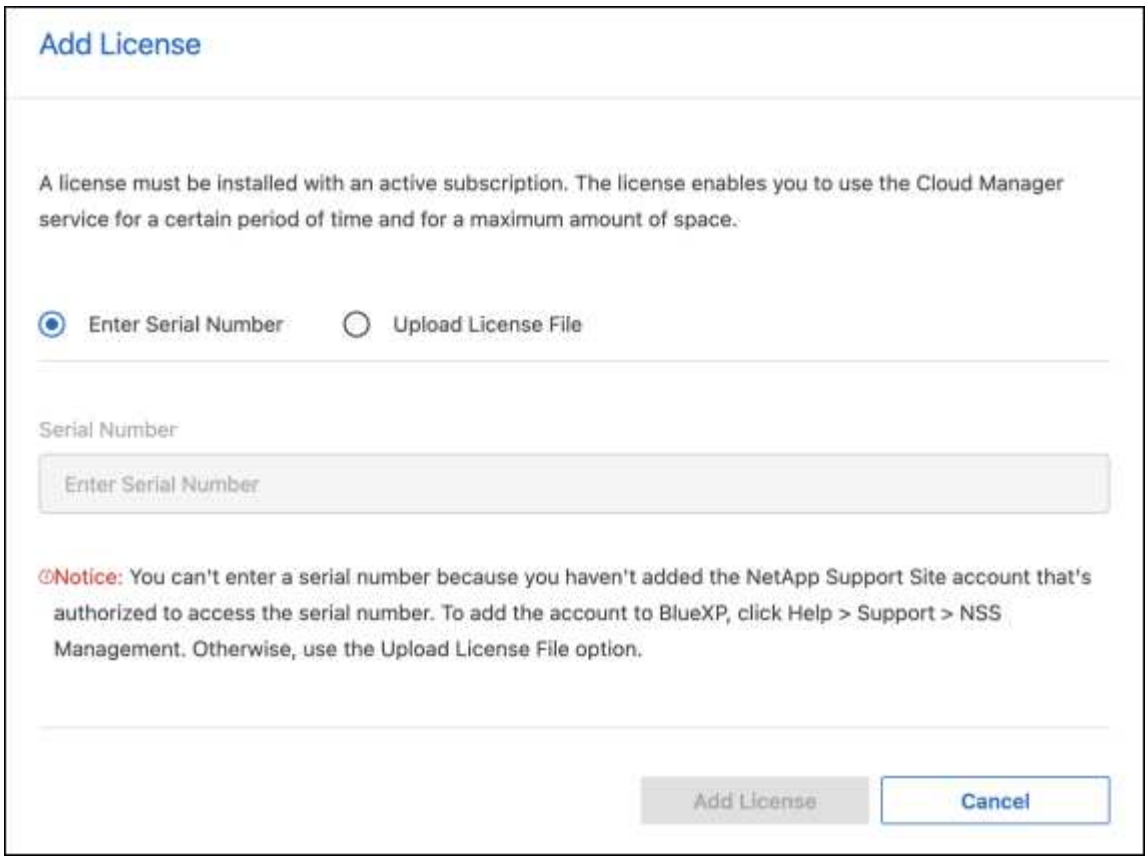


2. Na página métodos de pagamento, selecione **Inscrever-se no Azure Marketplace**.
3. No Azure Marketplace, selecione **Ver opções de compra**.
4. Use o Azure Marketplace para assinar a proteção contra ransomware do BlueXP .
5. Quando você retorna à proteção contra ransomware do BlueXP , uma mensagem indica que você está inscrito.

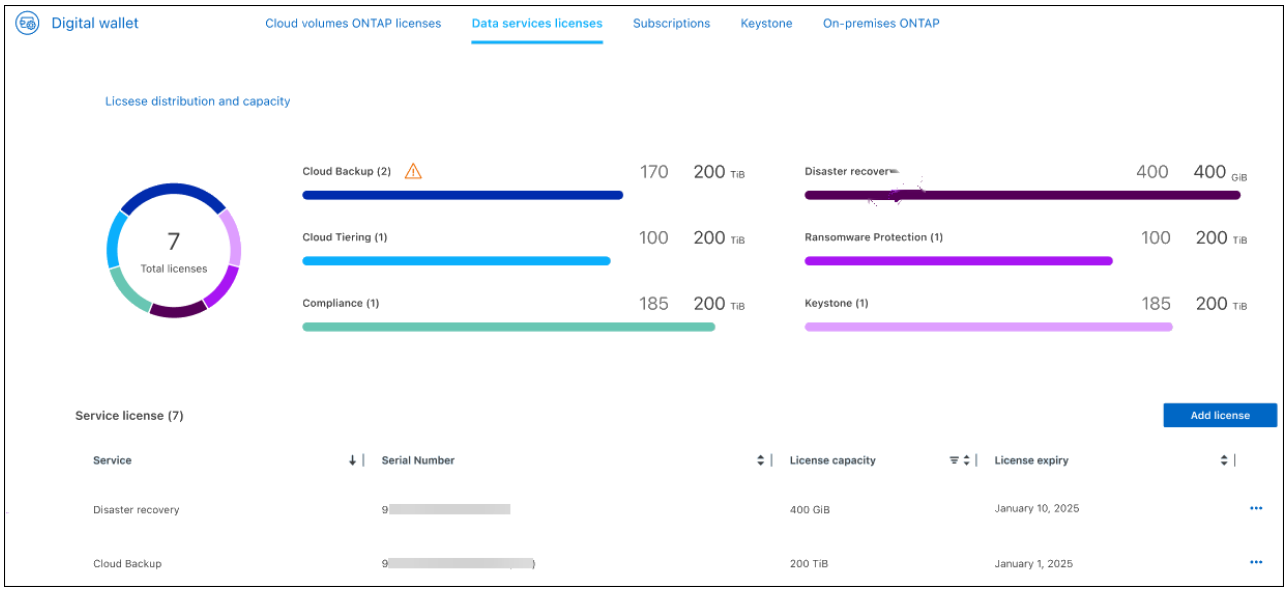
   Um e-mail é enviado a você que inclui o número de série da proteção contra ransomware da BlueXP e indica que a proteção contra ransomware da BlueXP está subscrita no Azure Marketplace.

6. Voltar à página métodos de pagamento de proteção contra ransomware BlueXP .
7. Adicione a licença ao BlueXP selecionando **Adicionar licença ao BlueXP** .

   O serviço de carteira digital BlueXP mostra a página Adicionar licença.



8. Na página Adicionar licença na carteira digital BlueXP , selecione **Digite o número de série**, digite o número de série que foi incluído no e-mail enviado a você e selecione **Adicionar licença**.
9. Para ver os detalhes da licença na carteira digital BlueXP , na navegação à esquerda do BlueXP , selecione **Governança** > **carteira digital**.
   - Para ver as informações da subscrição, selecione **Subscrições**.
   - Para ver licenças BYOL, selecione **licenças de serviços de dados**.



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

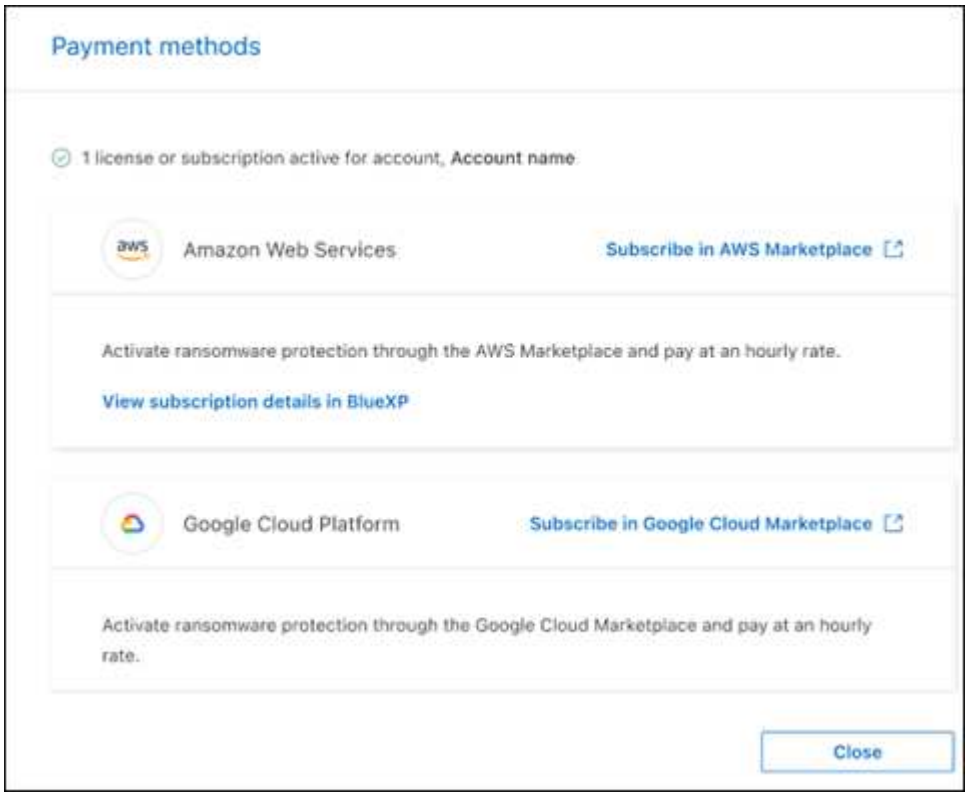
É apresentada uma mensagem a indicar que foi adicionada uma licença.

Inscreva-se no Google Cloud Marketplace

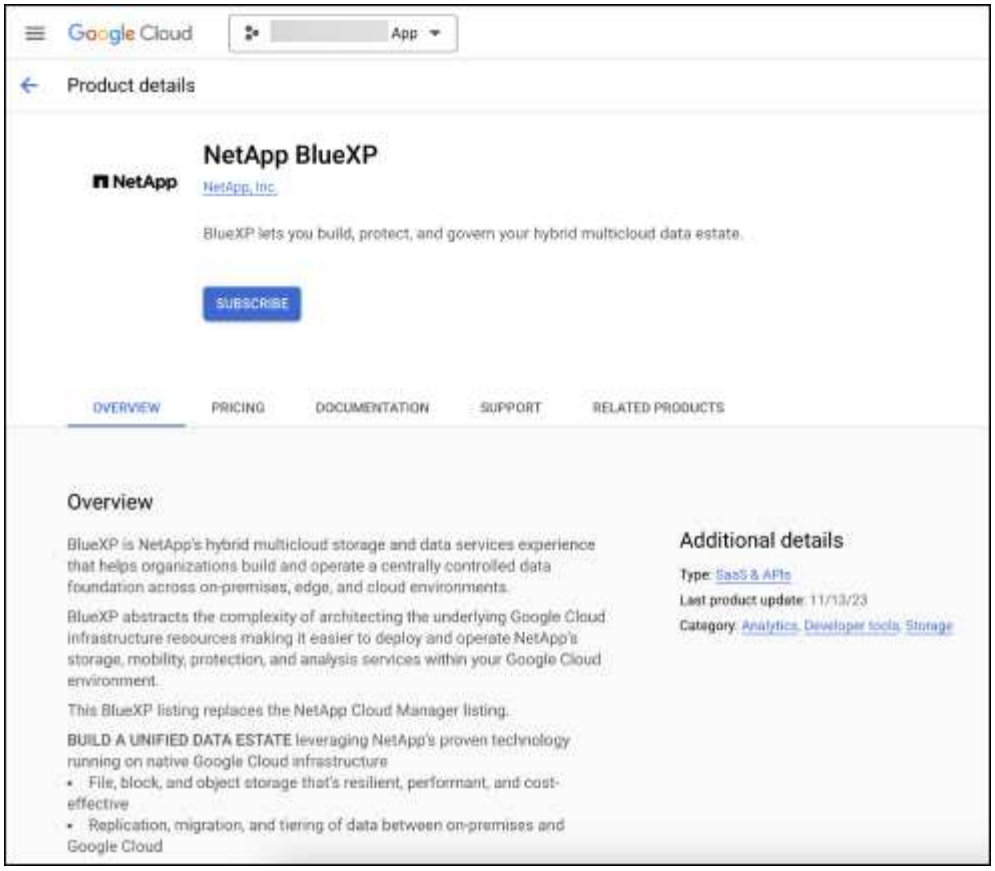
Este procedimento fornece uma visão geral de alto nível de como se inscrever diretamente no Google Cloud Marketplace.

Passos

1. Na proteção contra ransomware do BlueXP , siga um destes procedimentos:
   - Você vê uma mensagem de que o teste gratuito está expirando. Na mensagem, selecione **Exibir métodos de pagamento**.
   - Clique no aviso **avaliação gratuita** no canto superior direito e selecione **Ver métodos de pagamento**.



2. Na página métodos de pagamento, selecione **Inscrever-se no Google Cloud Marketplace**.
3. No Google Cloud Marketplace, selecione **Subscribe**.
4. Use o Google Cloud Marketplace para assinar a proteção contra ransomware do BlueXP .

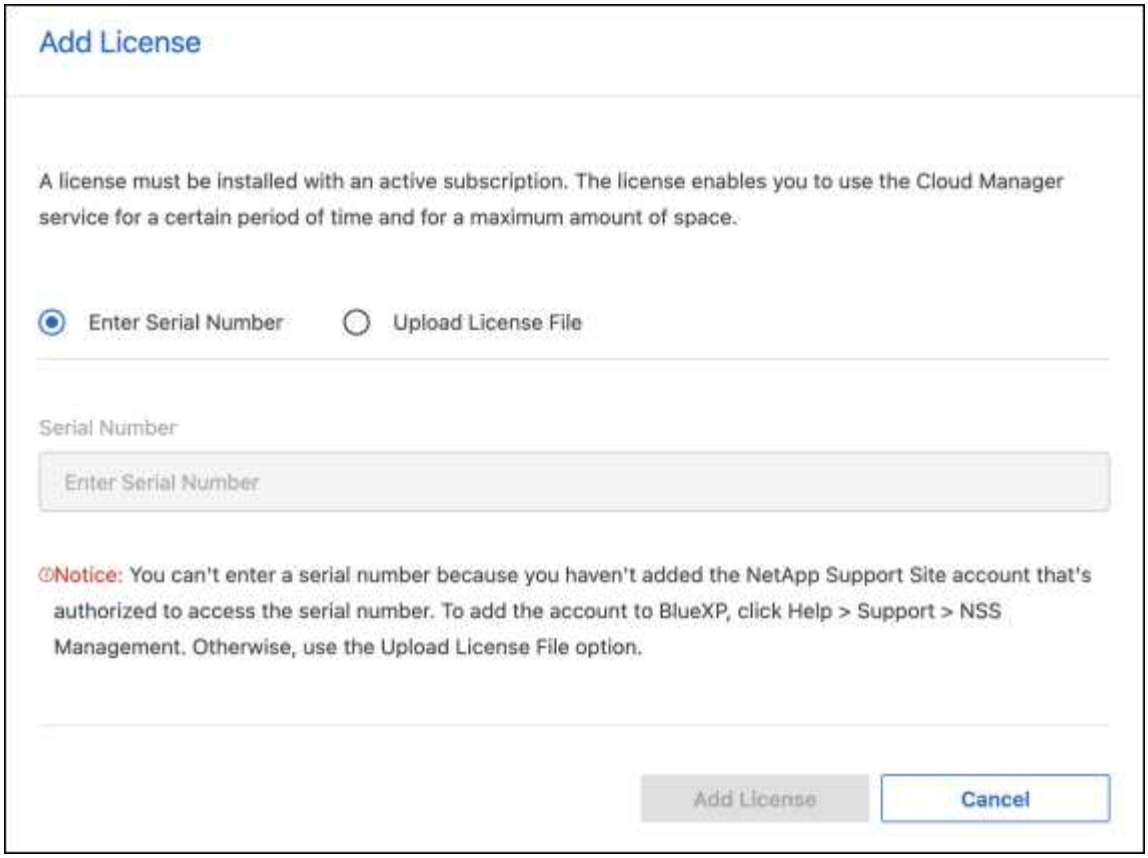


5. Quando você retorna à proteção contra ransomware do BlueXP , uma mensagem indica que você está inscrito.

> Um e-mail é enviado a você que inclui o número de série da proteção contra ransomware da BlueXP e indica que a proteção contra ransomware da BlueXP está subscrita no Google Cloud Marketplace.

6. Voltar à página métodos de pagamento de proteção contra ransomware BlueXP .
7. Adicione a licença ao BlueXP selecionando **Adicionar licença ao BlueXP** .

   O serviço de carteira digital BlueXP mostra a página Adicionar licença.



8. Na página Adicionar licença na carteira digital BlueXP , selecione **Digite o número de série**, digite o número de série que foi incluído no e-mail enviado a você e selecione **Adicionar licença**.
9. Para ver os detalhes da licença na carteira digital BlueXP , na navegação à esquerda do BlueXP , selecione **Governança** > **carteira digital**.
   - Para ver as informações da subscrição, selecione **Subscrições**.
   - Para ver licenças BYOL, selecione **licenças de serviços de dados**.

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

É apresentada uma mensagem a indicar que foi adicionada uma licença.

Traga sua própria licença (BYOL)

Se você quiser trazer sua própria licença (BYOL), precisará comprar a licença, obter o arquivo de licença NetApp (NLF) e adicionar a licença à carteira digital BlueXP .

Adicione o seu ficheiro de licença à carteira digital BlueXP

Depois de adquirir a licença de proteção contra ransomware BlueXP do seu representante de vendas da NetApp, ative a licença inserindo o número de série da proteção contra ransomware BlueXP e as informações da conta do site de suporte da NetApp (NSS).

Antes de começar

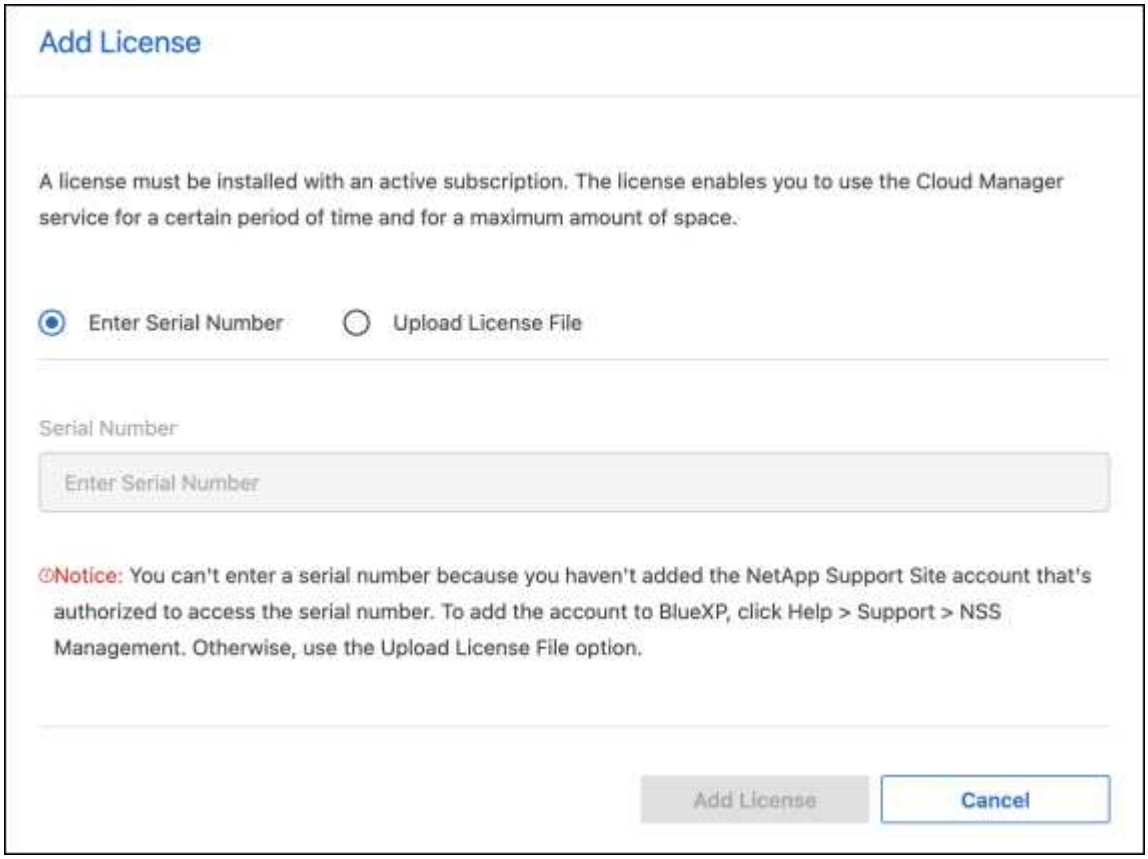
Você precisará do número de série da proteção contra ransomware BlueXP . Localize esse número no seu pedido de vendas ou entre em Contato com a equipe da conta para obter essas informações.

Passos

1. Depois de obter a licença, retorne à proteção contra ransomware do BlueXP . Selecione a opção **Exibir métodos de pagamento** no canto superior direito. Ou, na mensagem de que a avaliação gratuita está expirando, selecione **Subscribe ou compre uma licença**.
2. Selecione **Adicionar licença ao BlueXP** .

   Você será direcionado para a carteira digital BlueXP .

3. Na carteira digital BlueXP , na guia **licenças de serviços de dados**, selecione **Adicionar licença**.



4. Na página Adicionar licença, insira o número de série e as informações da conta do site de suporte da NetApp.
   - Se tiver o número de série da licença BlueXP e souber a sua conta NSS, selecione a opção **introduzir número de série** e introduza essas informações.

     Se a conta do site de suporte da NetApp não estiver disponível na lista suspensa, "Adicione a conta NSS ao BlueXP".

   - Se você tiver o arquivo de licença do BlueXP (necessário quando instalado em um site escuro), selecione a opção **carregar arquivo de licença** e siga as instruções para anexar o arquivo.
5. Selecione **Adicionar licença**.

Resultado

A carteira digital BlueXP agora mostra a proteção contra ransomware BlueXP com uma licença.

Atualize sua licença BlueXP quando ela expirar

Se o seu termo licenciado estiver próximo à data de expiração ou se a capacidade licenciada estiver atingindo o limite, você será notificado na IU de proteção contra ransomware da BlueXP . Você pode atualizar sua licença de proteção contra ransomware do BlueXP antes que ela expire para que não haja interrupção na capacidade de acessar os dados digitalizados.

Esta mensagem também aparece na carteira digital BlueXP e na "Notificações".

Passos

1. Selecione o ícone de bate-papo no canto inferior direito do BlueXP para solicitar uma extensão para o seu termo ou capacidade adicional para a sua licença para o número de série específico. Você também pode enviar um e-mail para solicitar uma atualização para sua licença.

   Depois de pagar a licença e esta ser registada no Site de suporte da NetApp, a BlueXP atualiza automaticamente a licença na carteira digital da BlueXP e a página licenças dos Serviços de dados refletirá a alteração em 5 a 10 minutos.

2. Se o BlueXP não puder atualizar automaticamente a licença (por exemplo, quando instalado em um site escuro), você precisará fazer o upload manual do arquivo de licença.
   a. Você pode obter o arquivo de licença no site de suporte da NetApp.
   b. Aceda à carteira digital BlueXP .
   c. Selecione a guia **licenças de serviços de dados**, selecione o ícone **ações …** para o número de série do serviço que você está atualizando e selecione **Licença de atualização**.

Descubra workloads na proteção de ransomware BlueXP

Para usar a proteção contra ransomware da BlueXP , o serviço precisa primeiro descobrir os dados. Durante a detecção, a proteção contra ransomware do BlueXP analisa todos os volumes e arquivos em ambientes de trabalho em todos os conetores e projetos do BlueXP dentro de uma organização.

A proteção contra ransomware do BlueXP avalia aplicações MySQL, aplicações Oracle, datastores VMware e compartilhamentos de arquivos.

As cargas de trabalho com volumes que usam FlexGroup ou iSCSI não serão descobertas.

O serviço avalia o nível de proteção existente, incluindo as opções atuais de proteção de backup, cópias Snapshot e proteção Autonomous ransomware do NetApp. Com base na avaliação, o serviço recomenda como melhorar a proteção contra ransomware.

Você pode fazer o seguinte:

- Em cada conetor, selecione os ambientes de trabalho onde você deseja descobrir cargas de trabalho. Você pode se beneficiar desse recurso se quiser proteger cargas de trabalho específicas em seu ambiente e não em outros.
- Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente.

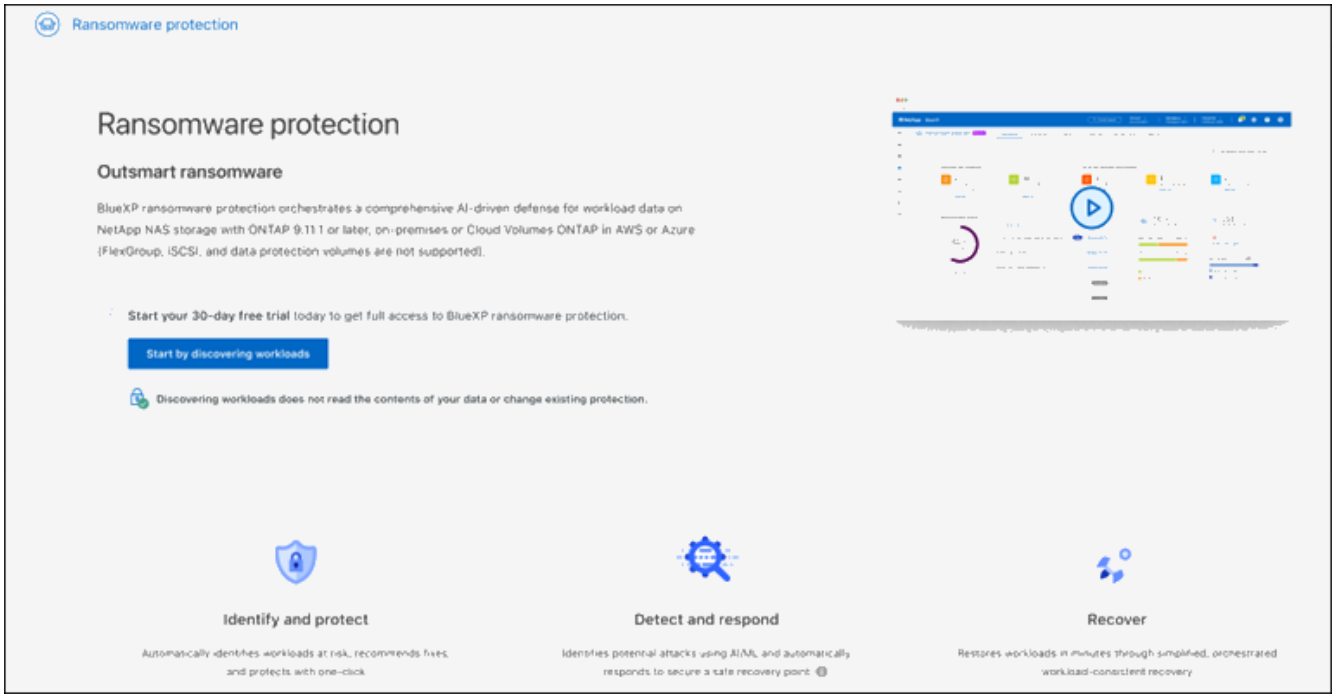
Selecione workloads para descobrir e proteger

Em cada conetor, selecione os ambientes de trabalho onde você deseja descobrir cargas de trabalho.

