



Comece agora

BlueXP ransomware protection

NetApp
December 20, 2024

Índice

Comece agora	1
Saiba mais sobre a proteção contra ransomware BlueXP	1
Pré-requisitos de proteção contra ransomware da BlueXP	7
Início rápido para proteção contra ransomware BlueXP	9
Configurar a proteção contra ransomware do BlueXP	10
Acesse a proteção contra ransomware do BlueXP	11
Configure o licenciamento para a proteção contra ransomware BlueXP	13
Descubra workloads na proteção de ransomware BlueXP	24
Configurar as configurações de proteção contra ransomware do BlueXP	29
Perguntas frequentes sobre proteção contra ransomware do BlueXP	43

Comece agora

Saiba mais sobre a proteção contra ransomware BlueXP

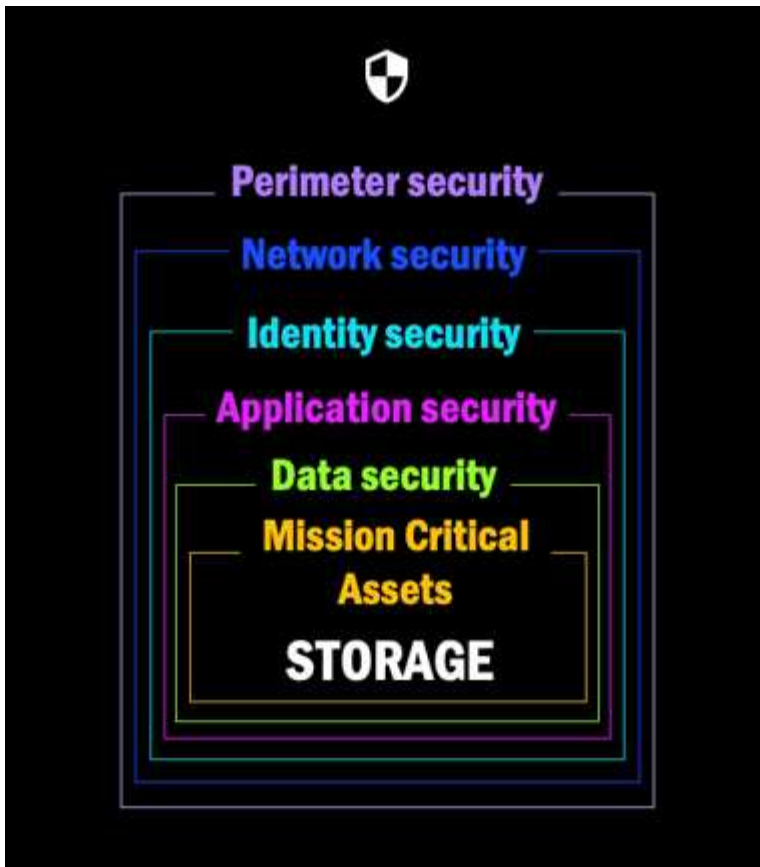
Os ataques de ransomware podem bloquear o acesso aos seus dados e os invasores podem pedir resgate em troca da liberação de dados ou descriptografia. De acordo com a IDC, não é incomum que as vítimas de ransomware sofram vários ataques de ransomware. O ataque pode interromper o acesso aos dados entre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

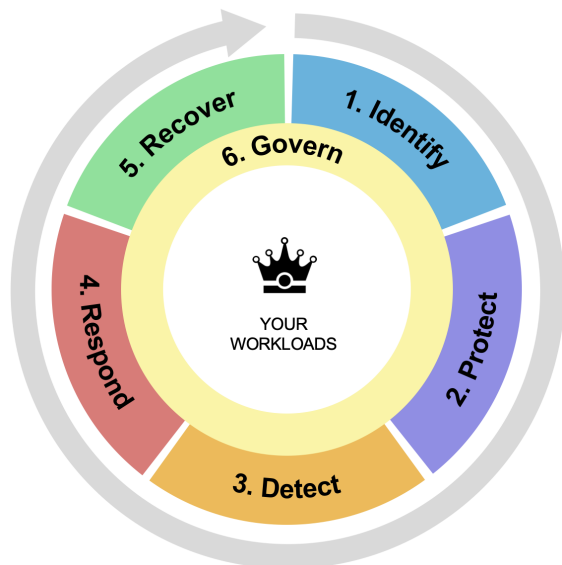
- *** Camada externa***: Esta é a sua primeira linha de defesa usando firewalls, sistemas de detecção de intrusão e redes privadas virtuais para proteger os limites da rede.
- **Segurança de rede**: Esta camada baseia-se na base com segmentação de rede, monitoramento de tráfego e criptografia.
- **Segurança 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 detecção 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.



1. Automatically **discovers** and prioritizes data