Passos

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

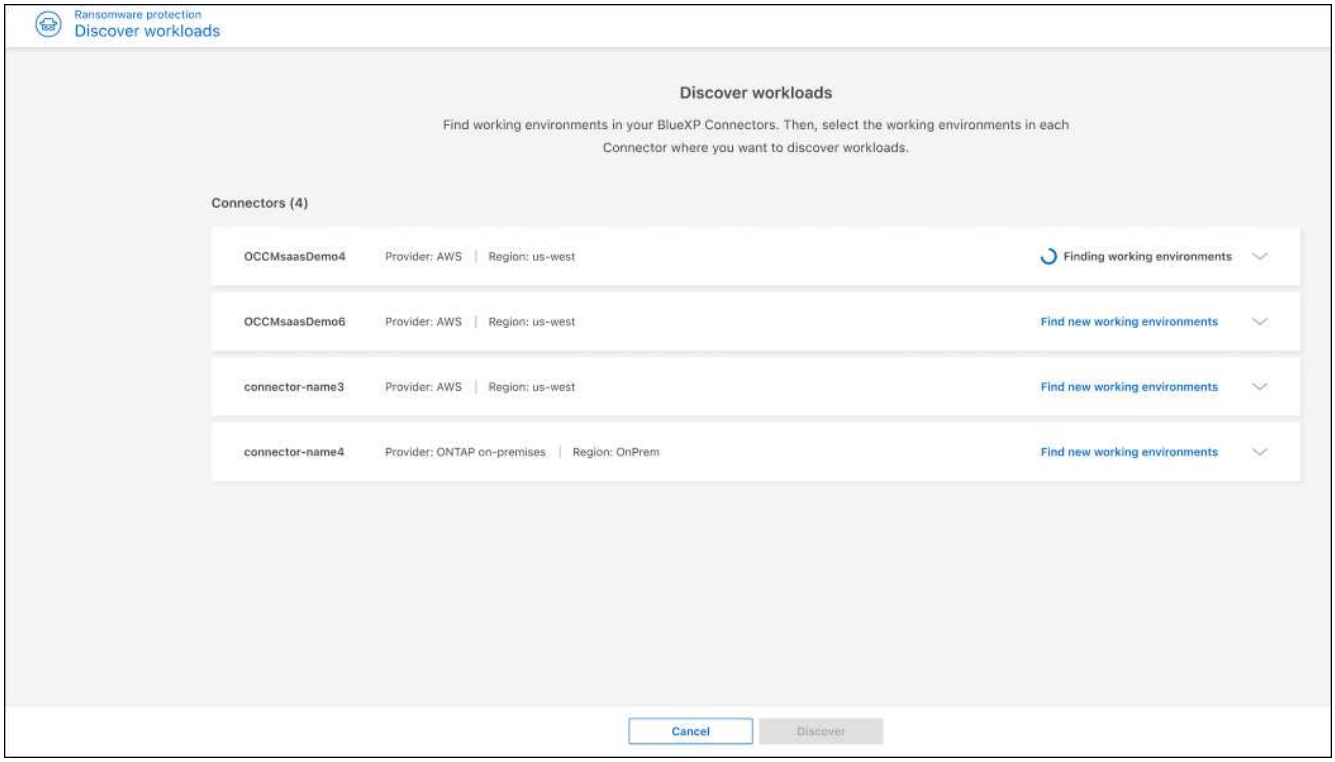
   Se esta for a primeira vez que fizer login neste serviço, a página de destino será exibida.



2. Na página inicial, selecione **Comece descobrindo cargas de trabalho**.

   O serviço encontra seus ambientes de trabalho em seus conetores BlueXP .

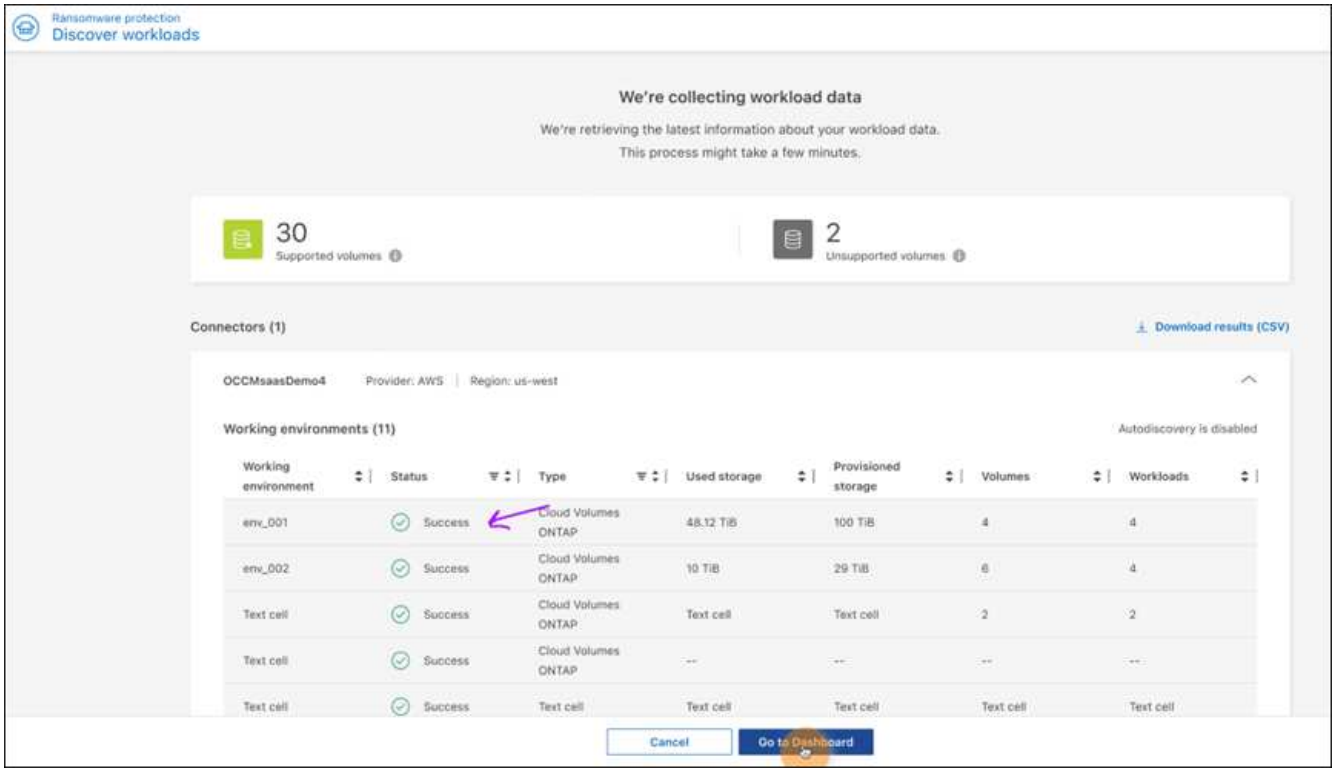
   Este processo pode demorar alguns minutos.



3. Na lista de conetores BlueXP , selecione **Localizar novos ambientes de trabalho** ao lado do conetor onde você deseja descobrir cargas de trabalho.
4. Selecione os ambientes de trabalho em que você deseja descobrir o workload ou marque a caixa no topo da tabela para localizar workloads em todos os ambientes de workload descobertos.
5. Selecione **Discover**.

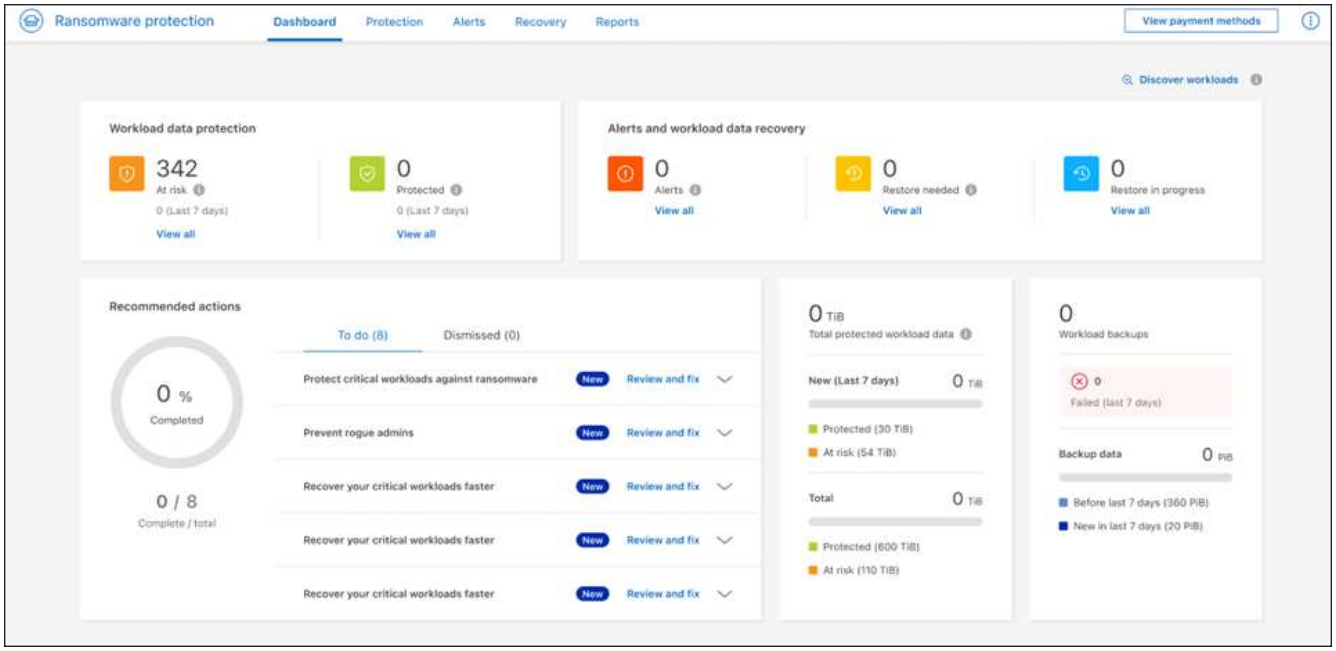
   O serviço detecta dados de workload somente para esses conetores com ambientes de trabalho selecionados.

   Este processo pode demorar alguns minutos.



6. Para fazer o download da lista de cargas de trabalho descobertas, selecione **Download Results (CSV)**.
7. Para exibir o Painel de proteção contra ransomware do BlueXP , selecione **ir para Painel**.

   O Dashboard mostra a integridade da proteção de dados. O número de cargas de trabalho protegidas ou em risco aumenta com base nas cargas de trabalho descobertas recentemente.



"Saiba o que o Dashboard mostra."

Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente

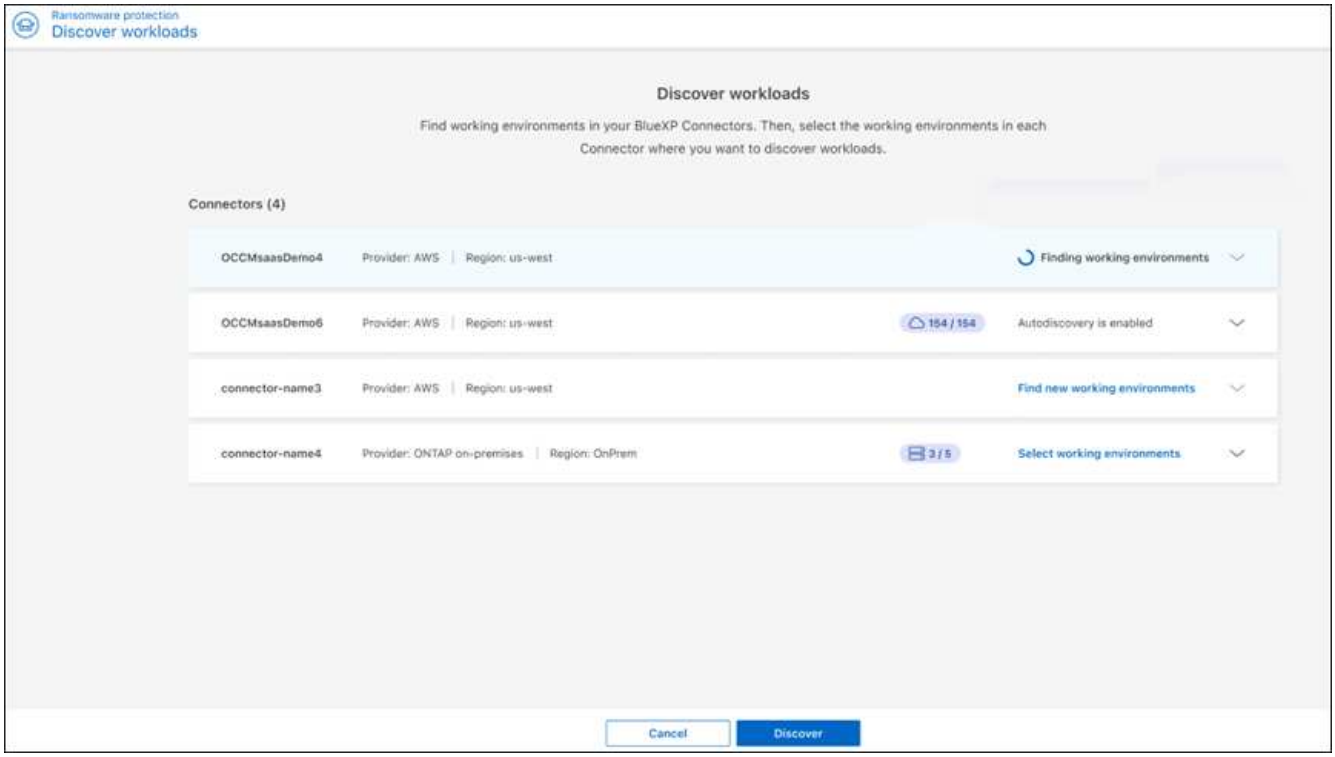
Se você já selecionou ambientes de trabalho para descoberta, poderá descobrir cargas de trabalho recém-criadas para esses ambientes.

Passos

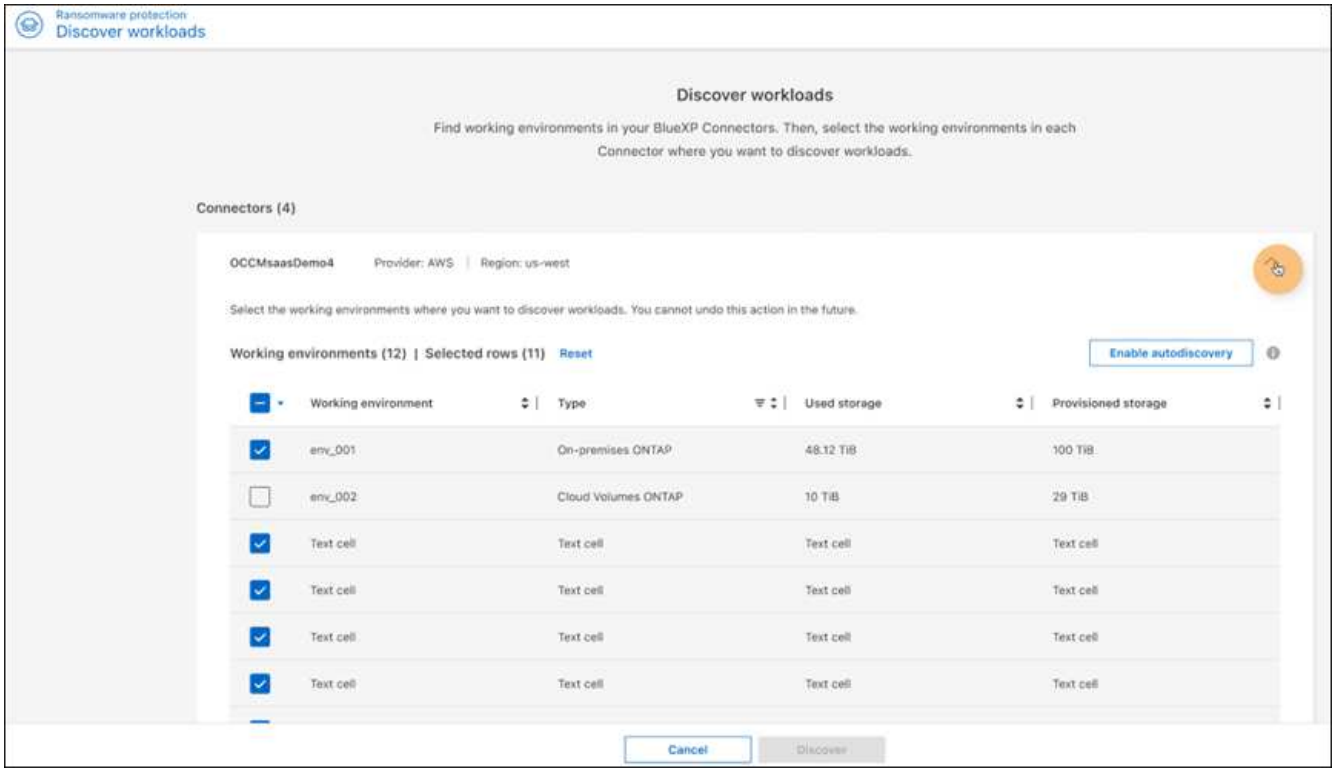
1. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.
2. Para identificar a data da última descoberta, no Dashboard, selecione o ícone de informações ao lado do link **Discover workloads** no canto superior direito.
3. No Dashboard, selecione **Discover cargas de trabalho**.

   Pode visualizar os ambientes de trabalho previamente selecionados para cada conetor e encontrar novos ambientes de trabalho.

4. Para cada conetor, selecione **Localizar novos ambientes de trabalho**.



Este processo pode demorar alguns minutos.



5. Selecione os ambientes de trabalho onde você deseja descobrir workloads ou marque a caixa na parte superior da tabela para descobrir workloads em todos os ambientes de workload descobertos.
6. Selecione **ir para Painel**.

Configurar as configurações de proteção contra ransomware do BlueXP

Você pode configurar um destino de backup, habilitar a deteção de ameaças ou configurar a conexão com a segurança de carga de trabalho do Data Infrastructure Insights acessando a opção **Configurações**. A ativação da deteção de ameaças envia automaticamente dados para o seu sistema de gerenciamento de eventos e segurança (SIEM) para análise de ameaças.

Na página Configurações, você pode fazer o seguinte:

- Configure a conexão com a segurança de workload do Data Infrastructure Insights para ver informações suspeitas de usuários em alertas de ransomware.
- Adicionar um destino de cópia de segurança.
- Conete seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e deteção de ameaças.

Acesse a página Configurações diretamente

Pode aceder facilmente à página Definições a partir da opção ações junto do menu superior.

1. No menu de proteção contra ransomware BlueXP , selecione a opção vertical … no canto superior

direito.

2. No menu suspenso, selecione **Configurações**.

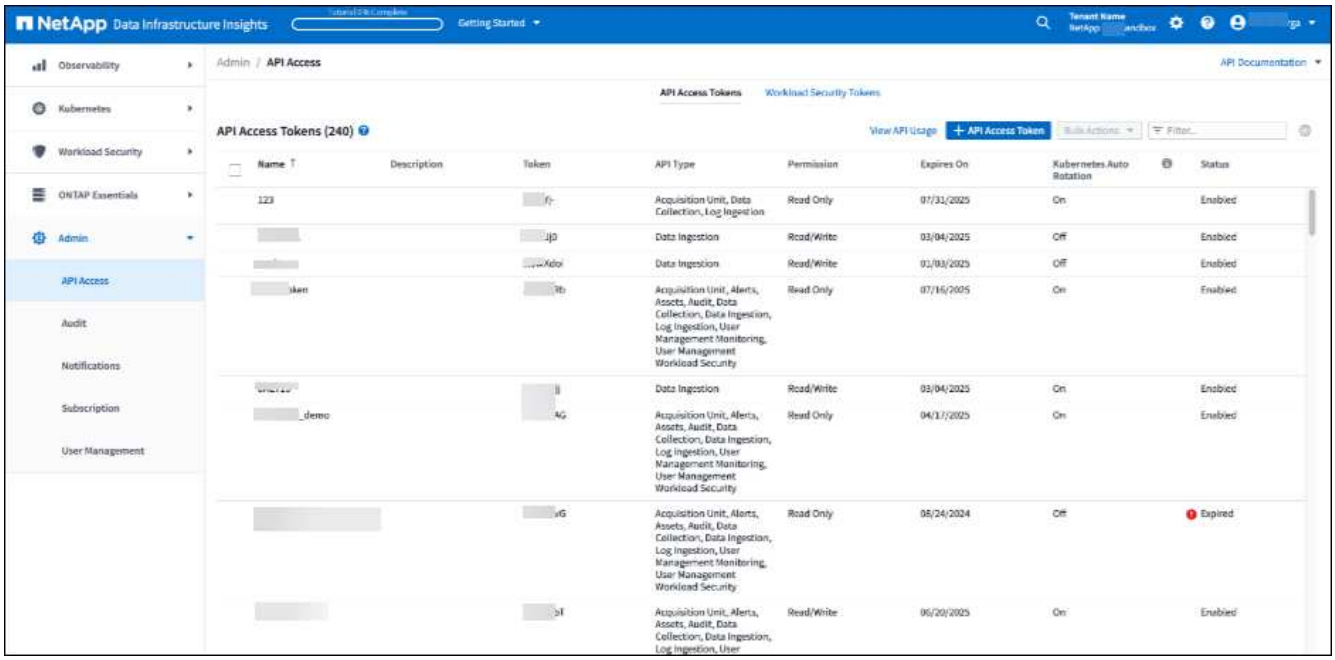
Conecte-se à segurança do workload do Data Infrastructure Insights para ver comportamentos anormais de usuários suspeitos

Antes de visualizar detalhes sobre comportamentos anormais de usuários suspeitos na proteção contra ransomware do BlueXP , é necessário configurar a conexão com o sistema de segurança de workload do Insights da infraestrutura de dados.

Obtenha um token de acesso à API do sistema de segurança Data Infrastructure Insights Workload

Obtenha um token de acesso à API do sistema de segurança Data Infrastructure Insights Workload.

1. Faça login no sistema de segurança de workload do Data Infrastructure Insights.
2. Na navegação à esquerda, selecione **Admin** > **API Access**.



3. Crie um token de acesso à API ou use um já existente.
4. Copie o token de acesso à API.

Conecte-se à segurança de workload do Data Infrastructure Insights

1. No menu Configurações de proteção contra ransomware do BlueXP , selecione **conexão de segurança de carga de trabalho**.
2. Selecione **Connect**.
3. Insira o URL da interface de usuário de segurança de carga de trabalho da infraestrutura de dados.
4. Insira o token de acesso à API que fornece acesso à segurança do Workload.
5. Selecione **Connect**.

Adicionar um destino de cópia de segurança

A proteção contra ransomware do BlueXP identifica workloads que ainda não têm backups e também workloads que ainda não têm destinos de backup atribuídos.

Para proteger esses workloads, você deve adicionar um destino de backup. Você pode escolher um dos seguintes destinos de backup:

- NetApp StorageGRID
- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure

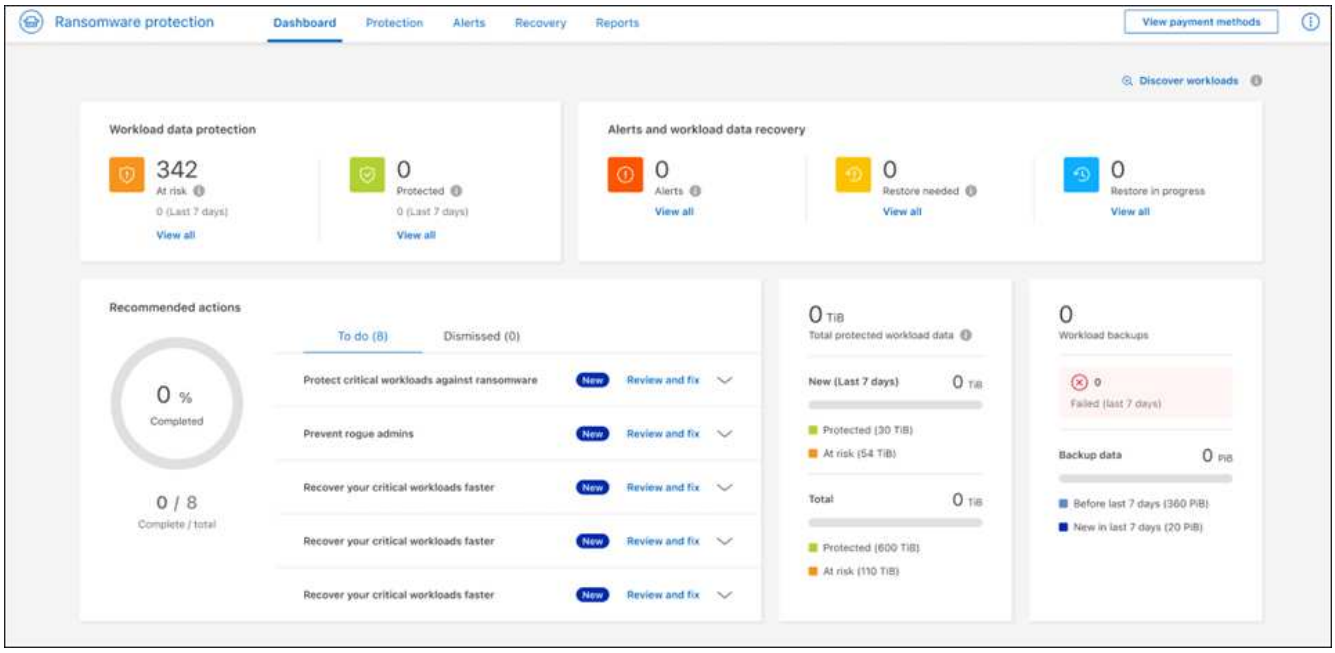
Pode adicionar um destino de cópia de segurança com base numa ação recomendada a partir do Painel de controlo ou a partir do acesso à opção Definições no menu.

Aceda às opções de destino da cópia de segurança a partir das ações recomendadas do Painel de controlo

O Dashboard fornece muitas recomendações. Uma recomendação pode ser configurar um destino de backup.

Passos

1. Na navegação à esquerda do BlueXP , selecione **proteção** > **proteção contra ransomware**.
2. Revise o painel ações recomendadas do Dashboard.



3. No Painel, selecione **Rever e corrigir** para a recomendação de "preparar <backup provider> como destino de backup".
4. Continue com as instruções, dependendo do provedor de backup.

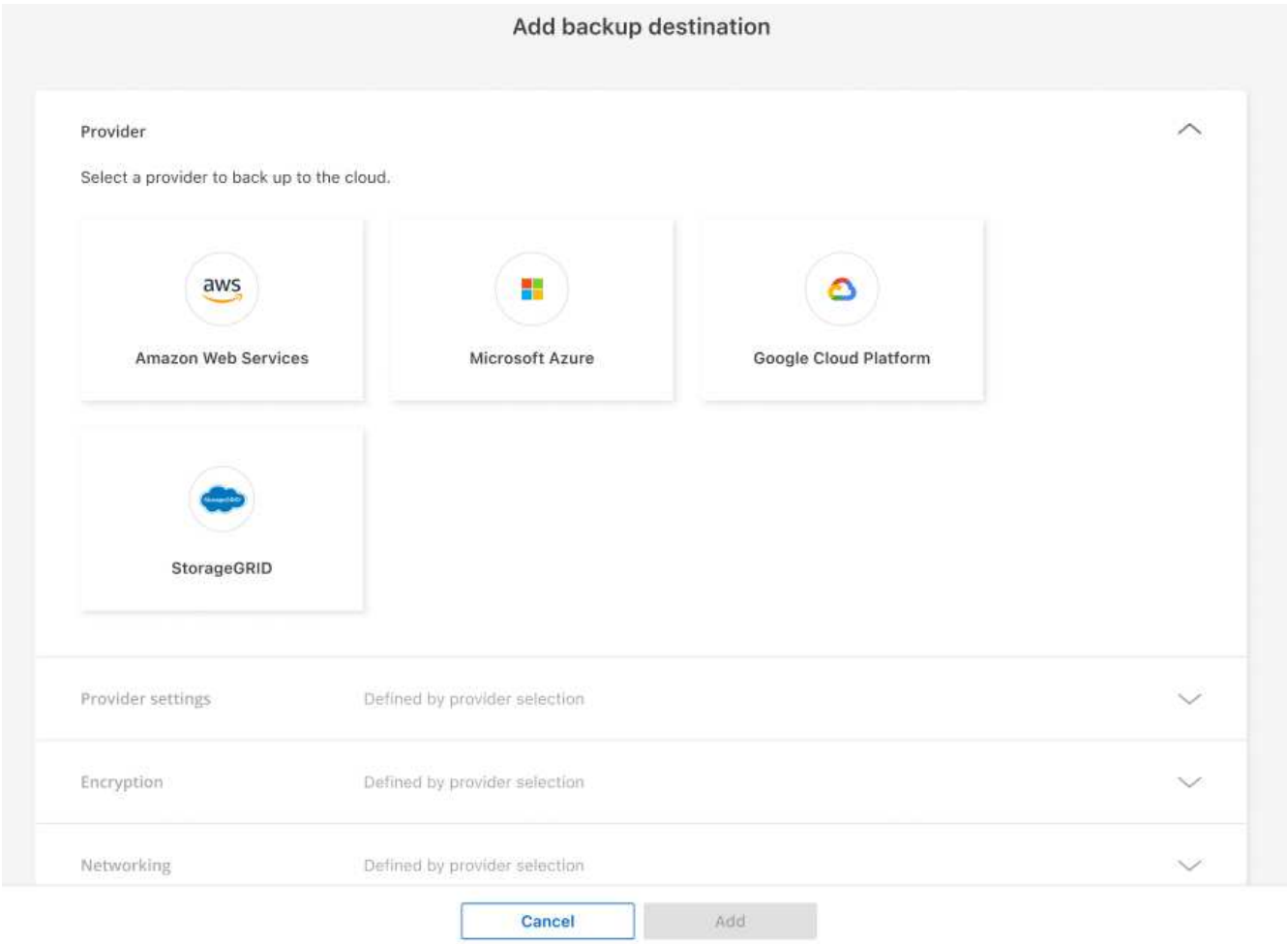
Adicione StorageGRID como destino de backup

Para configurar o NetApp StorageGRID como destino de cópia de segurança, introduza as seguintes

informações.

Passos

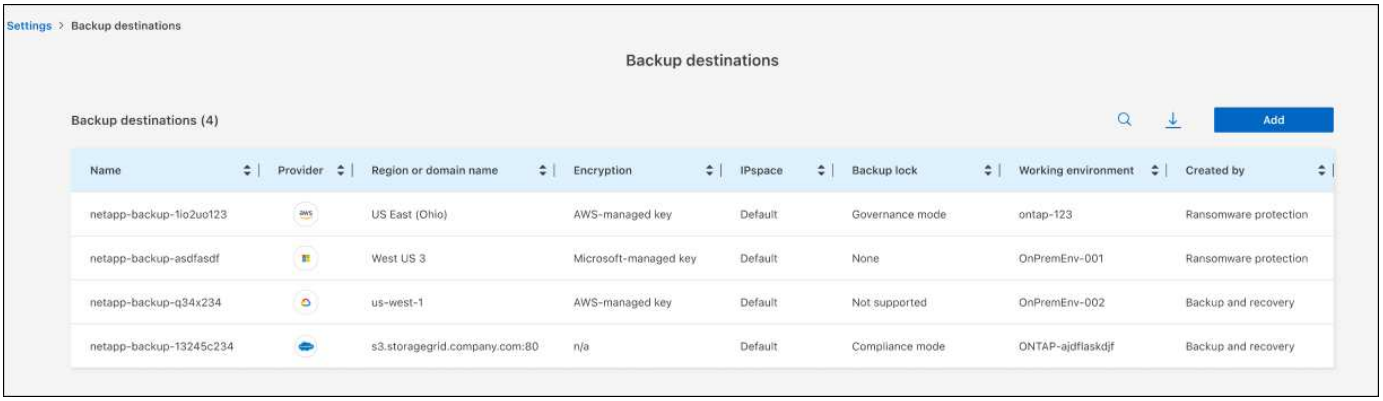
1. Na página **Definições > Destinos de cópia de segurança**, selecione **Adicionar**.
2. Introduza um nome para o destino da cópia de segurança.



3. Selecione **StorageGRID**.
4. Selecione a seta para baixo junto a cada definição e introduza ou selecione valores:
   - * Configurações do provedor*:
     - Crie um novo bucket ou traga seu próprio bucket que armazenará os backups.
     - Nome de domínio, porta, chave de acesso StorageGRID e credenciais de chave secreta totalmente qualificadas do nó de gateway StorageGRID.
   - **Networking**: Escolha o IPspace.
     - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
5. Selecione **Adicionar**.

Resultado

O novo destino de cópia de segurança é adicionado à lista de destinos de cópia de segurança.



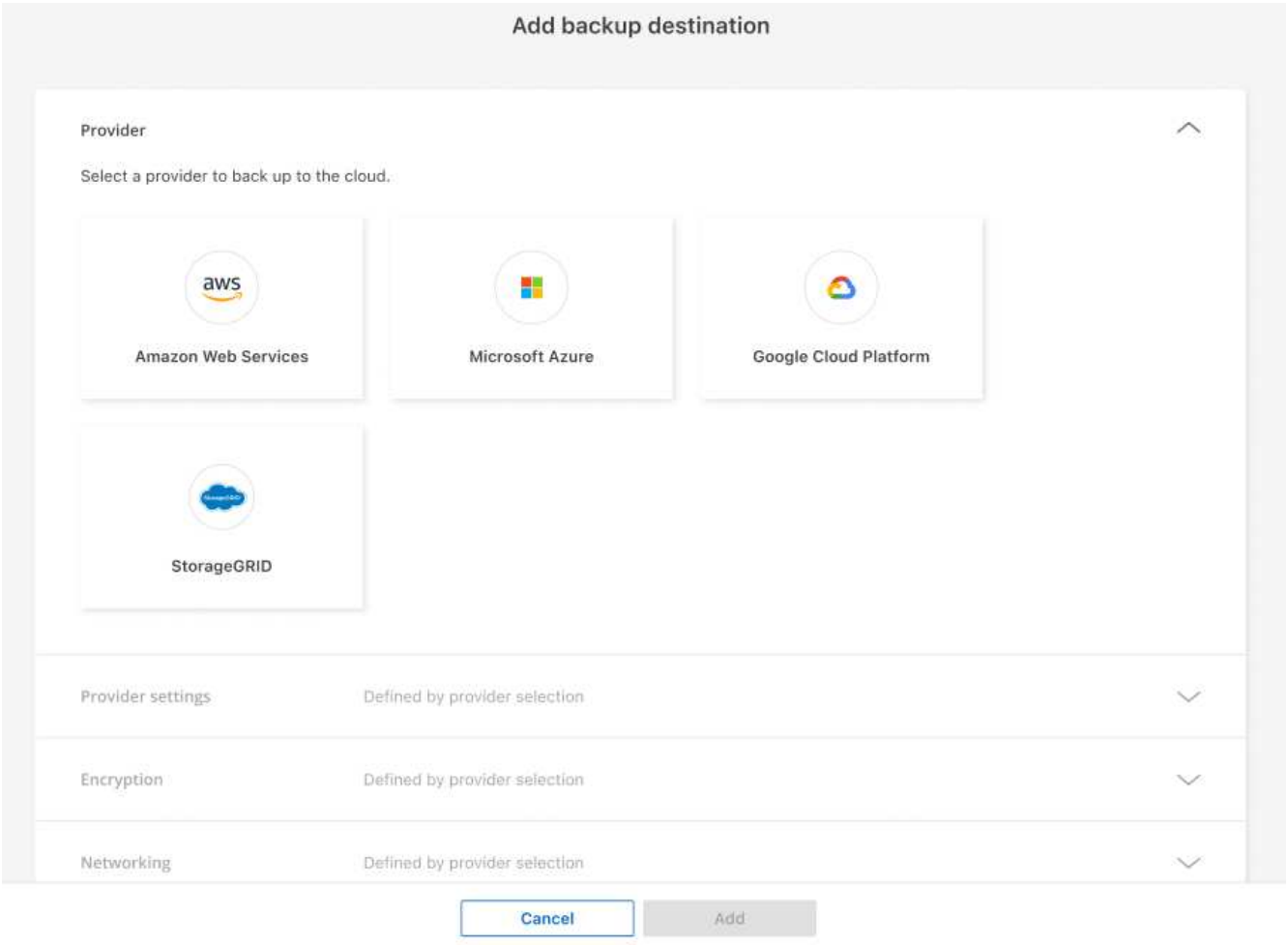
Adicione o Amazon Web Services como destino de backup

Para configurar a AWS como um destino de backup, insira as informações a seguir.

Para obter detalhes sobre como gerenciar seu storage da AWS no BlueXP , "Gerencie seus buckets do Amazon S3" consulte .

Passos

1. Na página **Definições > Destinos de cópia de segurança**, selecione **Adicionar**.
2. Introduza um nome para o destino da cópia de segurança.



3. Selecione **Amazon Web Services**.

4. Selecione a seta para baixo junto a cada definição e introduza ou selecione valores:
   - * Configurações do provedor*:
     - Crie um novo bucket, selecione um bucket existente se já existir um no BlueXP ou traga seu próprio bucket que armazenará os backups.
     - Conta, região, chave de acesso e chave secreta da AWS para credenciais da AWS

       "Se você quiser trazer seu próprio balde, consulte Adicionar baldes S3".
   - **Criptografia**: Se você estiver criando um novo bucket do S3, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis.

     Por padrão, os dados no bucket são criptografados com chaves gerenciadas pela AWS. Você pode continuar usando chaves gerenciadas pela AWS ou gerenciar a criptografia de seus dados usando suas próprias chaves.
   - **Networking**: Escolha o IPspace e se você usará um endpoint privado.
     - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
     - Opcionalmente, escolha se você usará um endpoint privado da AWS (PrivateLink) que você configurou anteriormente.

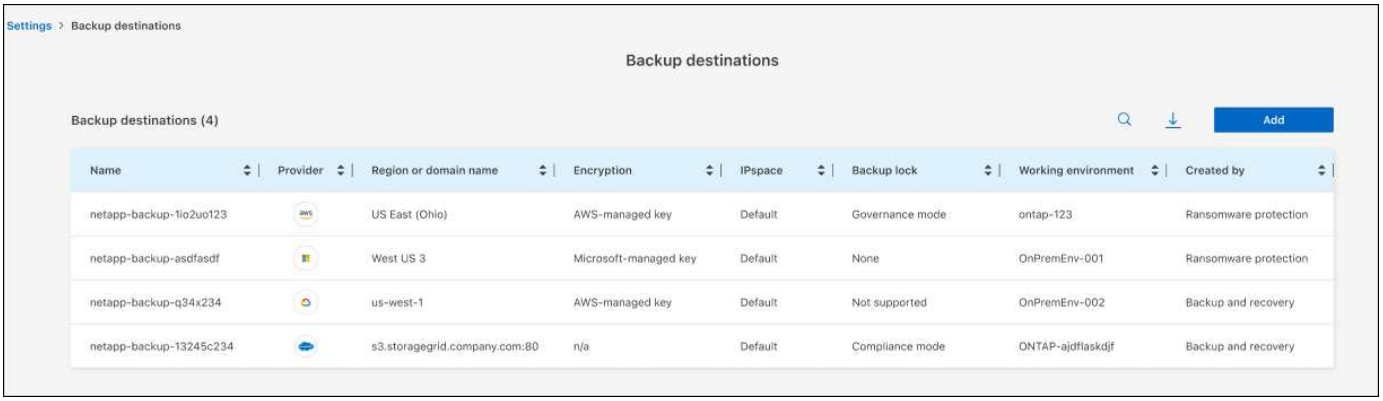
       Se você quiser usar o AWS PrivateLink, "AWS PrivateLink para Amazon S3" consulte .
   - **Bloqueio de backup**: Escolha se você deseja que o serviço proteja os backups de serem modificados ou excluídos. Esta opção usa a tecnologia NetApp DataLock. Cada backup será bloqueado durante o período de retenção, ou por um mínimo de 30 dias, além de um período de buffer de até 14 dias.

     Se você configurar a configuração de bloqueio de backup agora, não poderá alterar a configuração mais tarde depois que o destino de backup for configurado.

     - **Modo de governança**: Usuários específicos (com permissão S3:BypassGovernanceRetention) podem substituir ou excluir arquivos protegidos durante o período de retenção.
     - **Modo de conformidade**: Os usuários não podem substituir ou excluir arquivos de backup protegidos durante o período de retenção.
5. Selecione **Adicionar**.

Resultado

O novo destino de cópia de segurança é adicionado à lista de destinos de cópia de segurança.



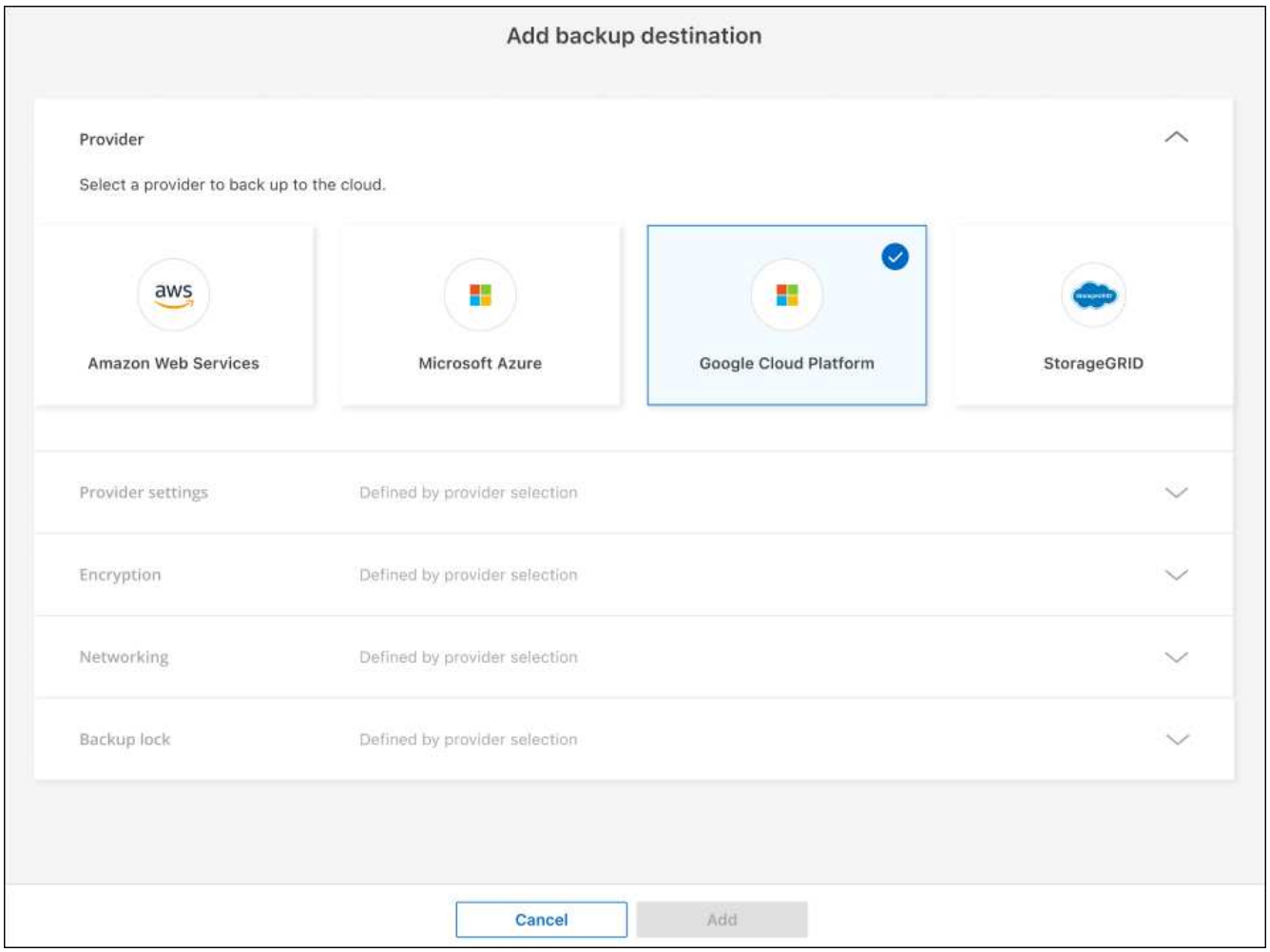
Adicione o Google Cloud Platform como destino de backup

Para configurar o Google Cloud Platform (GCP) como destino de backup, insira as informações a seguir.

Para obter detalhes sobre como gerenciar o armazenamento do GCP no BlueXP , "Opções de instalação do conetor no Google Cloud" consulte .

Passos

1. Na página **Definições > Destinos de cópia de segurança**, selecione **Adicionar**.
2. Introduza um nome para o destino da cópia de segurança.



3. Selecione **Google Cloud Platform**.
4. Selecione a seta para baixo junto a cada definição e introduza ou selecione valores:
   - * Configurações do provedor*:
     - Crie um novo bucket. Introduza a chave de acesso e a chave secreta.
     - Insira ou selecione seu projeto e região do Google Cloud Platform.
   - **Criptografia**: Se você estiver criando um novo bucket, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis.

     Os dados no intervalo são criptografados com chaves gerenciadas pelo Google por padrão. Você pode continuar a usar as chaves gerenciadas pelo Google.

   - **Networking**: Escolha o IPspace e se você usará um endpoint privado.
     - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
     - Opcionalmente, escolha se você usará um endpoint privado do GCP (PrivateLink) que você configurou anteriormente.
5. Selecione **Adicionar**.

Resultado

O novo destino de cópia de segurança é adicionado à lista de destinos de cópia de segurança.

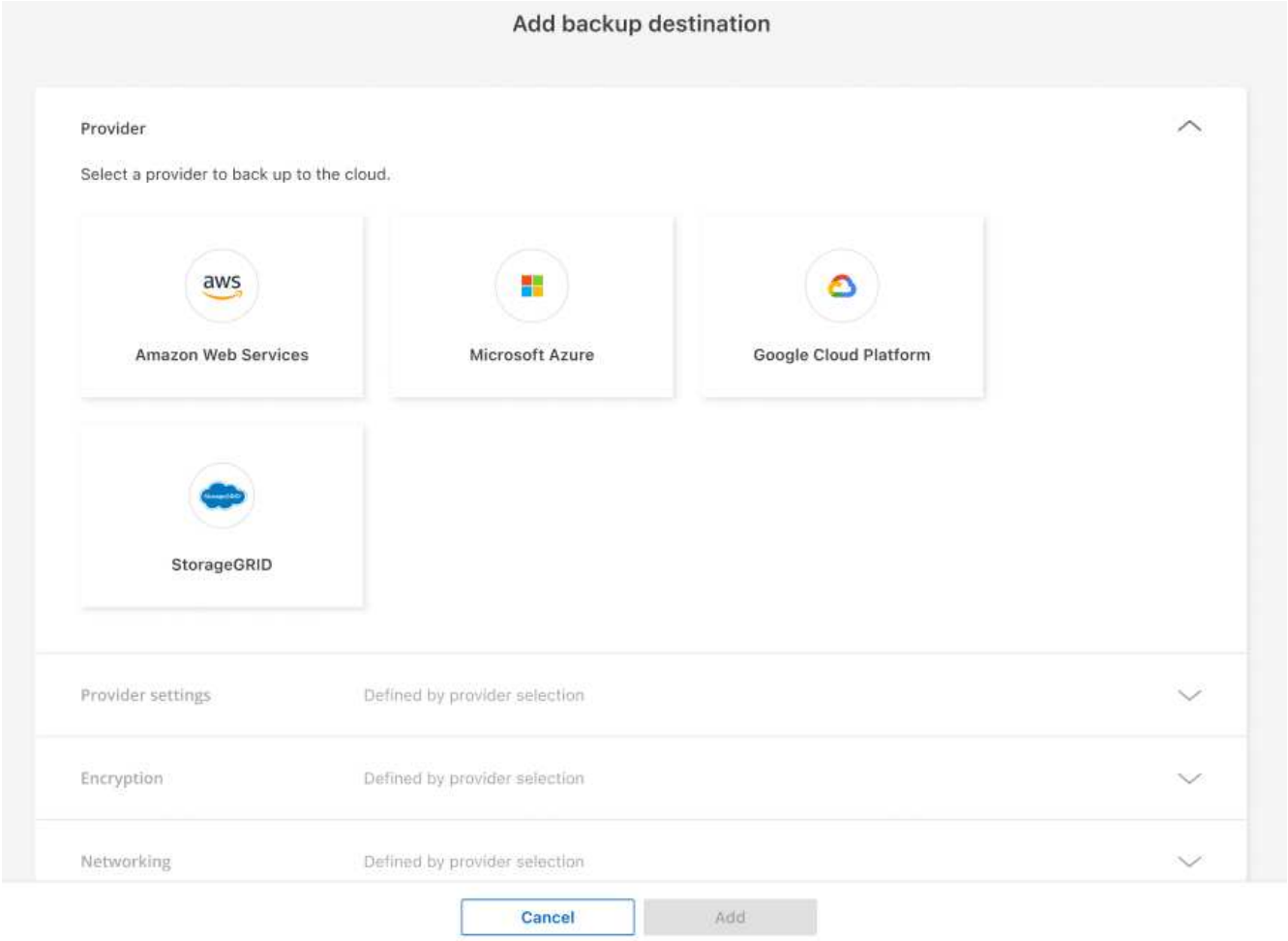
Adicione o Microsoft Azure como destino de backup

Para configurar o Azure como um destino de backup, insira as seguintes informações.

Para obter detalhes sobre como gerenciar suas credenciais do Azure e assinaturas de marketplace no BlueXP , "Gerencie suas credenciais do Azure e assinaturas do marketplace" consulte .

Passos

1. Na página **Definições > Destinos de cópia de segurança**, selecione **Adicionar**.
2. Introduza um nome para o destino da cópia de segurança.



3. Selecione **Azure**.
4. Selecione a seta para baixo junto a cada definição e introduza ou selecione valores:
   - * Configurações do provedor*:
     - Crie uma nova conta de armazenamento, selecione uma existente se já existir uma no BlueXP ou traga sua própria conta de armazenamento que armazenará os backups.
     - Subscrição, região e grupo de recursos do Azure para credenciais do Azure

       "Se você quiser trazer sua própria conta de storage, consulte Adicionar contas de armazenamento de Blob do Azure".
   - **Criptografia**: Se você estiver criando uma nova conta de armazenamento, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolher uma conta existente, as informações de criptografia já estarão disponíveis.

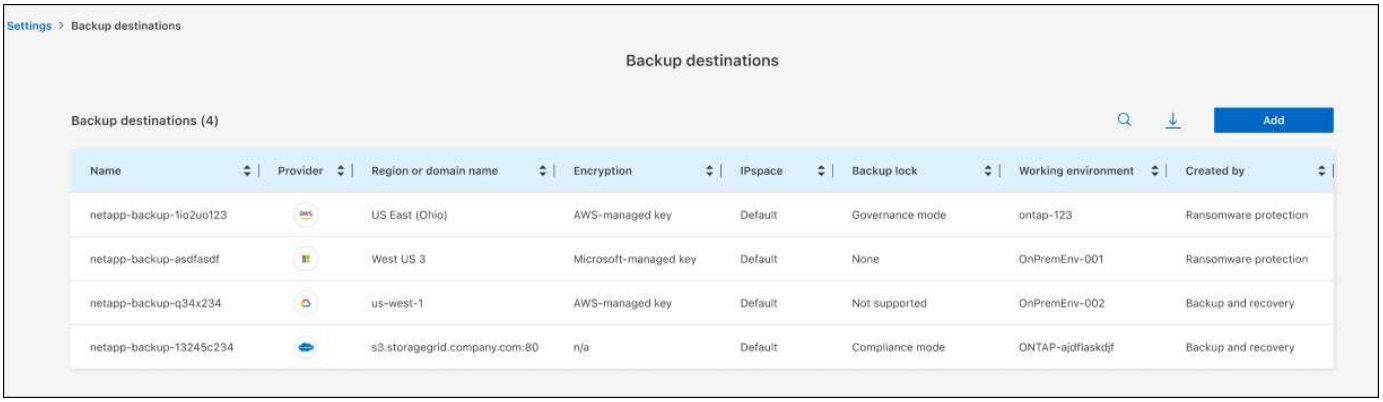
     Por padrão, os dados na conta são criptografados com chaves gerenciadas pela Microsoft. Pode continuar a utilizar chaves geridas pela Microsoft ou pode gerir a encriptação dos seus dados utilizando as suas próprias chaves.
   - **Networking**: Escolha o IPspace e se você usará um endpoint privado.
     - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
     - Opcionalmente, escolha se você usará um endpoint privado do Azure que você configurou anteriormente.

Se você quiser usar o Azure PrivateLink, "Azure PrivateLink" consulte .

5. Selecione **Adicionar**.

Resultado

O novo destino de cópia de segurança é adicionado à lista de destinos de cópia de segurança.



Ativar a deteção de ameaças

Você pode enviar dados automaticamente para o seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e deteção de ameaças. Você pode selecionar o AWS Security Hub, o Microsoft Sentinel ou o Splunk Cloud como seu SIEM.

Antes de ativar a proteção contra ransomware BlueXP , você precisa configurar seu sistema SIEM.

Configure o AWS Security Hub para deteção de ameaças

Antes de ativar o AWS Security Hub na proteção contra ransomware do BlueXP , você precisará fazer as seguintes etapas de alto nível no AWS Security Hub:

- Configurar permissões no AWS Security Hub.
- Configure a chave de acesso de autenticação e a chave secreta no AWS Security Hub. (Estes passos não são fornecidos aqui.)

Etapas para configurar permissões no AWS Security Hub

1. Vá para **Console do AWS IAM**.
2. Selecione **políticas**.
3. Crie uma política usando o seguinte código no formato JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Configure o Microsoft Sentinel para deteção de ameaças

Antes de ativar o Microsoft Sentinel na proteção contra ransomware do BlueXP , você precisará fazer as seguintes etapas de alto nível no Microsoft Sentinel:

- * Pré-requisitos*
  - Ative o Microsoft Sentinel.
  - Crie uma função personalizada no Microsoft Sentinel.
- **Inscrição**
  - Registre a proteção contra ransomware BlueXP para receber eventos do Microsoft Sentinel.
  - Crie um segredo para o Registro.
- **Permissões**: Atribua permissões ao aplicativo.
- **Autenticação**: Insira credenciais de autenticação para o aplicativo.

Passos para ativar o Microsoft Sentinel

1. Vá para Microsoft Sentinel.
2. Crie um espaço de trabalho **Log Analytics**.
3. Habilite o Microsoft Sentinel para usar o espaço de trabalho Log Analytics que você acabou de criar.

Etapas para criar uma função personalizada no Microsoft Sentinel

1. Vá para Microsoft Sentinel.
2. Selecione **Subscription** > **Access Control (IAM)**.
3. Introduza um nome de função personalizado. Use o nome **Configurador Sentinel de proteção contra ransomware BlueXP** .
4. Copie o JSON a seguir e cole-o na guia **JSON**.

```
{
  "roleName": "BlueXP Ransomware Protection Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Reveja e guarde as suas definições.

Etapas para Registrar a proteção contra ransomware do BlueXP para receber eventos do Microsoft Sentinel

1. Vá para Microsoft Sentinel.
2. Selecione **Entra ID** > **aplicações** > **inscrições de aplicações**.
3. Para o **Nome de exibição** para o aplicativo, digite "**proteção contra ransomware BlueXP** ".
4. No campo **Supported account type** (tipo de conta suportado), selecione **Accounts in this organizational Directory only** (apenas contas neste diretório organizacional).
5. Selecione um **índice padrão** onde os eventos serão enviados.
6. Selecione **Revisão**.
7. Selecione **Register** para salvar suas configurações.

   Após o Registro, o centro de administração do Microsoft Entra exibe o painel Visão geral do aplicativo.

Passos para criar um segredo para o registo

1. Vá para Microsoft Sentinel.
2. Selecione **certificados e segredos** > **Segredos do cliente** > **segredo do novo cliente**.
3. Adicione uma descrição para o segredo do seu aplicativo.
4. Selecione um **Expiration** para o segredo ou especifique uma vida útil personalizada.

   Uma vida secreta do cliente é limitada a dois anos (24 meses) ou menos. A Microsoft recomenda que você defina um valor de expiração inferior a 12 meses.

5. Selecione **Adicionar** para criar seu segredo.
6. Registre o segredo a ser usado na etapa Autenticação. O segredo nunca é exibido novamente depois de sair desta página.

Etapas para atribuir permissões ao aplicativo

1. Vá para Microsoft Sentinel.
2. Selecione **Subscription** > **Access Control (IAM)**.
3. Selecione **Adicionar** > **Adicionar atribuição de função**.
4. Para o campo **funções de administrador privilegiadas**, selecione **Configurador Sentinela de proteção contra ransomware BlueXP** .

Esta é a função personalizada que você criou anteriormente.

5. Selecione **seguinte**.
6. No campo **Assign Access to**, selecione **User, group ou Service Principal**.
7. Selecione **Selecionar Membros**. Em seguida, selecione **BlueXP ransomware Protection Sentinel Configurator**.
8. Selecione **seguinte**.
9. No campo **o que o usuário pode fazer**, selecione **permitir que o usuário atribua todas as funções, exceto as funções de administrador privilegiado Owner, UAA, RBAC (recomendado)**.
10. Selecione **seguinte**.
11. Selecione **Rever e atribuir** para atribuir as permissões.

Passos para introduzir credenciais de autenticação para a aplicação

1. Vá para Microsoft Sentinel.
2. Introduza as credenciais:
   a. Insira o ID do locatário, o ID do aplicativo do cliente e o segredo do aplicativo do cliente.
   b. Clique em **Authenticate**.

   Depois que a autenticação for bem-sucedida, é apresentada uma mensagem "autenticada".

3. Insira os detalhes da área de trabalho do Log Analytics para o aplicativo.
   a. Selecione a ID da assinatura, o grupo de recursos e a área de trabalho Log Analytics.

Configurar o Splunk Cloud para detecção de ameaças

Antes de ativar a proteção contra ransomware do BlueXP , você precisará seguir as etapas de alto nível abaixo:

- Habilite um coletor de eventos HTTP no Splunk Cloud para receber dados de eventos via HTTP ou HTTPS do BlueXP .
- Criar um token de Event Collector no Splunk Cloud.

Etapas para habilitar um coletor de eventos HTTP no Splunk

1. Vá para o Splunk Cloud.
2. Selecione **Definições** > **entradas de dados**.
3. Selecione **Coletor de eventos HTTP** > **Configurações globais**.
4. Na alternância todos os tokens, selecione **ativado**.
5. Para que o Event Collector ouça e se comunique por HTTPS em vez de HTTP, selecione **Ativar SSL**.
6. Insira uma porta em **número da porta HTTP** para o coletor de eventos HTTP.

Etapas para criar um token de Event Collector no Splunk

1. Vá para o Splunk Cloud.
2. Selecione **Definições** > **Adicionar dados**.

3. Selecione **Monitor** > **Coletor de eventos HTTP**.
4. Digite um Nome para o token e selecione **Next**.
5. Selecione um **índice padrão** onde os eventos serão enviados e, em seguida, selecione **Revisão**.
6. Confirme se todas as configurações para o endpoint estão corretas e selecione **Enviar**.
7. Copie o token e cole-o em outro documento para que ele esteja pronto para a etapa Autenticação.

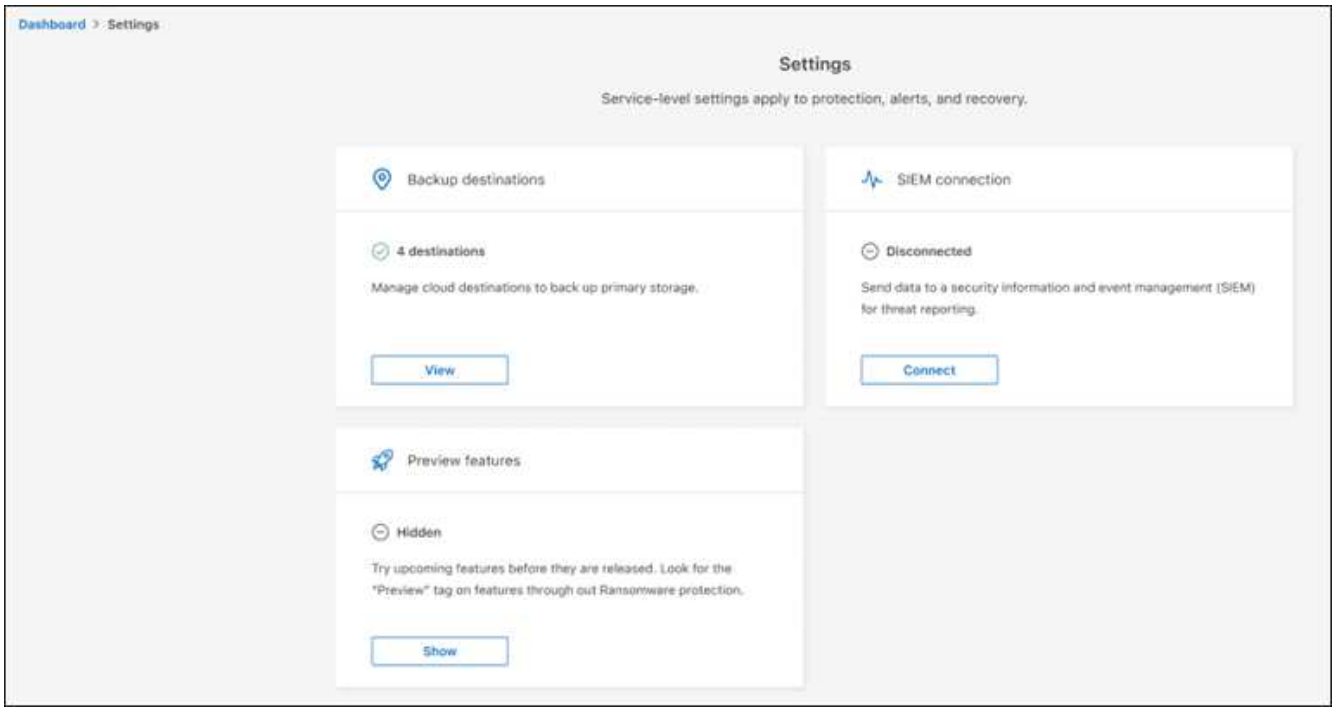
Conete SIEM na proteção contra ransomware BlueXP

A ativação DO SIEM envia dados da proteção contra ransomware BlueXP para seu servidor SIEM para análise e geração de relatórios de ameaças.

Passos

1. No menu BlueXP , selecione **proteção** > **proteção contra ransomware**.
2. No menu de proteção contra ransomware BlueXP , selecione a opção vertical … no canto superior direito.
3. Selecione **Definições**.

   A página Configurações é exibida.



4. Na página Configurações, selecione **conetar** no bloco de conexão SIEM.

5. Escolha um dos sistemas SIEM.
6. Insira os detalhes de token e autenticação configurados no AWS Security Hub ou Splunk Cloud.

   As informações inseridas dependem do SIEM selecionado.

7. Selecione **Ativar**.

   A página Configurações mostra "conectado".

Perguntas frequentes sobre proteção contra ransomware do BlueXP

Este FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

Implantação

- Você precisa de uma licença para usar a proteção contra ransomware BlueXP ?*

Você pode usar os seguintes tipos de licença:

- Inscreva-se para uma avaliação gratuita de 30 dias.
- Compre uma assinatura PAYGO (pay-as-you-go) com o Amazon Web Services (AWS) Marketplace, o Google Cloud Marketplace e o Microsoft Azure Marketplace (em breve).
- Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém de seu representante de vendas da NetApp Você pode usar o número de série da licença para ativar o BYOL na carteira digital BlueXP .

Como você ativa a proteção contra ransomware do BlueXP ? A proteção contra ransomware da BlueXP não exige capacitação. A opção de proteção contra ransomware é ativada automaticamente na navegação à esquerda do BlueXP .

Para começar, você precisa se inscrever ou entrar em Contato com seu representante de vendas da NetApp para experimentar este serviço. Em seguida, quando você usar o BlueXP Connector, ele incluirá os recursos

apropriados para o serviço.

Para começar a usar a proteção contra ransomware do BlueXP , clique em "Iniciar a descoberta de cargas de trabalho" na página inicial.

A proteção contra ransomware do BlueXP está disponível nos modos padrão, restrito e privado? No momento, a proteção contra ransomware BlueXP está disponível apenas no modo padrão. Fique atento para mais.

Para obter uma explicação sobre esses modos em todos os serviços BlueXP , "Modos de implantação do BlueXP" consulte .

Acesso

- Qual é a URL de proteção contra ransomware do BlueXP ?* Para o URL, em um navegador, digite: "https://console.bluexp.netapp.com/ransomware-protection" Para acessar o console do BlueXP .

Como as permissões de acesso são tratadas? Somente os administradores da organização podem iniciar o serviço e descobrir cargas de trabalho (porque isso envolve o compromisso com o uso de um recurso). Interações subsequentes podem ser feitas por qualquer função.

Qual é a melhor resolução do dispositivo? A resolução recomendada do dispositivo para a proteção contra ransomware BlueXP é 1920x1080 ou melhor.

Qual navegador devo usar? Qualquer navegador moderno funcionará.

Interação com outros serviços

A proteção contra ransomware BlueXP está ciente das configurações de proteção feitas no NetApp ONTAP? Sim, a proteção contra ransomware do BlueXP descobre as programações de snapshot definidas no ONTAP.

Se você definir uma política usando a proteção contra ransomware do BlueXP , você precisa fazer alterações futuras apenas neste serviço? Recomendamos que você faça alterações de política em relação ao serviço de proteção contra ransomware da BlueXP .

Como a proteção contra ransomware do BlueXP interage com o backup e recuperação do BlueXP e o SnapCenter?

A proteção contra ransomware da BlueXP usa os seguintes produtos e serviços:

- Backup e recuperação do BlueXP para descobrir e definir políticas de snapshot e backup para workloads de compartilhamento de arquivos
- O SnapCenter ou o SnapCenter para VMware podem descobrir e definir políticas de snapshot e backup para workloads de aplicações e VMs.

Além disso, a proteção contra ransomware do BlueXP usa backup e recuperação do BlueXP e o SnapCenter / SnapCenter para VMware para executar recuperação consistente com arquivos e workloads.

Workloads

O que compõe uma carga de trabalho? Uma carga de trabalho é uma aplicação, uma VM ou um compartilhamento de arquivos. Um workload inclui todos os volumes usados por uma única instância de aplicação. Por exemplo, uma instância do Oracle DB implantada no ora3.host.com pode ter vol1 e vol2 para

seus dados e logs, respetivamente. Esses volumes juntos constituem a carga de trabalho para essa instância específica da instância do Oracle DB.

Como a proteção contra ransomware do BlueXP prioriza os dados da carga de trabalho? A prioridade de dados é determinada pelas cópias Snapshot feitas e pelos backups programados.

A prioridade da carga de trabalho (crítica, padrão, importante) é determinada pelas frequências Snapshot já aplicadas a cada volume associado à carga de trabalho.

"Saiba mais sobre prioridade ou importância da carga de trabalho".

Quais cargas de trabalho a proteção contra ransomware BlueXP é compatível?

A proteção contra ransomware do BlueXP identifica os seguintes workloads: Oracle, MySQL, compartilhamentos de arquivos, VMs e datastores de VM.

Além disso, se o cliente estiver usando o SnapCenter ou o SnapCenter para VMware, todos os workloads com suporte desses produtos também serão identificados na proteção contra ransomware da BlueXP e na proteção contra ransomware da BlueXP poderão protegê-los e recuperá-los de maneira consistente com o workload.

Como você associa dados a uma carga de trabalho?

A proteção contra ransomware da BlueXP associa dados a um workload das seguintes maneiras:

- A proteção contra ransomware do BlueXP descobre os volumes e as extensões de arquivos e os associa à carga de trabalho apropriada.
- Além disso, se você tiver o SnapCenter ou o SnapCenter para VMware e tiver workloads configurados no backup e recuperação do BlueXP , a proteção contra ransomware da BlueXP detetará os workloads gerenciados pelo SnapCenter e SnapCenter para VMware e seus volumes associados.

O que é uma carga de trabalho "protegida"? Na proteção contra ransomware do BlueXP , um workload mostra um status "protegido" quando tem uma política de detecção primária habilitada. Por enquanto, isso significa que o ARP está ativado em todos os volumes relacionados à carga de trabalho.

O que é uma carga de trabalho "em risco"? Se uma carga de trabalho não tiver uma política de detecção primária habilitada, ela estará "em risco" mesmo que tenha uma política de backup e snapshot habilitada.

Novo volume adicionado, mas ainda não aparece se você adicionou um novo volume ao seu ambiente, inicie a descoberta novamente e aplique políticas de proteção para proteger esse novo volume.

O Dashboard não mostra todas as minhas cargas de trabalho. O que pode estar errado? Atualmente, apenas são suportados volumes NFS e CIFS. Os volumes iSCSI e outras configurações não suportadas são filtrados e não aparecem no Dashboard.

Políticas de proteção

As políticas de ransomware do BlueXP coexistem com os outros tipos de políticas de carga de trabalho? No momento, o backup e a recuperação do BlueXP (backup em nuvem) são compatíveis com uma política de backup por volume. Portanto, backup e recuperação do BlueXP e proteção contra ransomware BlueXP compartilham políticas de backup.

As cópias snapshot não são limitadas e podem ser adicionadas separadamente de cada serviço.

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 .

A proteção contra ransomware BlueXP está ciente das configurações de proteção feitas no NetApp ONTAP?

Sim, a proteção contra ransomware do BlueXP descobre as programações de snapshot definidas no ONTAP e se o ARP e o FPolicy estão ativados em todos os volumes em um workload descoberto. As informações que você vê inicialmente no Painel são agregadas de outras soluções e produtos da NetApp.

A proteção contra ransomware da BlueXP está ciente das políticas já feitas no backup e recuperação do BlueXP e no SnapCenter?

Sim, se você tiver workloads gerenciados no backup e recuperação do BlueXP ou no SnapCenter, as políticas gerenciadas por esses produtos são trazidas para a proteção contra ransomware do BlueXP .

Você pode modificar políticas transferidas do backup e recuperação do BlueXP e/ou do SnapCenter?

Não, você não pode modificar políticas gerenciadas pelo backup e recuperação do BlueXP ou pelo SnapCenter na proteção contra ransomware do BlueXP . Você gerencia quaisquer alterações nessas políticas no backup e recuperação do BlueXP ou no SnapCenter.

Se existirem políticas do ONTAP (já ativadas no System Manager, como ARP, FPolicy e snapshots), essas políticas são alteradas na proteção contra ransomware BlueXP ?

Não. A proteção contra ransomware BlueXP não modifica nenhuma política de deteção existente (ARP, configurações FPolicy) do ONTAP.

O que acontece se você adicionar novas políticas no backup e recuperação do BlueXP ou no SnapCenter depois de se inscrever para a proteção contra ransomware do BlueXP ?

A proteção contra ransomware do BlueXP reconhece todas as novas políticas criadas no backup e recuperação do BlueXP ou no SnapCenter.

Você pode alterar as políticas do ONTAP?

Sim, você pode alterar as políticas do ONTAP na proteção contra ransomware do BlueXP . Também é possível criar novas políticas na proteção contra ransomware do BlueXP e aplicá-las a workloads. Essa ação substitui as políticas atuais da ONTAP pelas políticas criadas na proteção contra ransomware do BlueXP .

Você pode desativar políticas?

Você pode desativar o ARP em políticas de deteção usando a IU, APIs ou CLI do System Manager.

Você pode desativar as políticas de FPolicy e backup aplicando uma política diferente que não as inclua.

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 proteçãoão".

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.

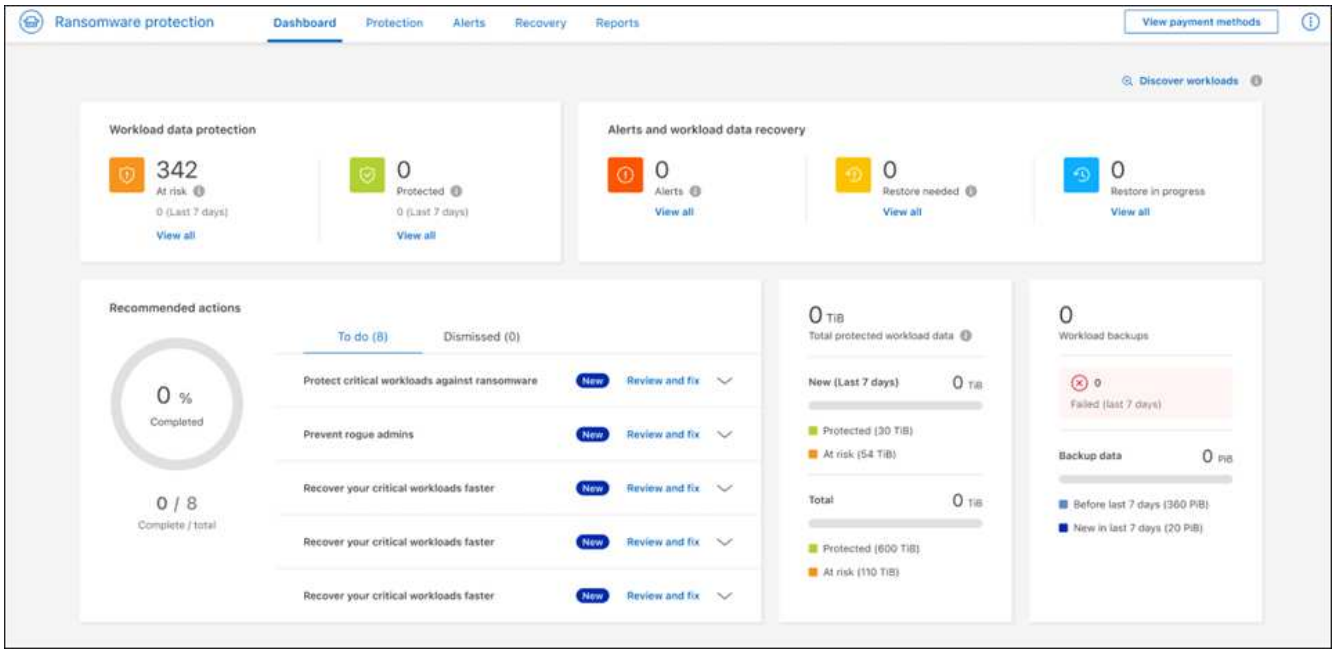
Você também pode usar o Painel para analisar e agir de acordo com as recomendações de proteção, acessar configurações globais, fazer download de relatórios e acessar esta documentação técnica.

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 .
Conete-se ao SEIM para relatórios de ameaças.	Envie dados para um sistema de gerenciamento de eventos e segurança (SIEM) para análise e deteção de ameaças.	Insira os detalhes do servidor SIEM/XDR para habilitar a deteção de ameaças. "Configure as definições de proteçãoão"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 deteção 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 proteçãoão"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:

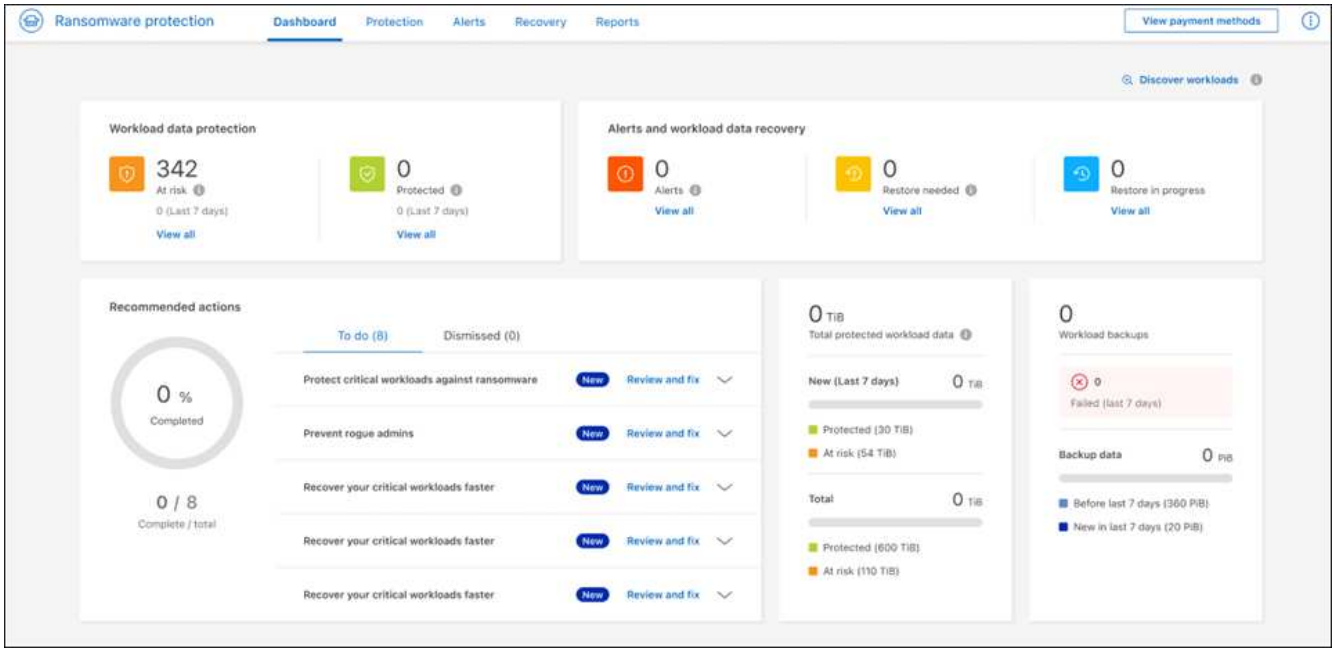
- **Proteção**: Contém o status e detalhes de todas as cargas de trabalho, incluindo o número total protegido e em risco.
- **Alertas**: Inclui o status e detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação**: Inclui o status e os detalhes de 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**.



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)**.

Acesse 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 .

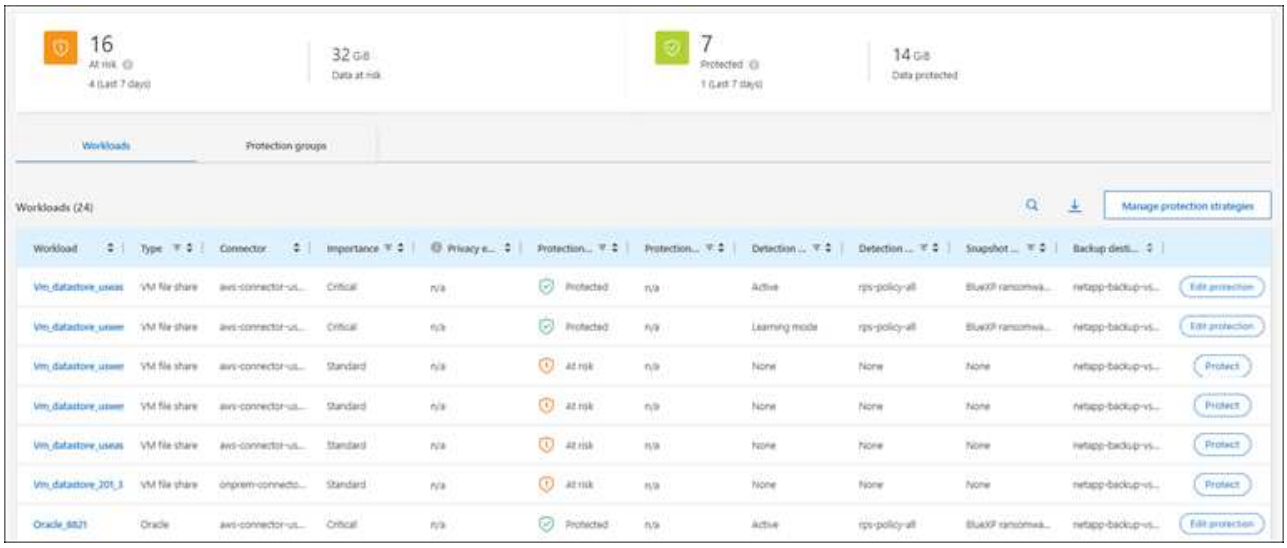
Ver a proteção contra ransomware em um workload

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**.



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

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

Detalhes de proteção na página proteção

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

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

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

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

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

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

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

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

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

Importância da carga de trabalho

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

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

Políticas de deteção predefinidas

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

Nível de política	Snapshot	Frequência	Retenção (dias)	nº de cópias snapshot	Número máximo total de cópias snapshot
Política de carga 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 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 deteção para cargas de trabalho que já tenham políticas de snapshot e backup**, que são gerenciadas em outros produtos ou serviços da NetApp. A política de deteção não alterará as políticas gerenciadas em outros produtos.

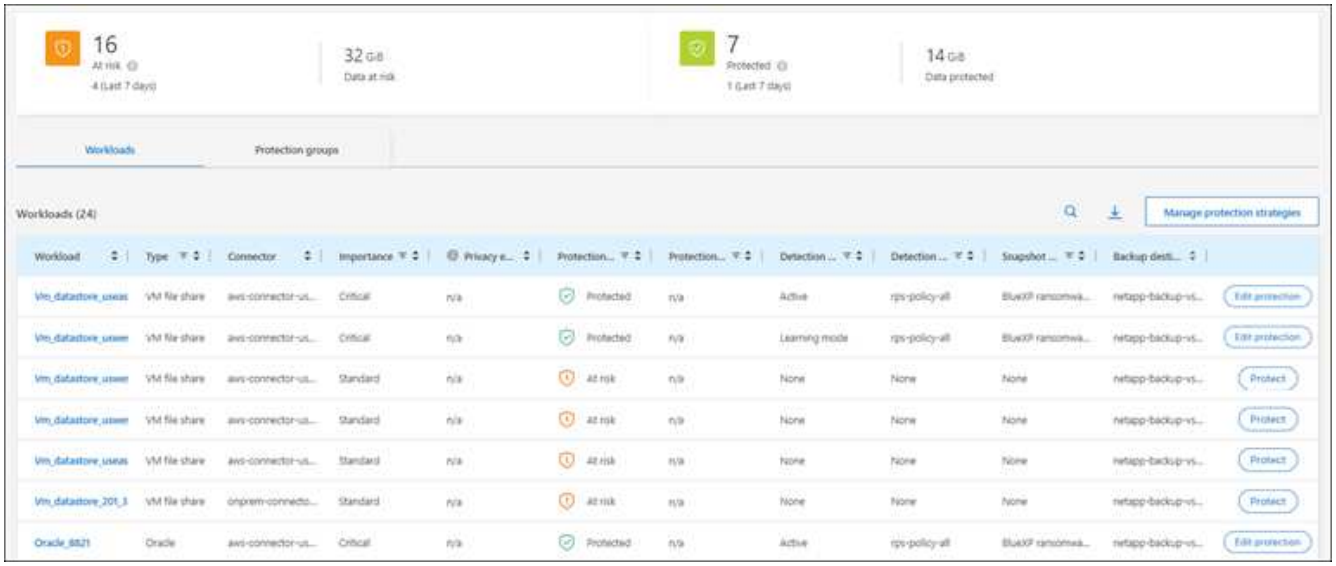
Criar uma estratégia de proteção contra ransomware (se você não tiver políticas de snapshot ou backup)

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

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

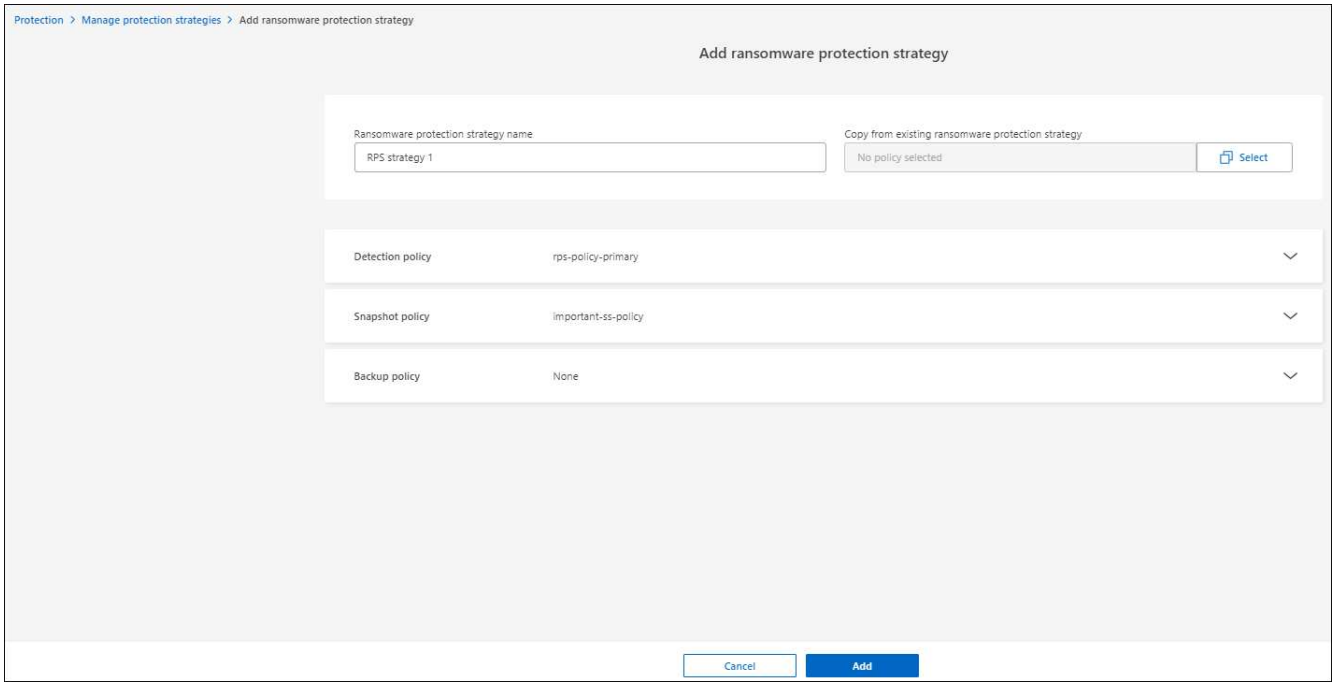
Etapas para criar uma estratégia de proteção contra ransomware

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



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

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



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

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

5. Para cada item, selecione a **seta para baixo**.

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

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

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

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

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

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

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

6. Selecione **Adicionar**.

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

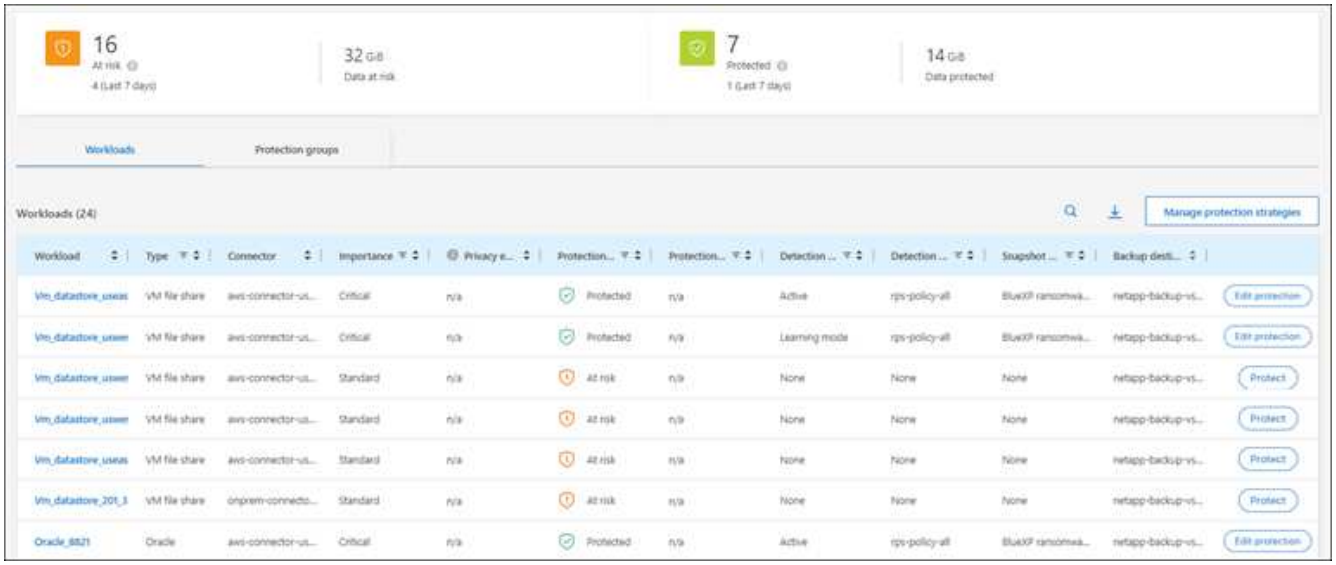
Com a proteção contra ransomware do BlueXP , você pode atribuir uma política de detecção de ransomware a workloads que já tenham políticas de snapshot e backup, gerenciados em outros produtos ou serviços da NetApp. A política de deteção não alterará as políticas gerenciadas em outros produtos.

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

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

Passos

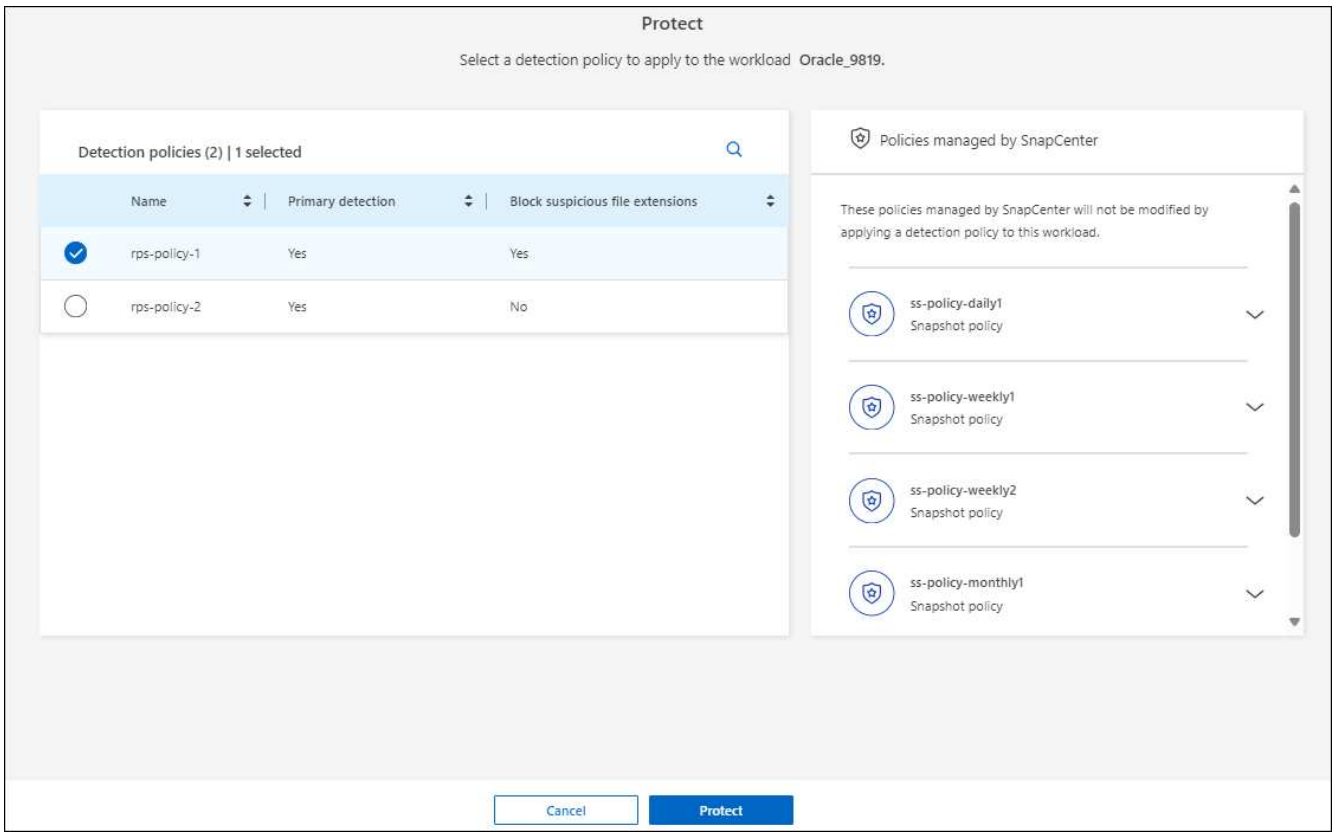
1. No menu proteção contra ransomware BlueXP , selecione **proteção**.



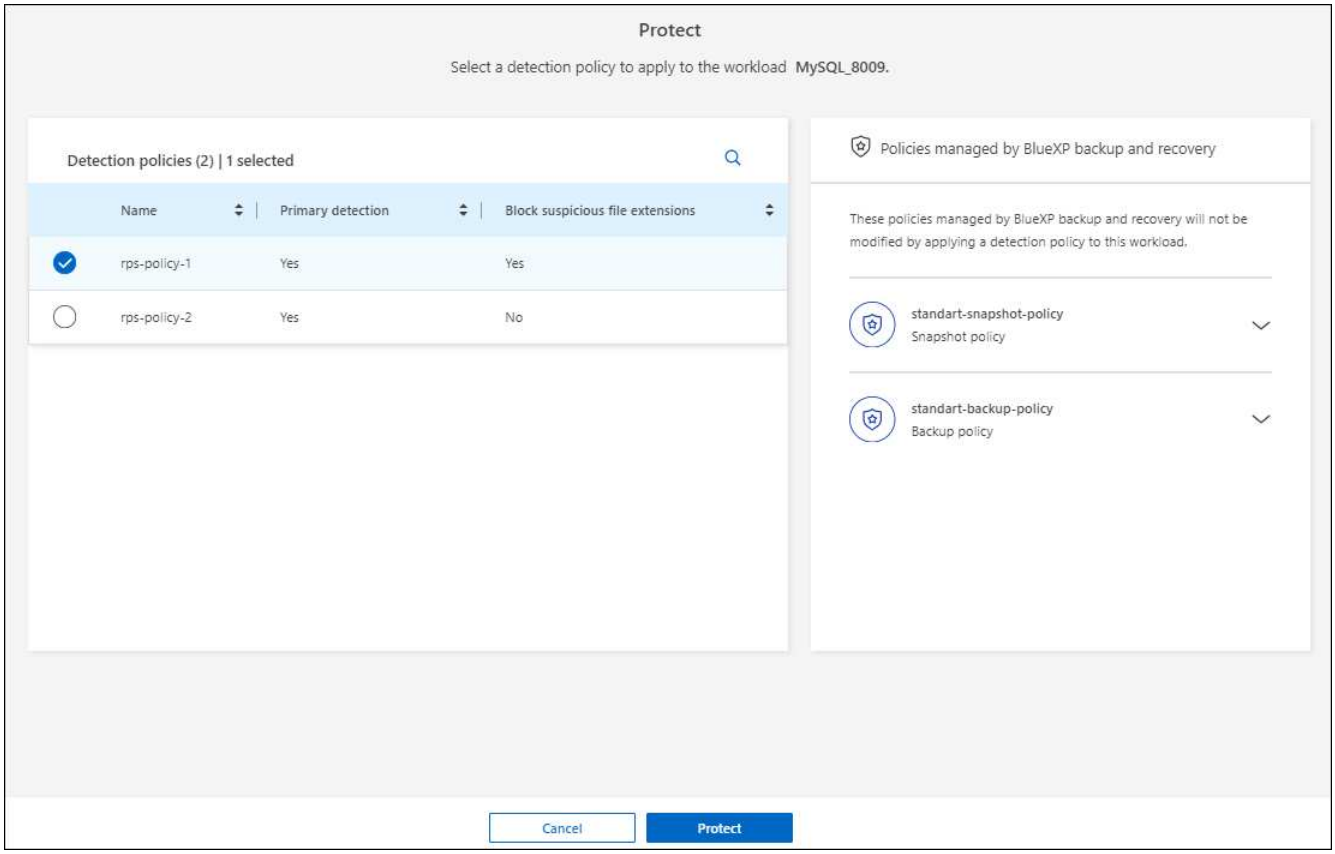
2. Na página proteção, selecione uma carga de trabalho e selecione **proteger**.

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

Atribua uma política diferente

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

Passos

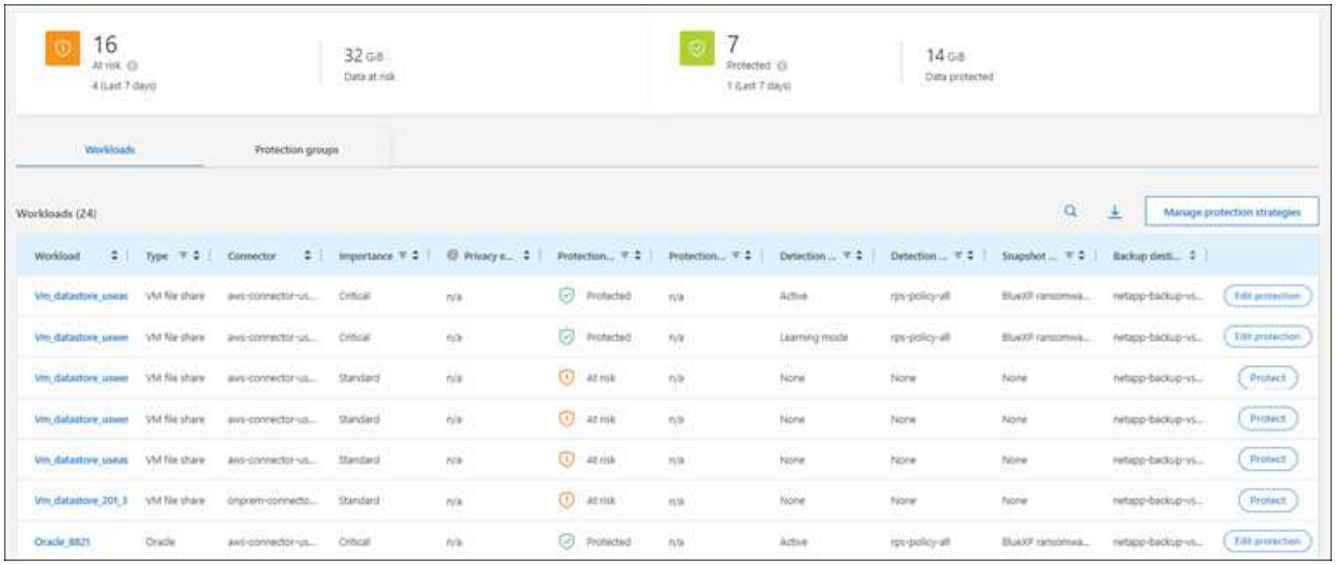
1. No menu proteção contra ransomware BlueXP , selecione **proteção**.
2. Na página proteção, na linha carga de trabalho, selecione **Editar proteção**.
3. Na página políticas, clique na seta para baixo da política que você deseja atribuir para revisar os detalhes.
4. Selecione a política que pretende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

Compartilhe arquivos de grupo para facilitar a proteção

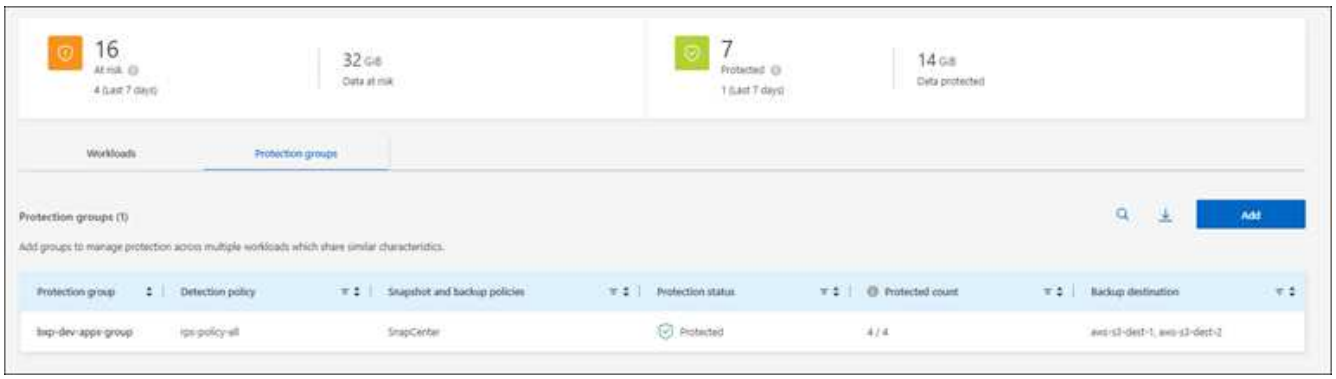
Agrupar compartilhamentos de arquivos facilita a proteção de seu data Estate. O serviço pode proteger todos os volumes em um grupo ao mesmo tempo em vez de proteger cada volume separadamente.

Passos

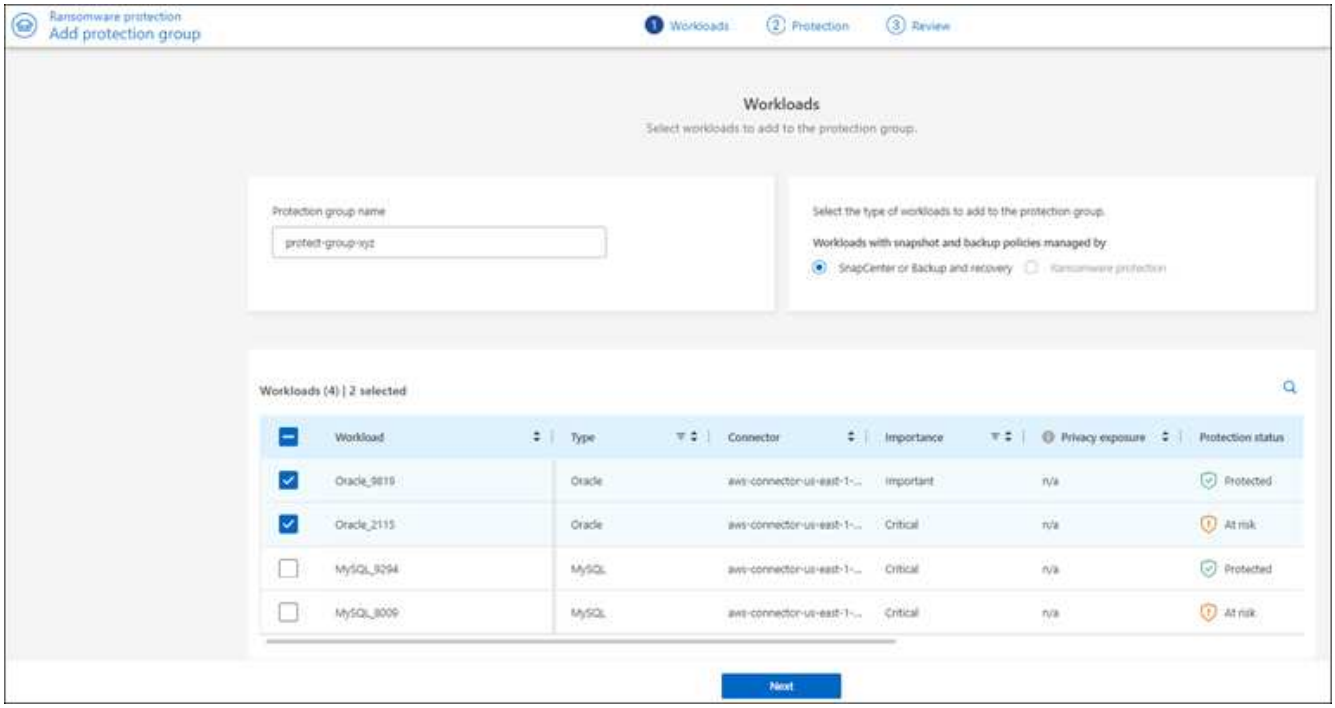
1. No menu proteção contra ransomware BlueXP , selecione **proteção**.



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



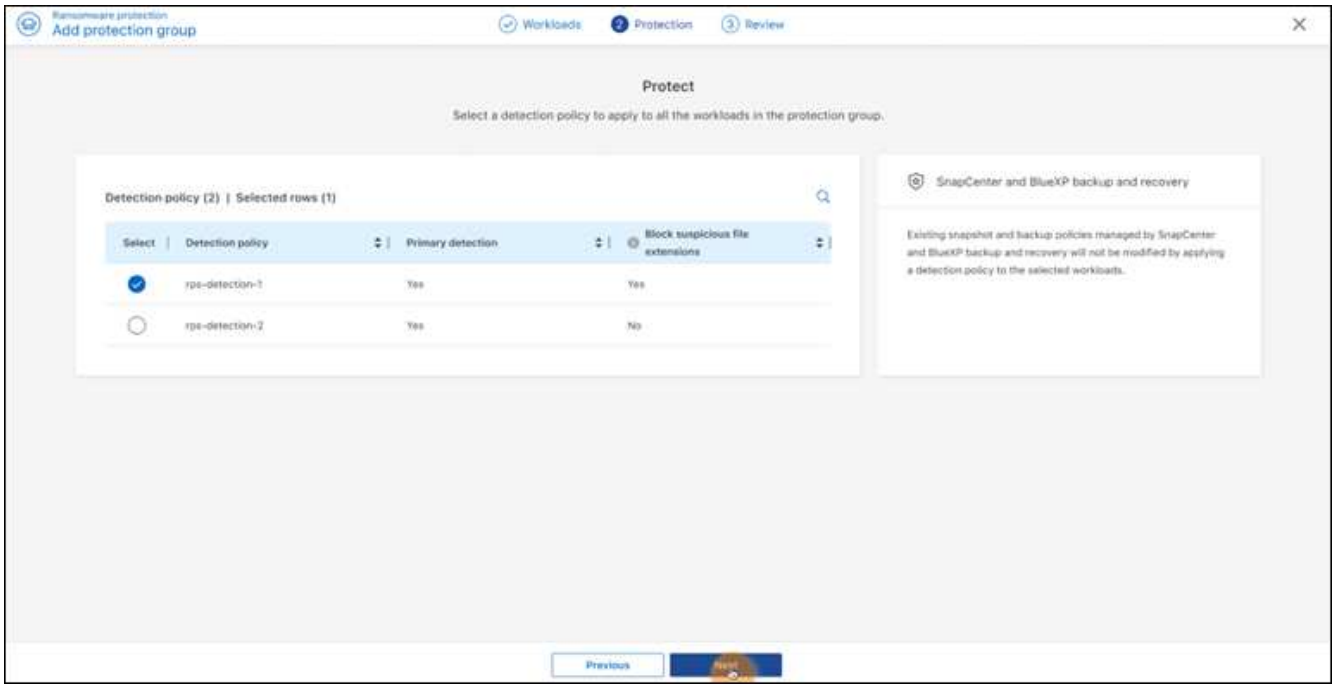
3. Selecione **Adicionar**.



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

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

7. Selecione **seguinte**.



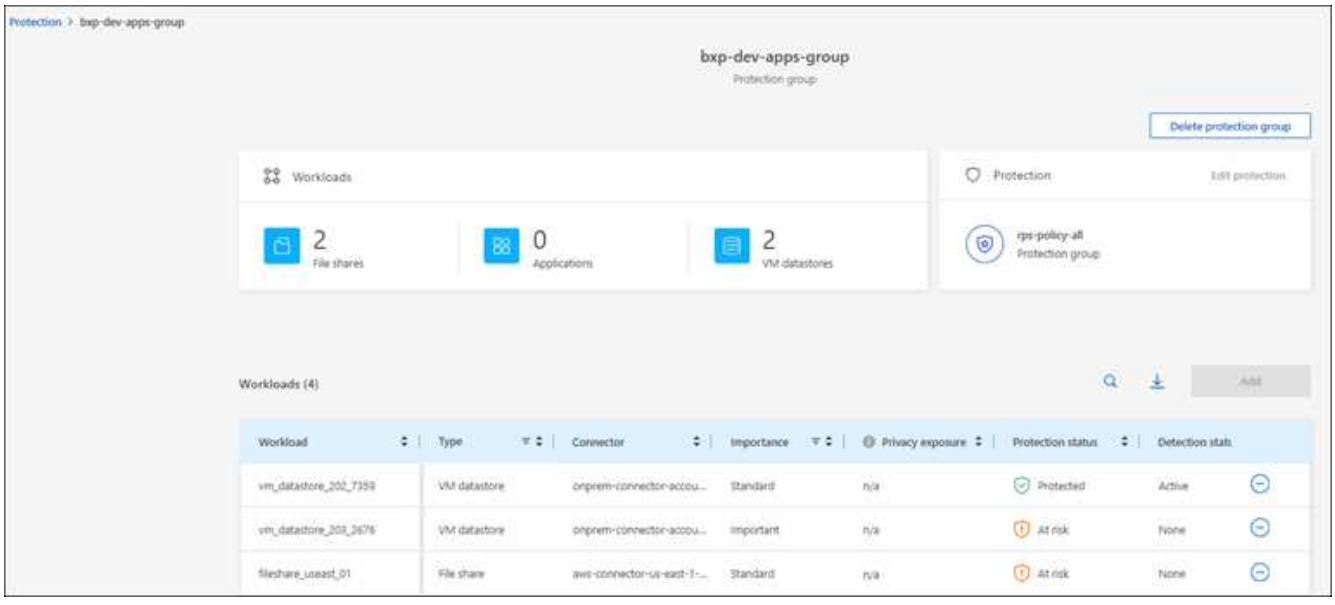
8. Selecione a política que governará a proteção para este grupo.
9. Selecione **seguinte**.
10. Reveja as seleções para o grupo de proteçãoão.
11. Selecione **Adicionar**.

Remover workloads de um grupo

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

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.



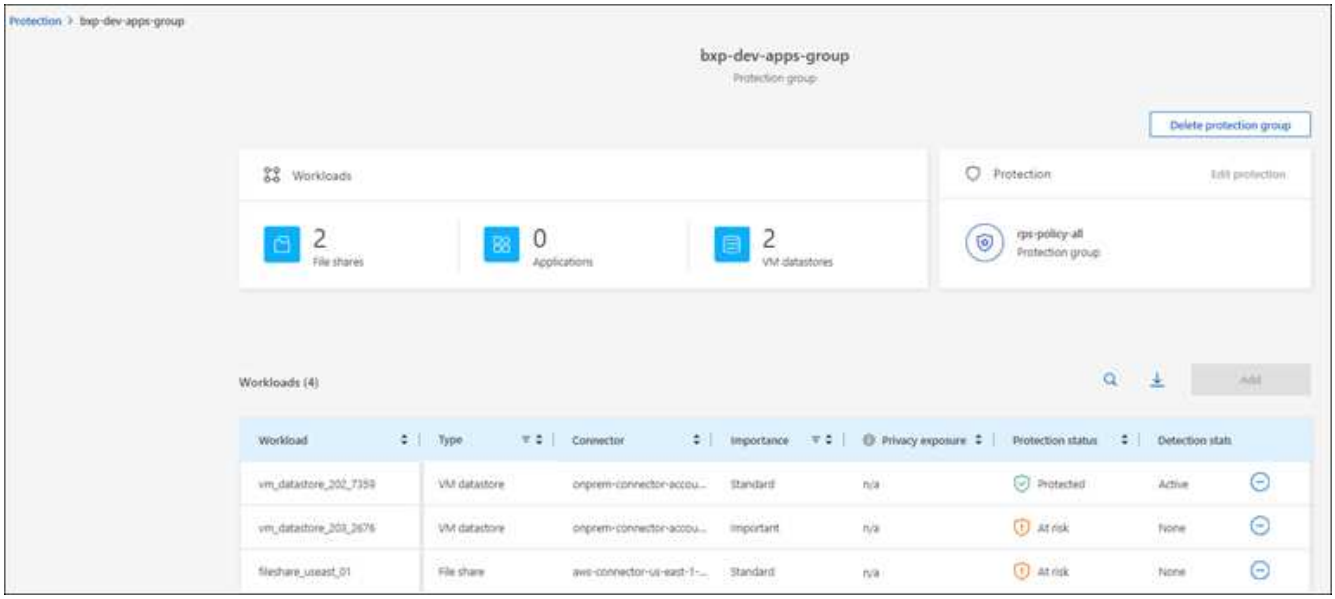
4. Na página do grupo de proteção selecionado, selecione a carga de trabalho que deseja remover do grupo e selecione a opção *ações*•••.
5. No menu ações, selecione **Remover carga de trabalho**.
6. Confirme se deseja remover a carga de trabalho e selecione **Remover**.

Elimine o grupo de proteçãoão

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

Passos

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



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.

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:

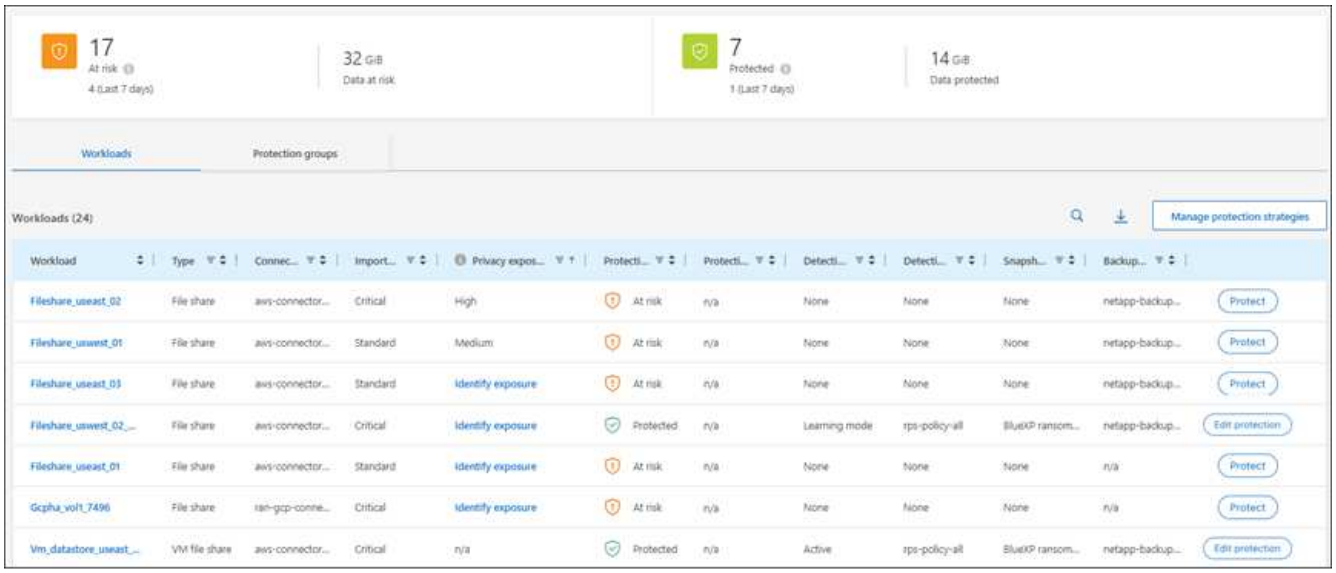
- "Saiba mais sobre a classificação BlueXP"
- "Categorias de dados privados"
- "Investigue os dados armazenados em sua organização"

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.



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.

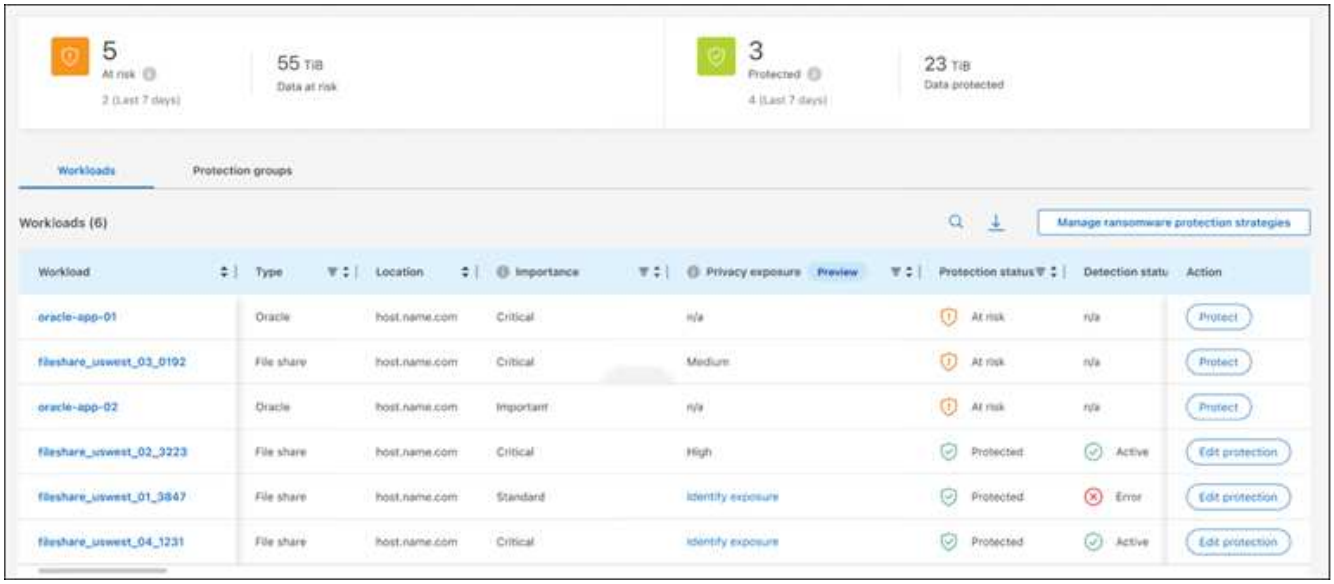
Os dados PII podem ter um dos seguintes Estados de risco de exposição à privacidade.

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

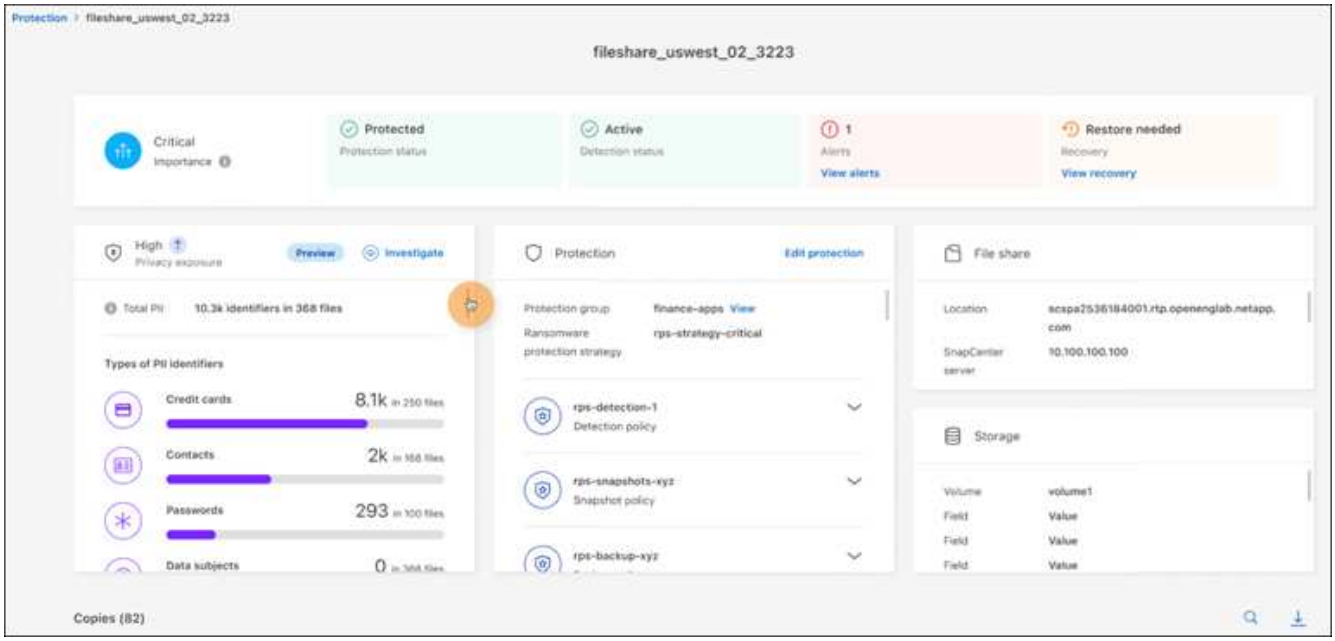
- * Baixo *: Maior que 0 e menos de 30% dos arquivos têm PII

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
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 deteção 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.

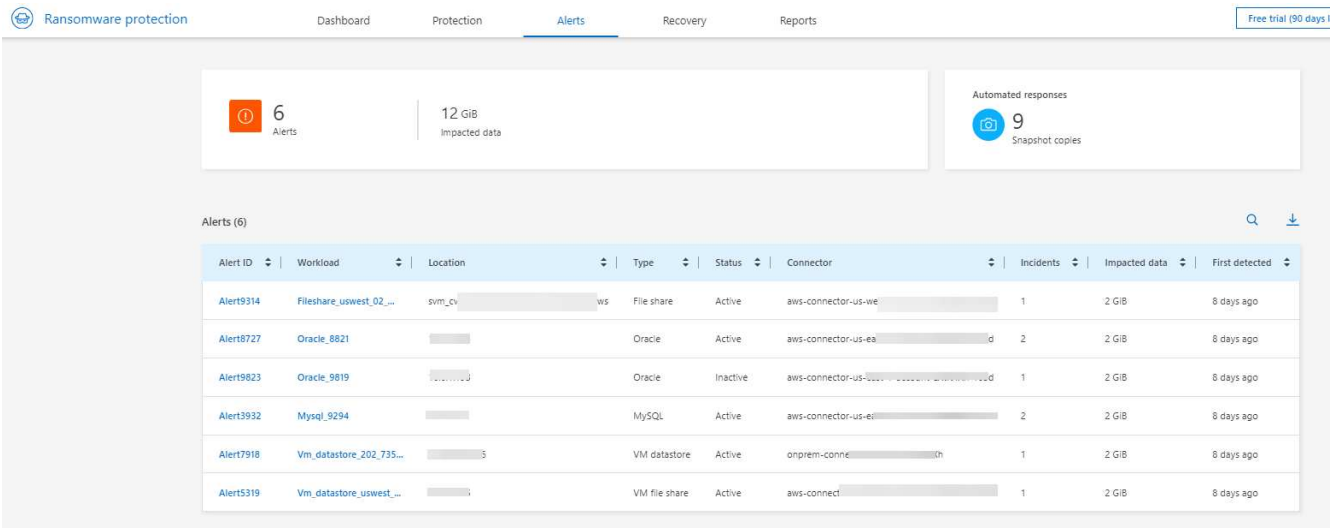
- **Dismissing**: O incidente está em processo de desistência.
- **Resolvido**: O incidente foi mitigado.

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.



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 deteta 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 Infrastuture 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.

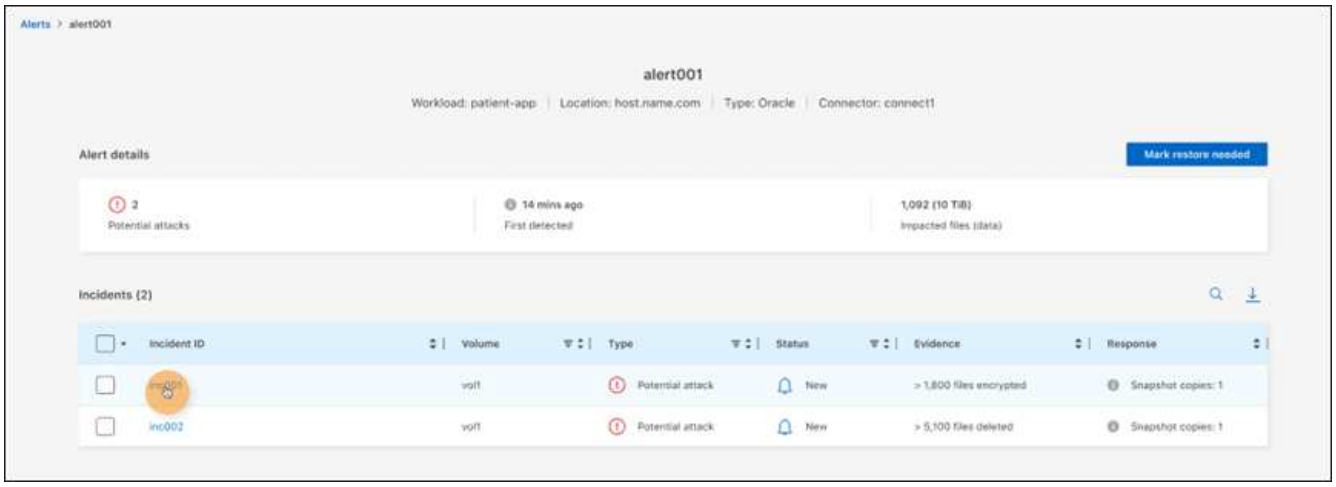
Visualizar apenas atividades maliciosas do Autonomous ransomware Protection

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

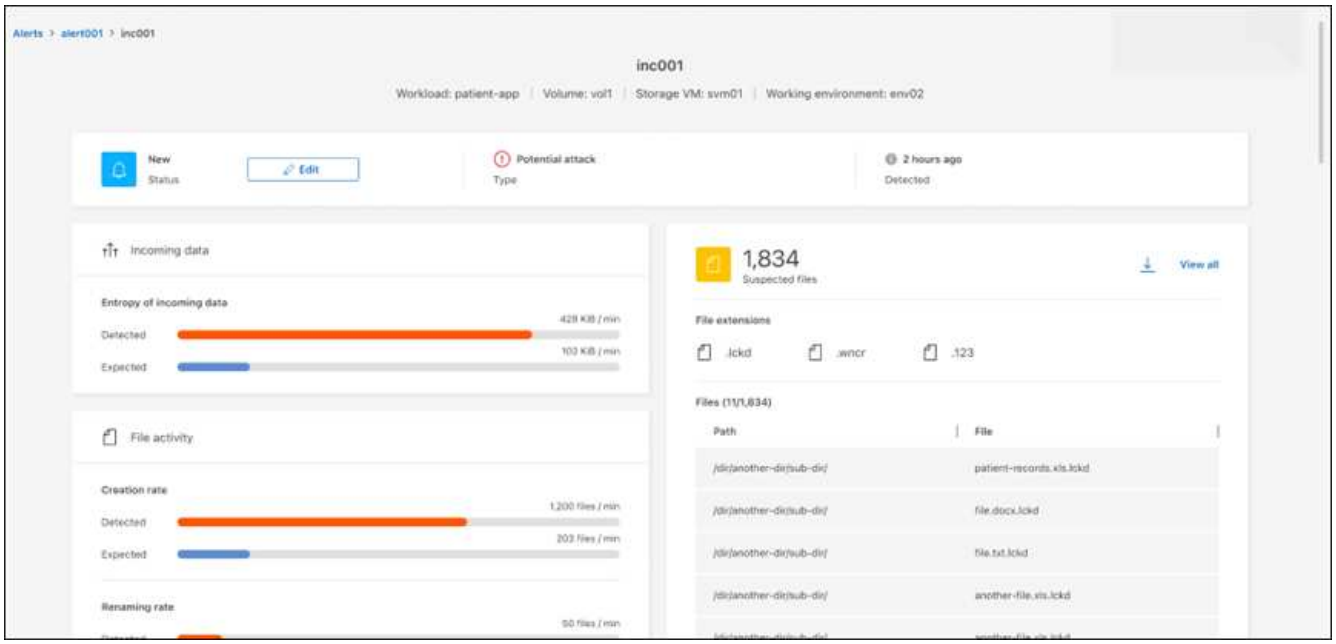
- Entropia de dados de entrada
- Taxa de criação esperada de novos arquivos em comparação com a taxa detetada
- Taxa de exclusão esperada de arquivos em comparação com a taxa detetada
- Taxa de renomeação esperada dos arquivos em comparação com a taxa detetada

Passos

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



4. Selecione 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 .

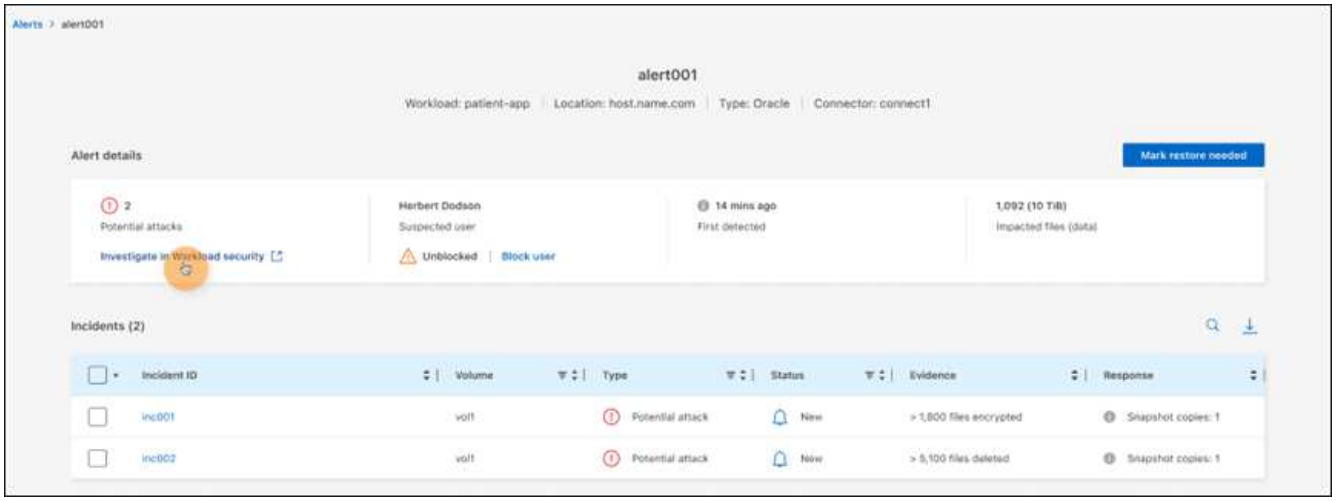
Para habilitar a segurança de workloads na proteção contra ransomware do BlueXP , faça o seguinte:

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

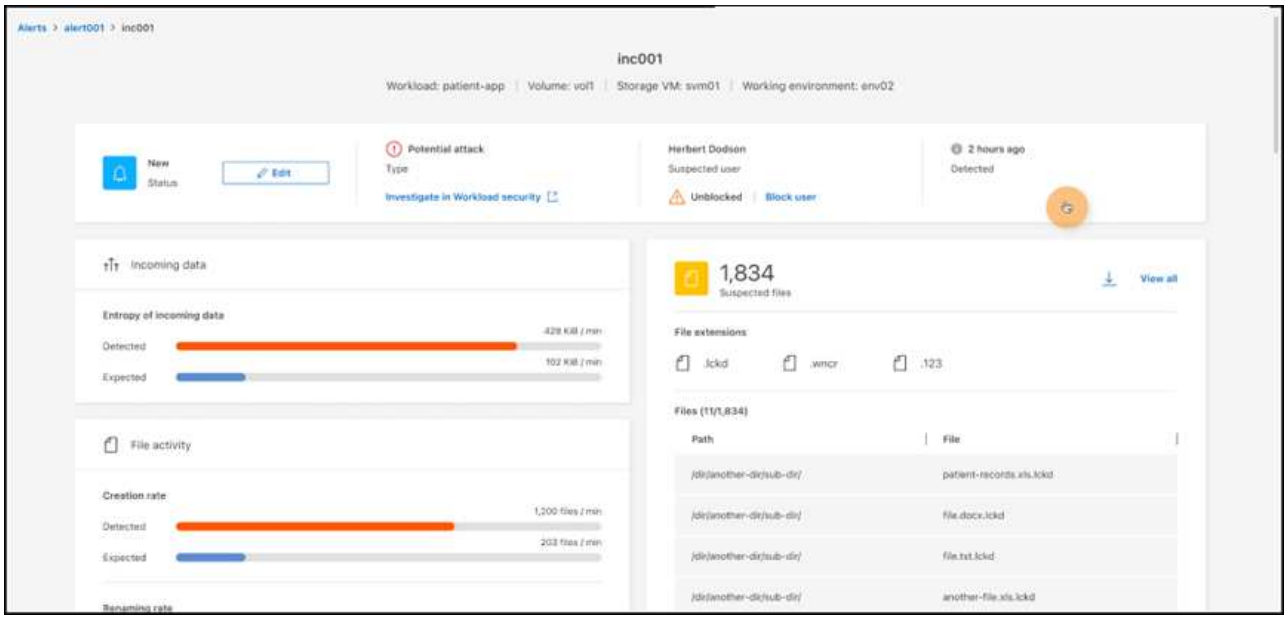
1. No menu de proteção contra ransomware BlueXP , selecione **Alertas**.
2. Selecione um alerta.
3. Reveja os incidentes no alerta.



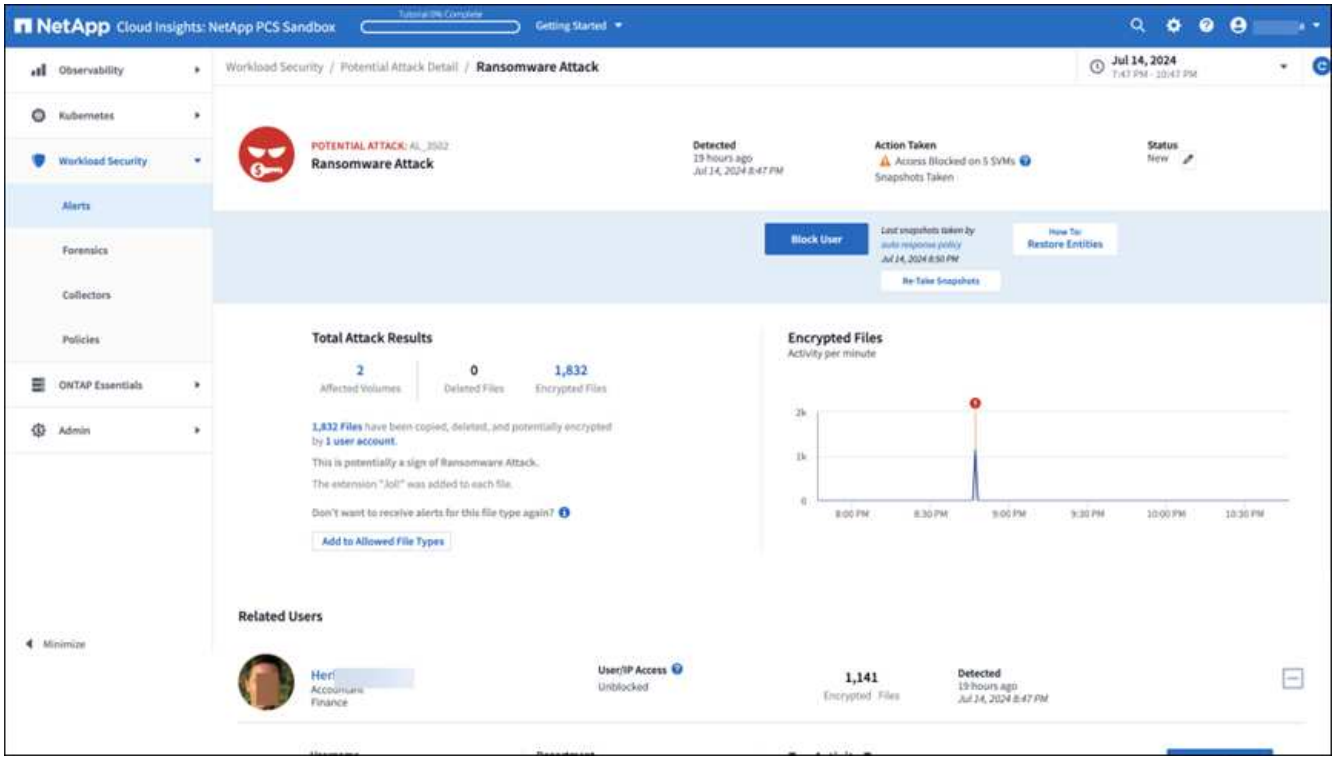
4. Para bloquear um usuário suspeito de acesso adicional em seu ambiente monitorado pelo BlueXP , selecione o link **Bloquear usuário**.
5. PESQUISE o alerta ou um incidente no alerta:

   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.

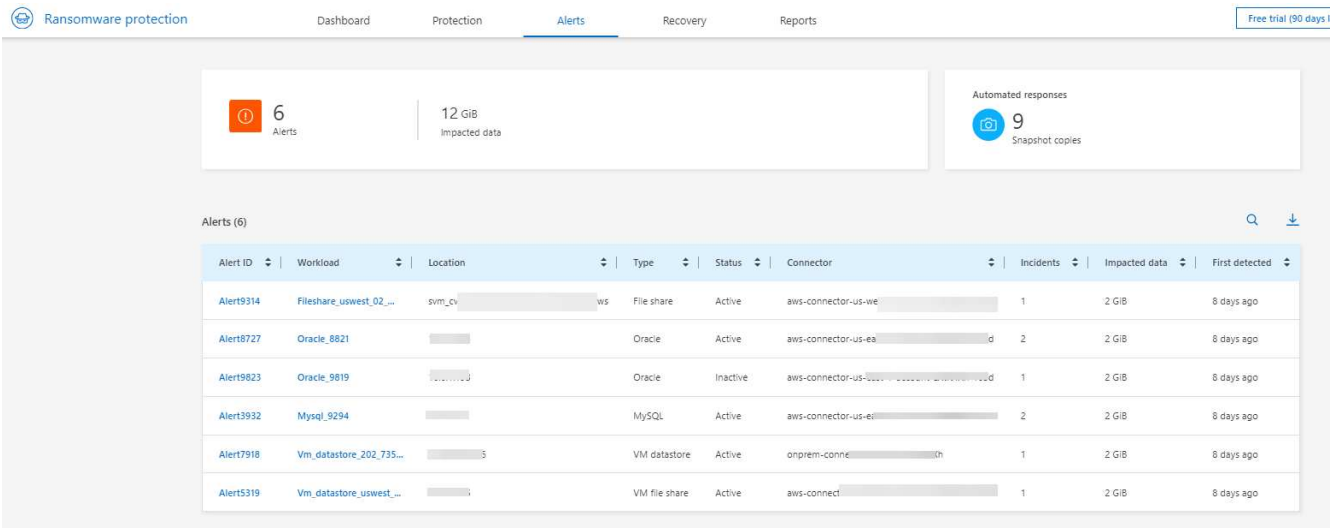


Marque os incidentes de ransomware como prontos para recuperação (após os incidentes serem neutralizados)

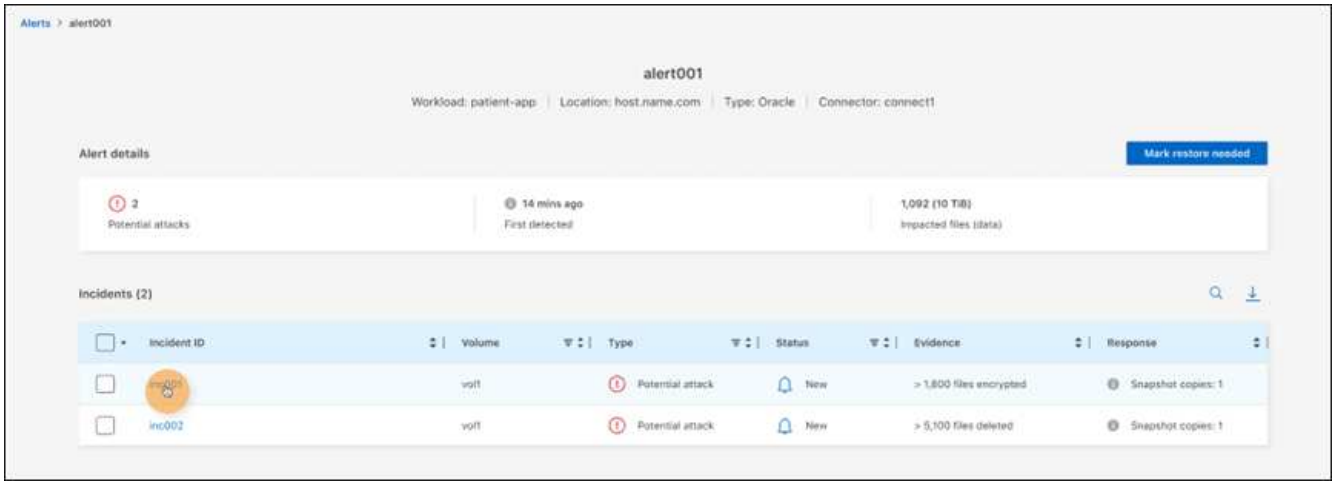
Depois de atenuar o ataque e estar pronto para recuperar cargas de trabalho, você deve se comunicar com sua equipe de administração de storage que os dados estão prontos para recuperação para que possam iniciar o processo de recuperação.

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.

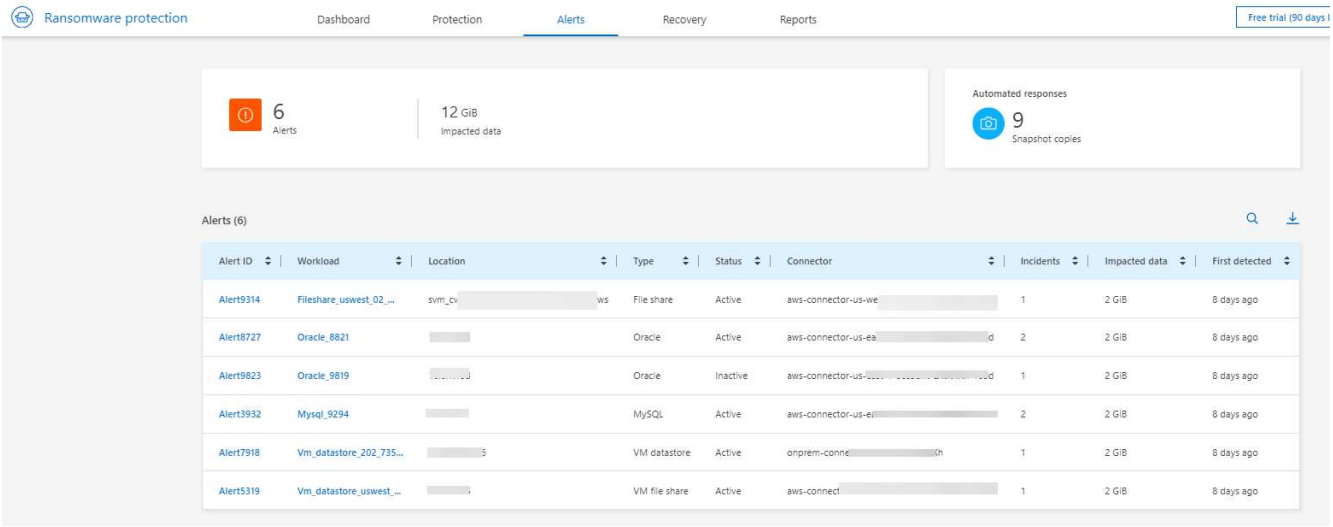
Se você ignorar um workload, todas as cópias Snapshot feitas automaticamente em resposta ao possível

ataque de ransomware serão excluídas permanentemente.

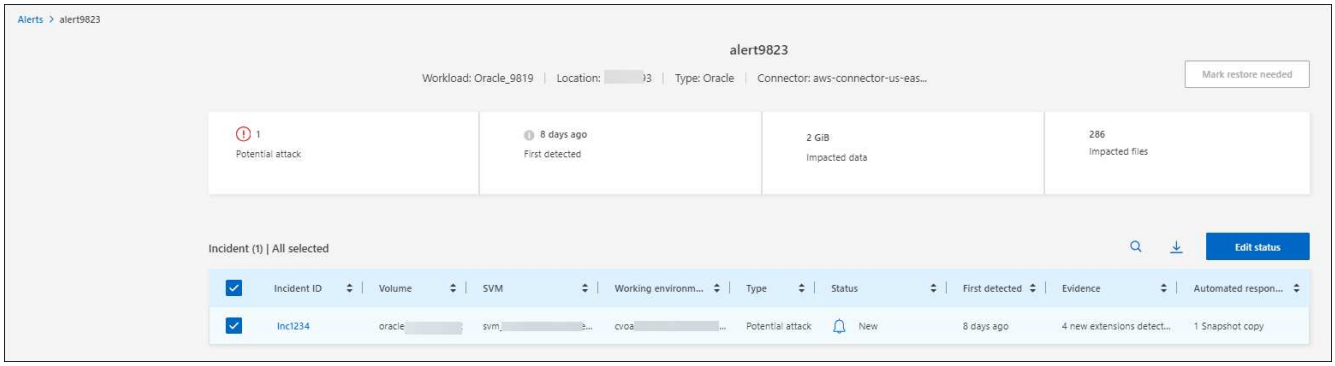
> Se você ignorar um alerta, não poderá alterar esse status de volta para qualquer outro status e não poderá desfazer essa alteração.

Passos

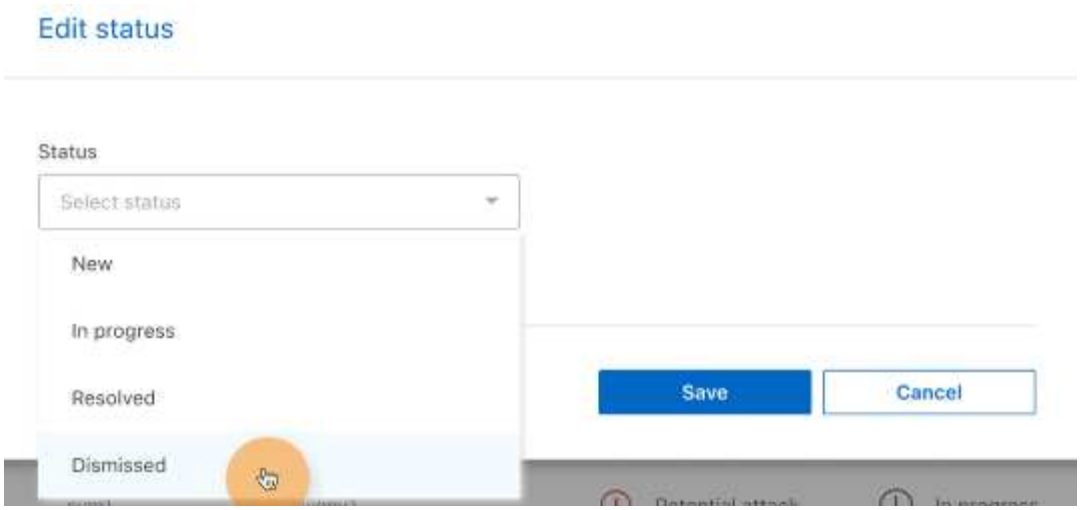
1. No menu de proteção contra ransomware BlueXP , selecione **Alertas**.



2. Na página Alertas, selecione o alerta.



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.



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

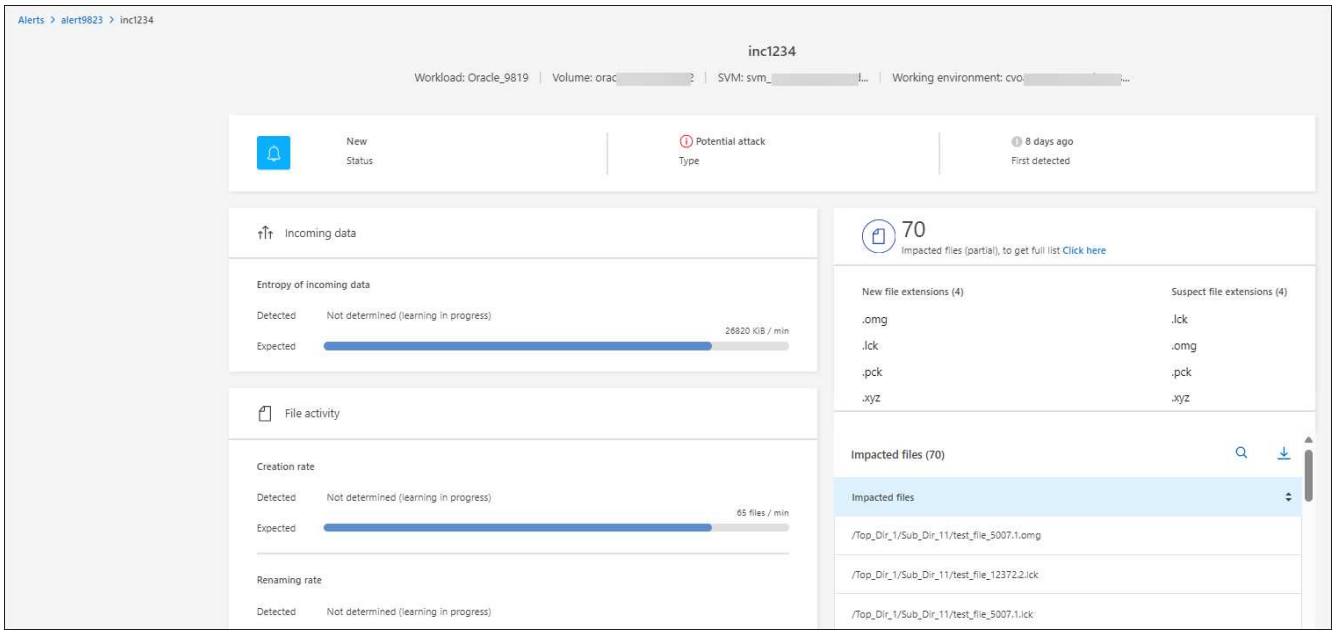
Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, pode ver uma lista de ficheiros afetados. Pode aceder à página Alertas para transferir uma lista de ficheiros afetados. Em seguida, use a página recuperação para carregar a lista e escolher quais arquivos restaurar.

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.



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.

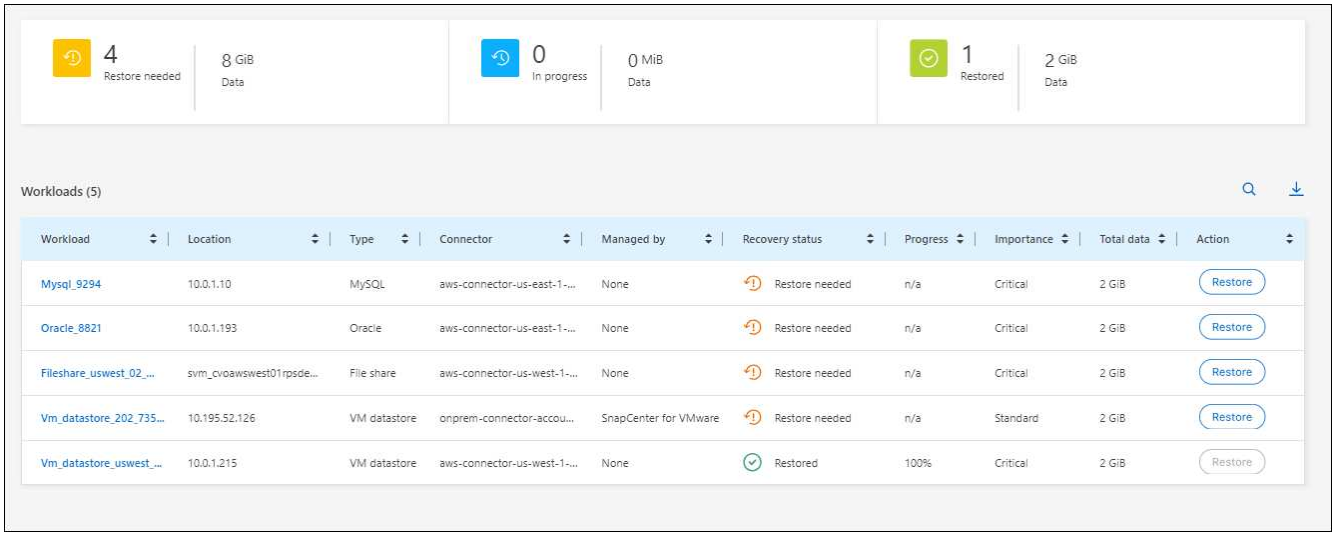
- **Falhou**: O processo de restauração da carga de trabalho não pôde ser concluído.

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**.



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

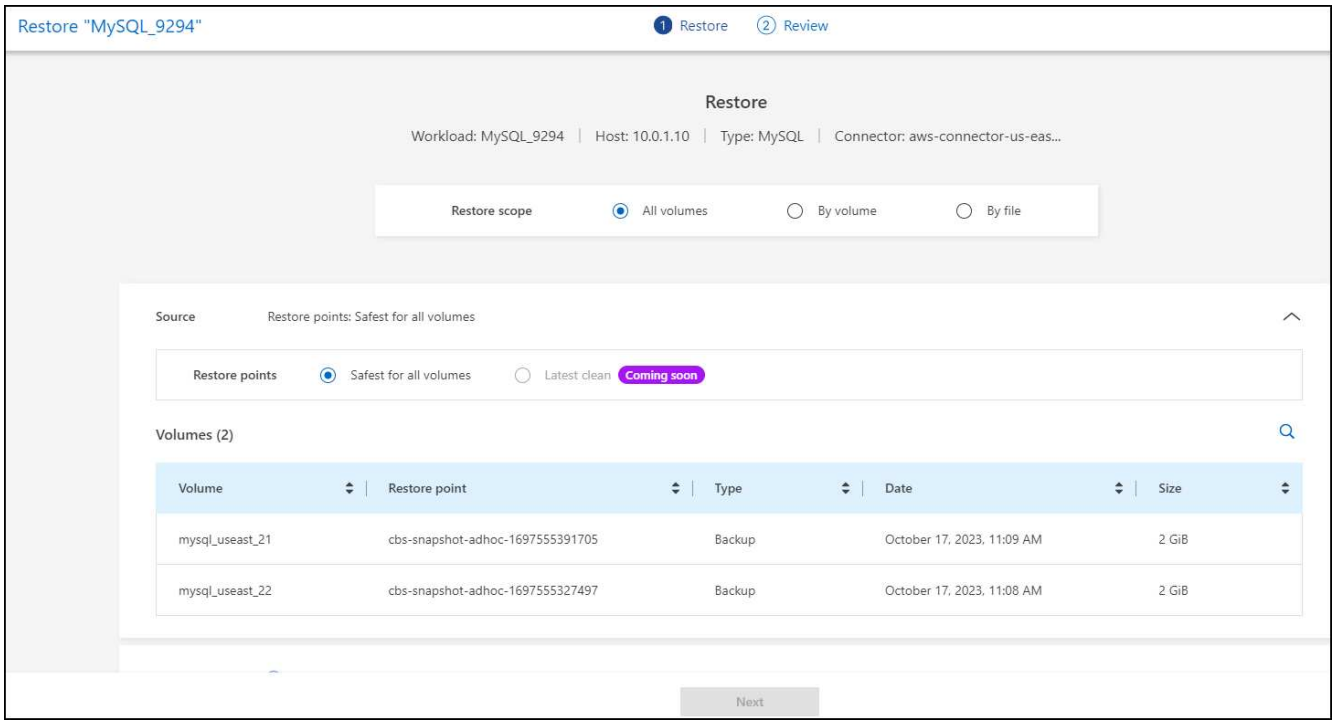
◦ Por arquivo: Você pode especificar uma pasta ou arquivos únicos para restaurar.

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.

Restaure 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.

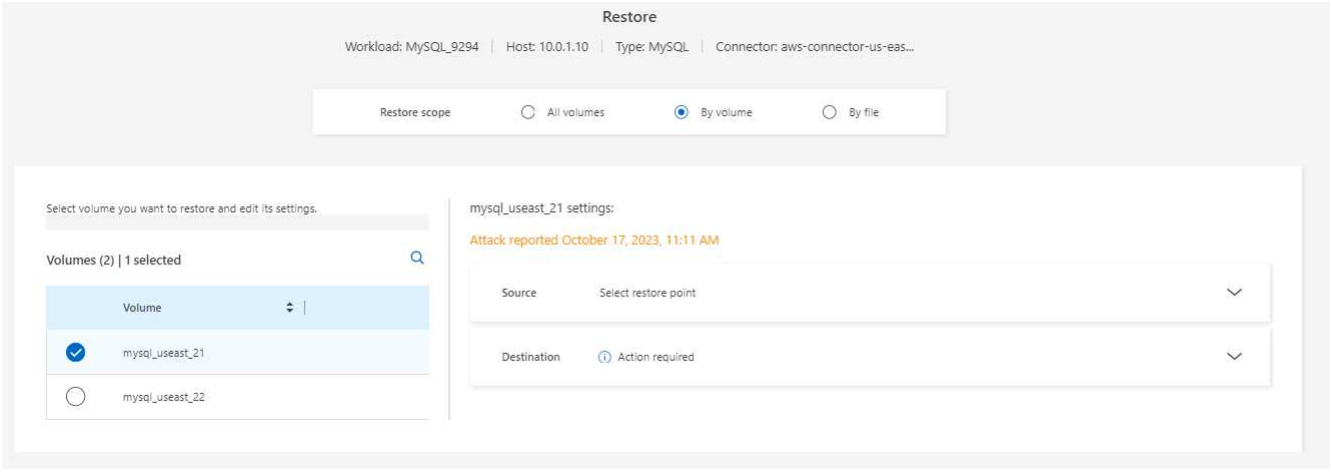
6. **Destino**: Selecione a seta para baixo ao lado de destino para ver os detalhes.
   a. Selecione o ambiente de trabalho.
   b. Selecione a VM de armazenamento.
   c. Selecione o agregado.
   d. Altere o prefixo de volume que será prepended para todos os novos volumes.

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 infetados 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 infetados 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.

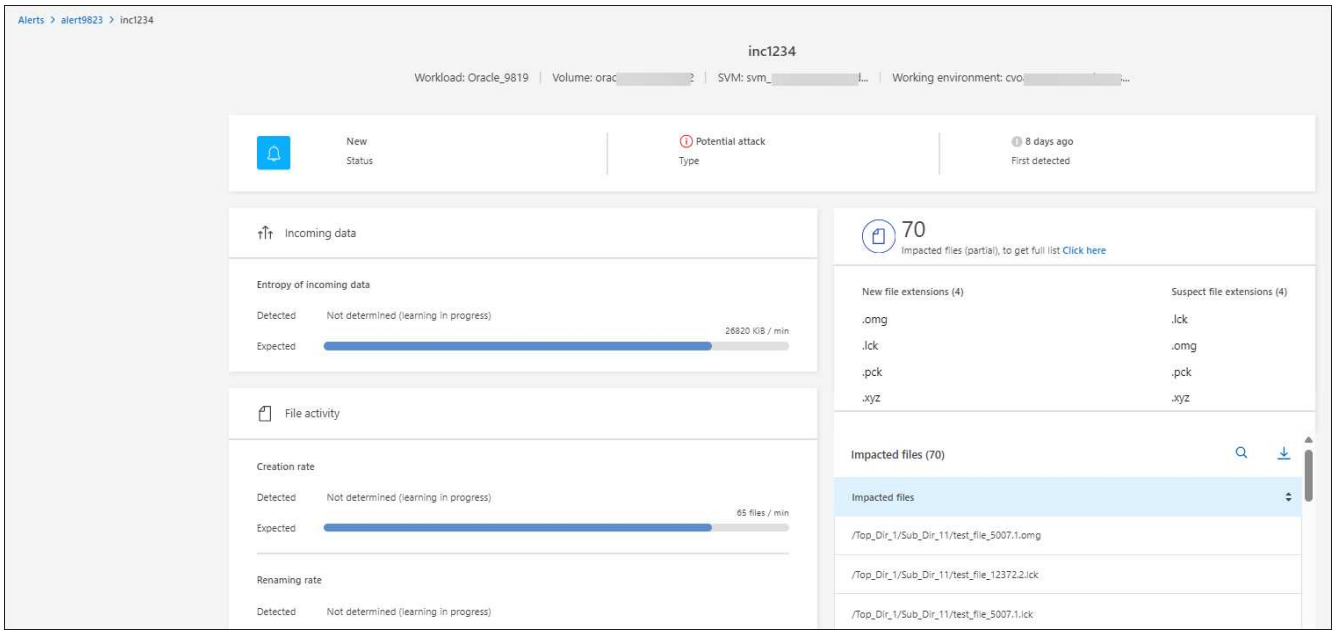
É possível restaurar um workload de aplicação no nível do arquivo para o mesmo ambiente de trabalho ou diferente.

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.



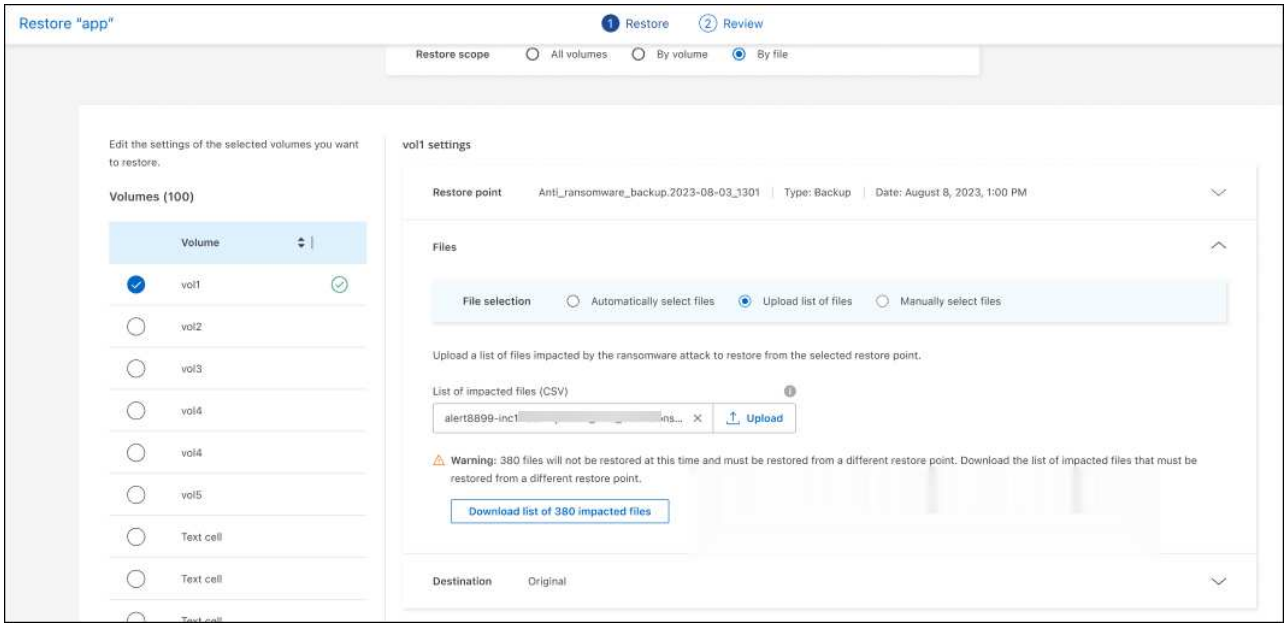
5. Para ver a lista completa de arquivos, selecione **clique aqui** na parte superior do painel arquivos afetados.
6. Para esse incidente, selecione o ícone de download e faça o download da lista de arquivos afetados no formato CSV.

Passos para restaurar esses arquivos

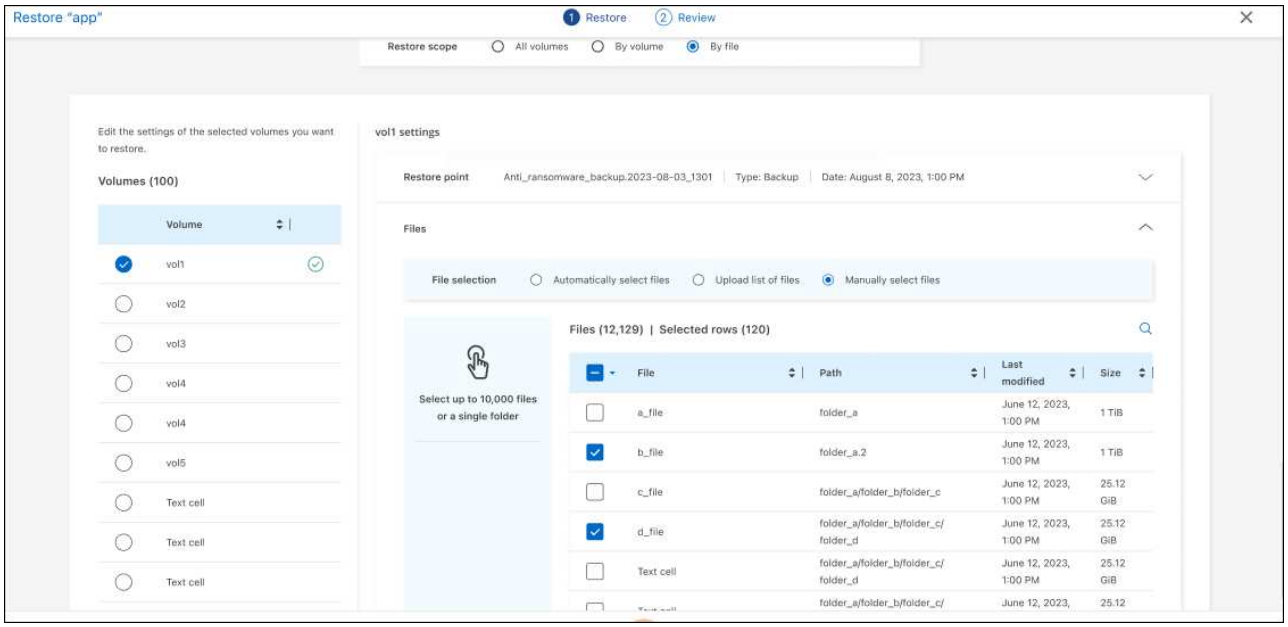
1. No menu de proteção contra ransomware BlueXP , selecione **recuperação**.
2. Selecione uma carga de trabalho de aplicativo que esteja no estado "Restaurar necessário".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no âmbito Restaurar, selecione **por ficheiro**.
5. Na lista de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



◦ * Selecione manualmente arquivos*: Selecione 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.
   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.

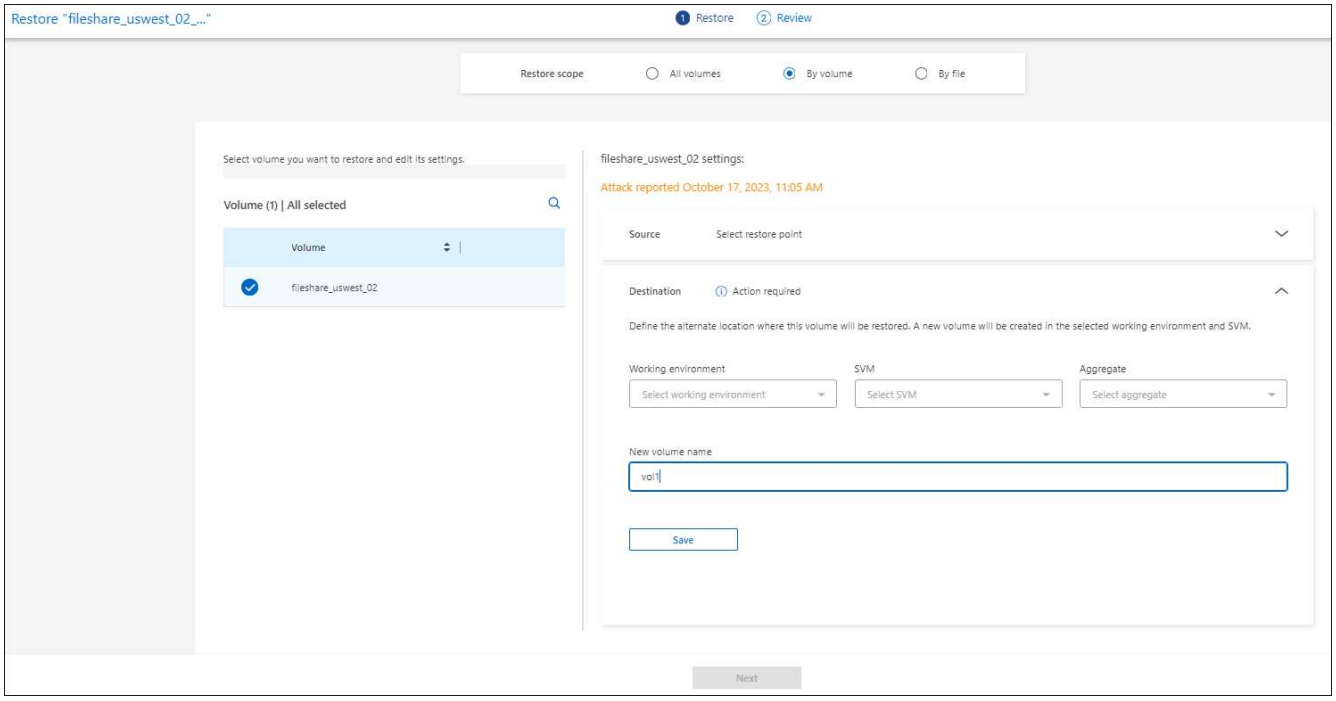
> Se você não especificar um caminho para a restauração, os arquivos serão restaurados para um novo volume no diretório de nível superior.

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**.



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.

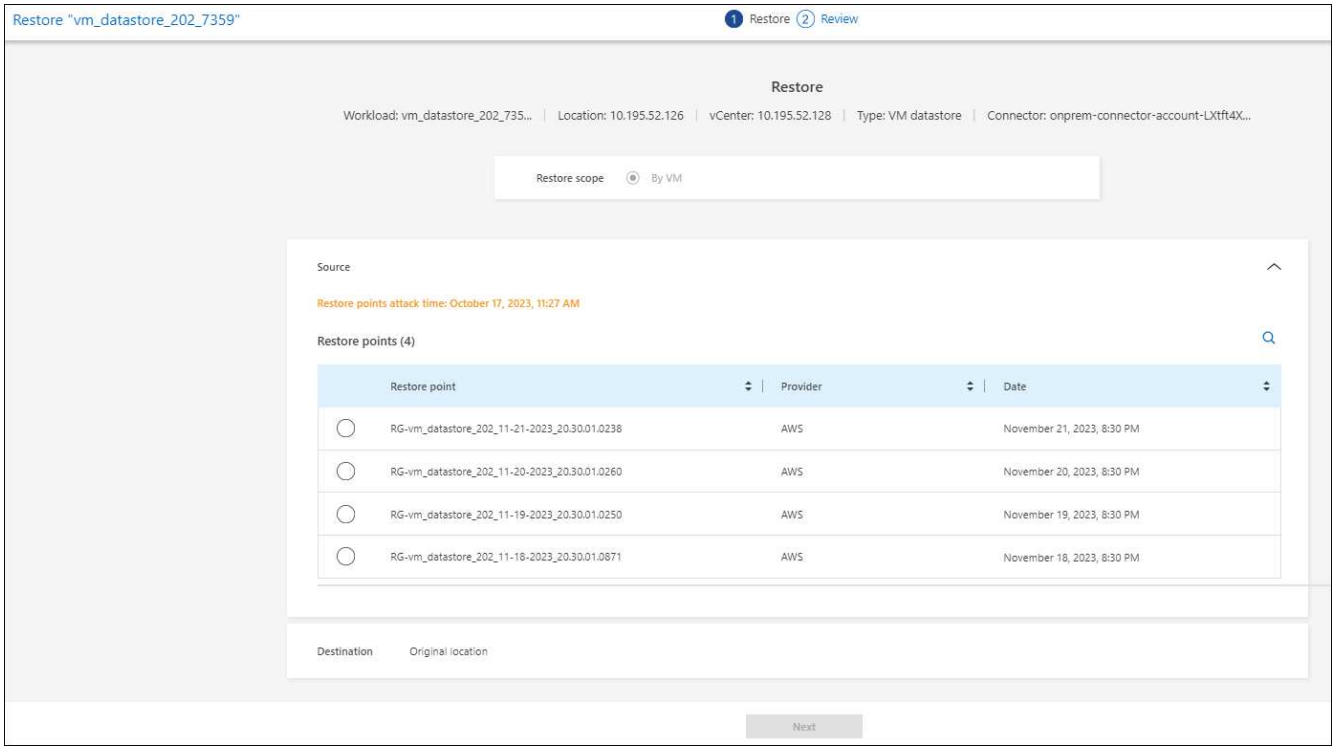
      Se você não especificar um caminho para a restauração, os arquivos serão restaurados para um novo volume no diretório de nível superior.

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:

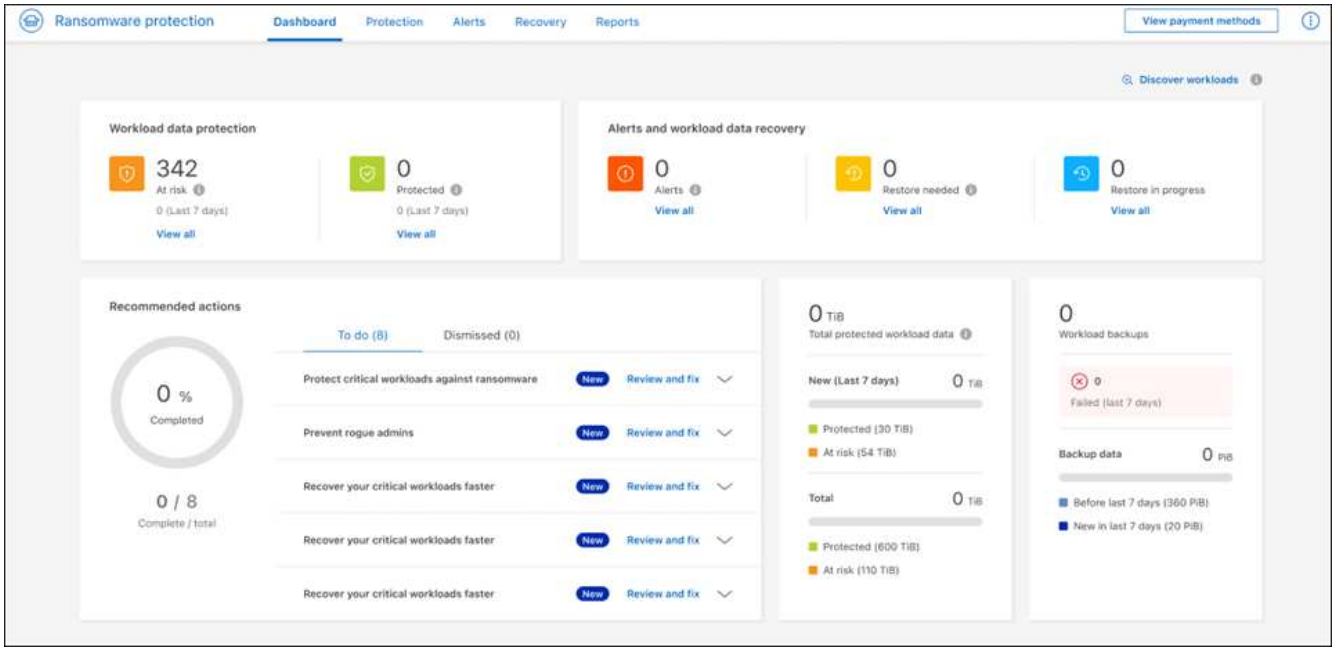
- **Proteção**: Contém o status e detalhes de todas as cargas de trabalho, incluindo o número total protegido e em risco.
- **Alertas**: Inclui o status e detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação**: Inclui o status e os detalhes de 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.

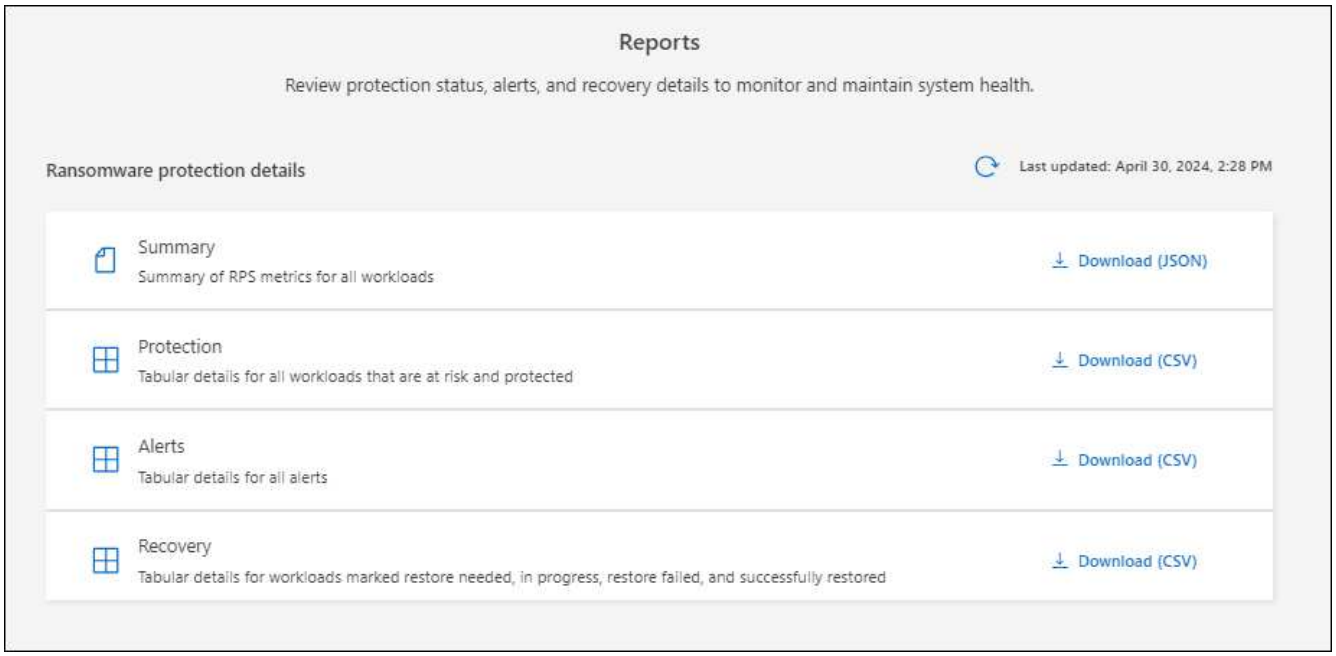
Os arquivos CSV incluem dados para todos os workloads em todos os ambientes de trabalho do BlueXP .

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)

Conhecimento e apoio

Registre-se para obter suporte

O Registro de suporte é necessário para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage. O Registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP.

O Registro para suporte não ativa o suporte do NetApp para um serviço de arquivos de provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Visão geral do Registro de suporte

Existem duas formas de Registro para ativar o direito de suporte:

- Registar o número de série da sua conta BlueXP (o número de série 960xxxxxxxx de 20 dígitos localizado na página recursos de suporte no BlueXP).

  Isso serve como seu ID de assinatura de suporte único para qualquer serviço no BlueXP . Cada assinatura de suporte no nível de conta do BlueXP deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no mercado do seu provedor de nuvem (estes são números de série de 20 dígitos 909201xxxxxxxx).

  Esses números de série são comumente referidos como *PAYGO serial numbers* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP.

Registrar ambos os tipos de números de série permite recursos como abrir tickets de suporte e geração automática de casos. O Registro é concluído adicionando contas do site de suporte da NetApp (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para obter suporte ao NetApp

Para se Registrar para obter suporte e ativar o direito de suporte, um usuário em sua organização (ou conta) do BlueXP deve associar uma conta do site de suporte da NetApp ao login do BlueXP . A forma como você se Registra no suporte da NetApp depende se você já tem uma conta do site de suporte da NetApp (NSS).

Cliente existente com uma conta NSS

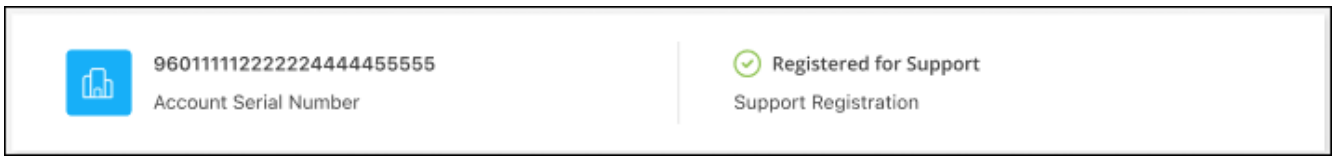
Se você é um cliente da NetApp com uma conta NSS, você simplesmente precisa se Registrar para obter suporte através do BlueXP .

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (NSS).
4. Para confirmar que o processo de Registro foi bem-sucedido, selecione o ícone Ajuda e selecione **suporte**.

   A página **recursos** deve mostrar que sua organização do BlueXP está registrada para suporte.



   Observe que outros usuários do BlueXP não verão esse mesmo status de Registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização do BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido esses passos, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é um cliente NetApp com licenças e números de série existentes, mas *no* conta NSS, você precisa criar uma conta NSS e associá-la ao seu login no BlueXP .

Passos

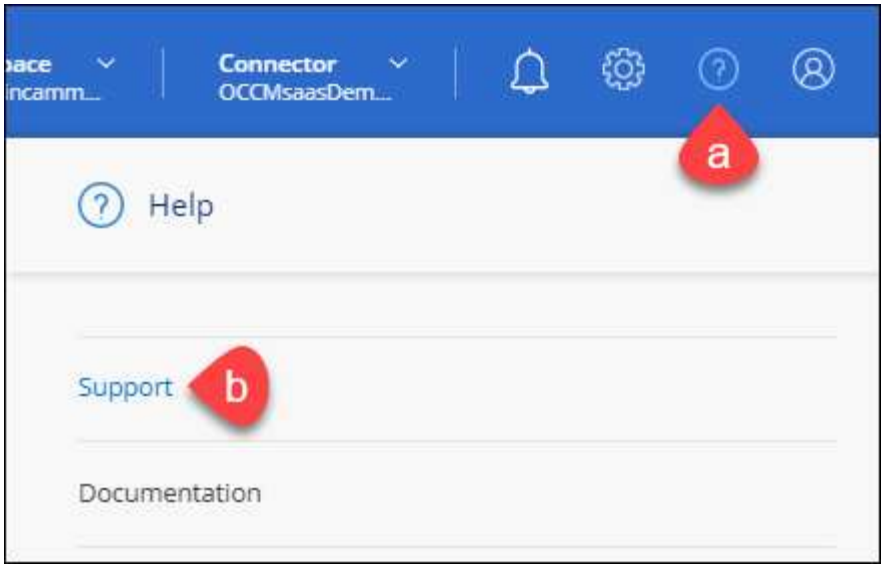
1. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento da conta.
2. Associe a sua nova conta NSS ao seu login no BlueXP executando as etapas em Cliente existente com uma conta NSS.

Novo na NetApp

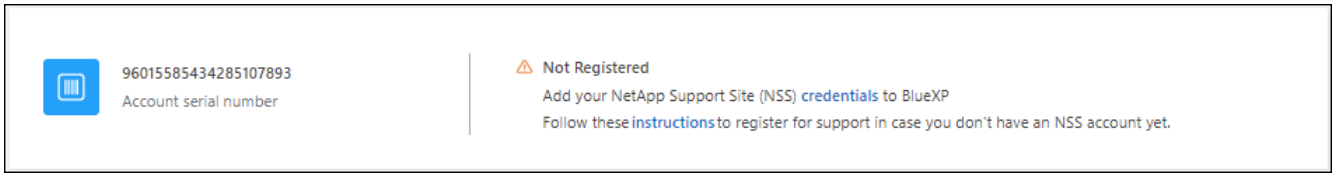
Se você é novo no NetApp e não tem uma conta NSS, siga cada passo abaixo.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Localize o número de série da ID da conta na página Registro de suporte.



3. Navegue "Site de Registro de suporte da NetApp" e selecione **não sou um Cliente NetApp registado**.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta a partir da etapa 2 acima, complete a verificação de segurança e confirme se leu a Política de Privacidade de dados globais da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam se o e-mail de validação não chegar em poucos minutos.

7. Confirme a ação a partir do e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta do site de suporte da NetApp.

8. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento.

Depois de terminar

O NetApp deve entrar em Contato com você durante esse processo. Este é um exercício de integração única para novos usuários.

Depois de ter sua conta do site de suporte da NetApp, associe a conta ao login do BlueXP , executando as

etapas em Cliente existente com uma conta NSS.

Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

A associação das credenciais do site de suporte da NetApp à sua organização do BlueXP é necessária para ativar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

  Fornecer sua conta NSS é necessário para ativar o suporte para o seu sistema e para obter acesso aos recursos de suporte técnico da NetApp.

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer a sua conta NSS para que o BlueXP possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizar o software Cloud Volumes ONTAP para a versão mais recente

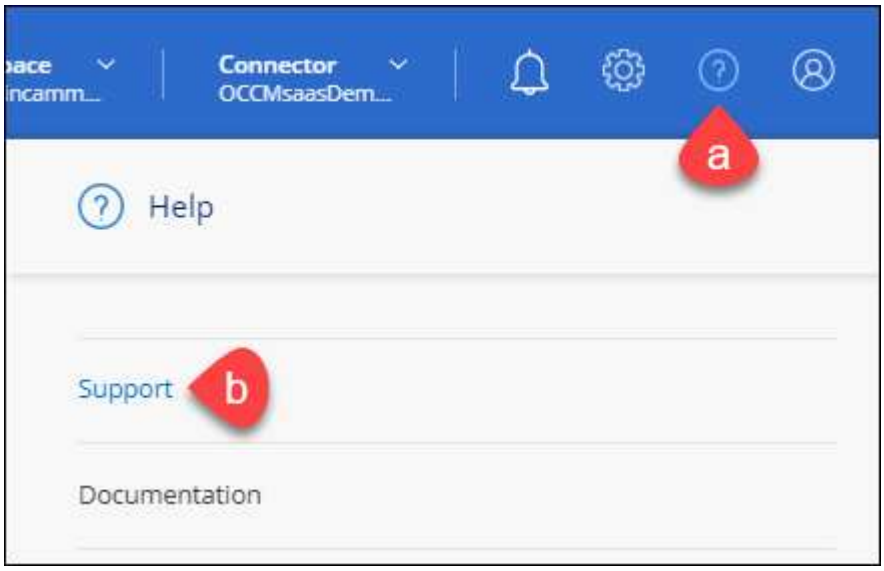
Associar credenciais NSS à sua organização do BlueXP é diferente da conta NSS associada a um login de usuário do BlueXP .

Essas credenciais do NSS estão associadas ao ID específico da organização do BlueXP . Os utilizadores que pertencem à organização BlueXP podem aceder a estas credenciais a partir de **suporte > Gestão NSS**.

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação

específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

   Essas ações permitem que o BlueXP use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

   Observe o seguinte:

   - A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

   O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, há também uma opção **Atualizar credenciais** ••• no menu.

     Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

Obtenha ajuda

A NetApp oferece suporte ao BlueXP e seus serviços de nuvem de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. O seu registo de suporte inclui suporte técnico remoto através de Bilheteira na Web.

Obtenha suporte para um serviço de arquivos do provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage, use as opções de suporte descritas abaixo.

Use opções de suporte autônomo

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do BlueXP que você está visualizando no momento.

- "Base de conhecimento"

  PESQUISE na base de conhecimento do BlueXP para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Junte-se à comunidade BlueXP para seguir as discussões em curso ou criar novas.

Crie um caso com o suporte do NetApp

Além das opções de suporte autônomo acima, você pode trabalhar com um especialista de suporte da NetApp para resolver quaisquer problemas depois de ativar o suporte.

Antes de começar

- Para usar o recurso **criar um caso**, primeiro você deve associar suas credenciais do site de suporte da NetApp ao login do BlueXP . "Saiba como gerenciar credenciais associadas ao seu login no BlueXP".
- Se você estiver abrindo um caso para um sistema ONTAP com um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Na página **recursos**, escolha uma das opções disponíveis em suporte técnico:

   a. Selecione **Ligue para nós** se quiser falar com alguém no telefone. Você será direcionado para uma página no NetApp.com que lista os números de telefone que você pode ligar.

   b. Selecione **criar um caso** para abrir um ticket com um especialista em suporte da NetApp:

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, BlueXP quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do serviço.
      - **Ambiente de trabalho**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **no local** e, em seguida, o ambiente de trabalho associado.

        A lista de ambientes de trabalho está dentro do escopo da organização (ou conta) do BlueXP , do projeto (ou da área de trabalho) e do conetor que você selecionou no banner superior do serviço.

      - **Prioridade do caso**: Escolha a prioridade para o caso, que pode ser baixa, média, alta ou Crítica.

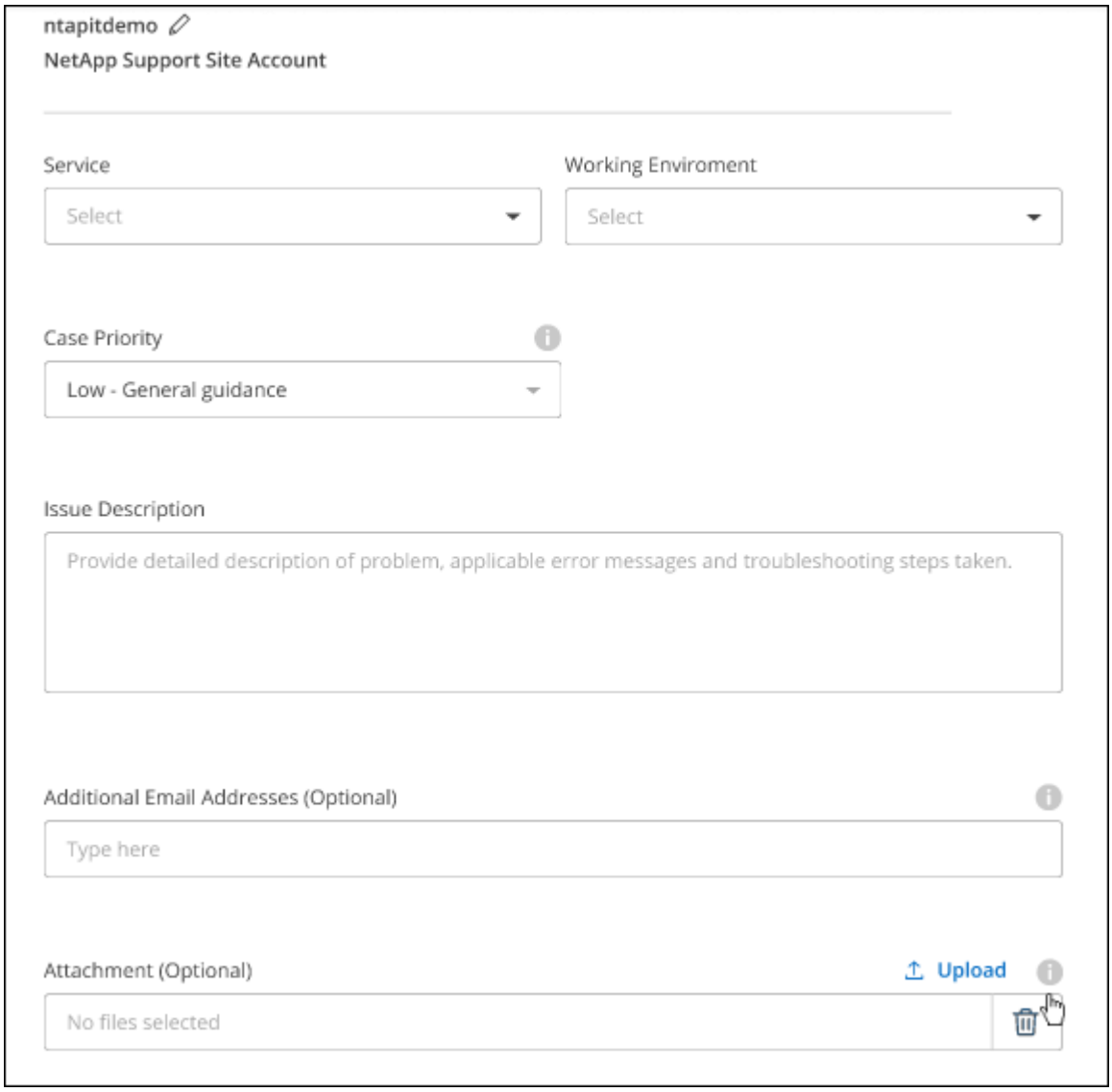
        Para saber mais detalhes sobre essas prioridades, passe o Mouse sobre o ícone de informações ao lado do nome do campo.

      - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
      - **Endereços de e-mail adicionais**: Insira endereços de e-mail adicionais se você quiser que outra

pessoa saiba sobre esse problema.

- **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

  Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois de terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp irá rever o seu caso e voltar para você em breve.

Para obter um histórico de seus casos de suporte, você pode selecionar **Configurações > linha do tempo** e procurar ações chamadas "criar caso de suporte". Um botão à direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa de Registro com a qual está associada não são a mesma empresa de Registro para o número de série da conta BlueXP (ou seja. 960xxxx) ou o número de

série do ambiente de trabalho. Pode procurar assistência utilizando uma das seguintes opções:

- Use o chat no produto
- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerenciar seus casos de suporte (prévia)

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do BlueXP . Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

O gerenciamento de casos está disponível como uma prévia. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A vista à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta do usuário NSS que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses ao nível da sua empresa com base na sua conta NSS de utilizador.

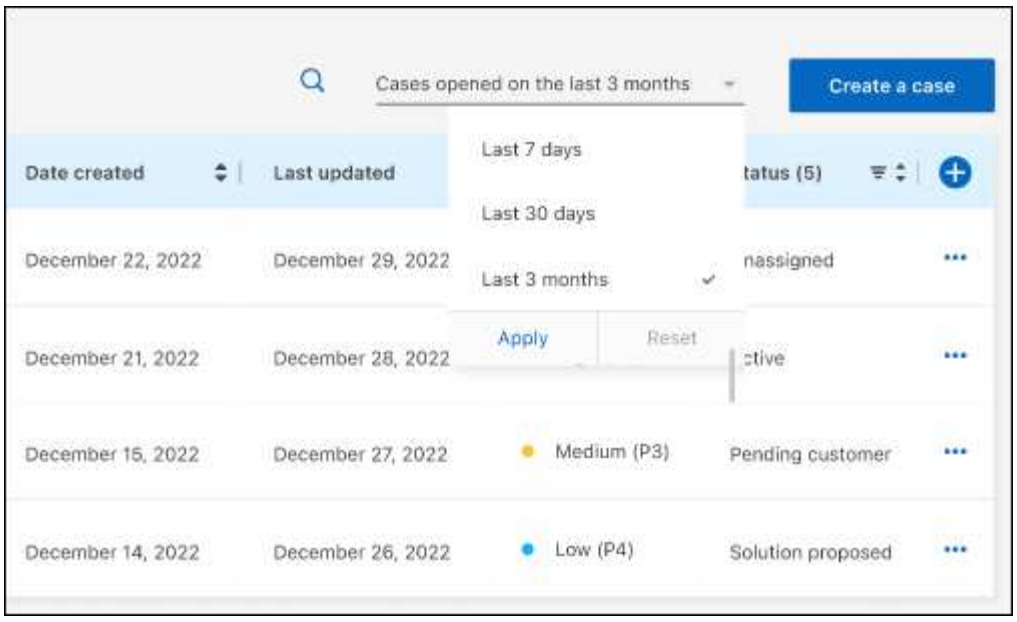
  Os resultados na tabela refletem os casos relacionados à exibição selecionada.
- Você pode adicionar ou remover colunas de interesse e pode filtrar o conteúdo de colunas como prioridade e Status. Outras colunas fornecem apenas capacidades de ordenação.

  Veja os passos abaixo para obter mais detalhes.
- Em um nível por caso, oferecemos a capacidade de atualizar notas de caso ou fechar um caso que ainda não esteja no status fechado ou pendente fechado.

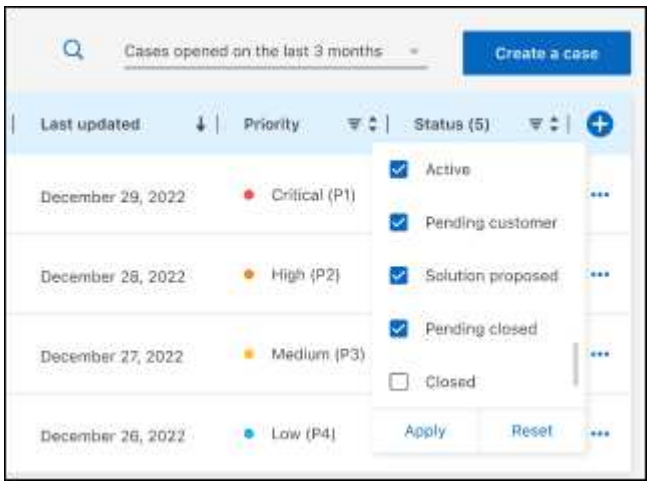
Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Selecione **Gerenciamento de casos** e, se for solicitado, adicione sua conta NSS ao BlueXP .

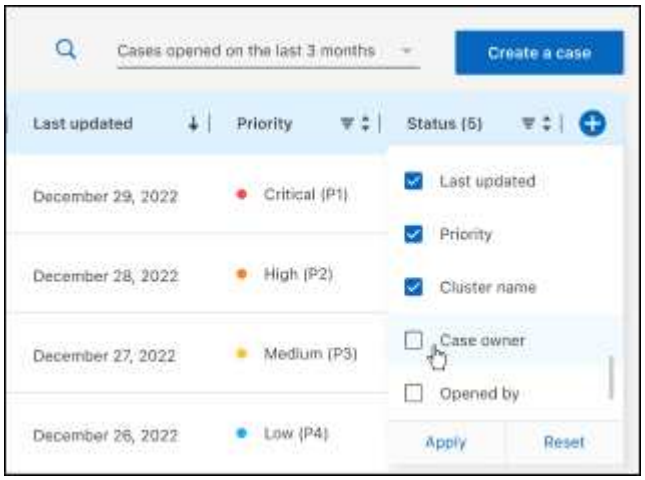
   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à conta de usuário do BlueXP . Esta é a mesma conta NSS que aparece na parte superior da página **NSS Management**.
3. Opcionalmente, modifique as informações exibidas na tabela:
   - Em **casos da organização**, selecione **Exibir** para ver todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um intervalo de tempo diferente.



- Filtre o conteúdo das colunas.



- Altere as colunas que aparecem na tabela selecionando e escolhendo as colunas que você deseja exibir.

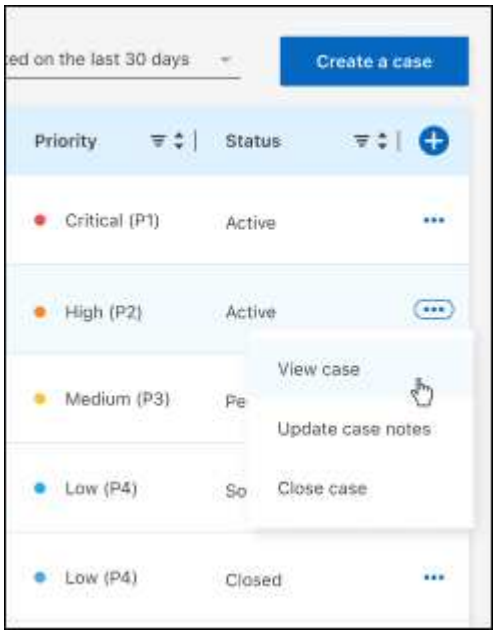


4. Gerencie um caso existente •••selecionando e selecionando uma das opções disponíveis:

   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - * Atualizar notas de caso*: Forneça detalhes adicionais sobre o seu problema ou selecione **carregar arquivos** para anexar até um máximo de cinco arquivos.

     Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - * Fechar caso*: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.



Referência

Privileges de controle de acesso baseado em funções de proteção contra ransomware da BlueXP

A proteção contra ransomware do BlueXP usa o controle de acesso baseado em funções (RBAC) para controlar o acesso que cada usuário tem a recursos e ações específicos. O serviço usa as principais funções do BlueXP de Administrador e Visualizador da Organização (não Administrador da Organização).

A tabela a seguir indica quais ações cada função pode executar.

Recurso e ação	Administrador da Organização BlueXP	Não Admin (Visualizador)
Inicie o teste gratuito	Y	N
Visualização do painel	Y	Y
Ver separador proteção	Y	Y
Guia Exibir Alertas	Y	Y
Ver separador recuperar	Y	Y
Exibir relatórios guia	Y	Y
Ver separador Definições	Y	Y
Inicie a descoberta de cargas de trabalho	Y	N
Proteger: Modificar ou excluir políticas	Y	N
Proteger: Adicione políticas	Y	N
Proteção: Proteja workloads	Y	N
Proteger: Identificar dados confidenciais	Y	N
Proteger: Editar proteção da carga de trabalho	Y	N
Proteção: Veja os detalhes da carga de trabalho	Y	Y
Proteger: Transferir dados	Y	Y

Recurso e ação	Administrador da Organização BlueXP	Não Admin (Visualizador)
Alertas: Veja os detalhes do alerta	Y	Y
Alertas: Editar o status do incidente	Y	N
Alertas: Veja os detalhes do incidente	Y	Y
Alertas: Obtenha a lista completa dos arquivos afetados	Y	N
Alertas: Baixe dados de alertas	Y	Y
Recuperar: Baixe arquivos afetados	Y	N
Recuperar: Restaure a carga de trabalho	Y	N
Recuperar: Baixar dados de recuperação	Y	Y
Recuperar: Baixar relatórios	Y	Y
Configurações: Adicionar ou modificar destinos de backup	Y	N
Configurações: Adicione ou modifique destinos SIEM	Y	N
Relatórios: Baixe relatórios	Y	Y
Documentação: Veja a documentação sobre o produto	Y	Y
Documentação: Veja a documentação sobre o que há de novo no produto	Y	Y

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- "Aviso para BlueXP"

Informações sobre direitos autorais

Informações sobre marcas comerciais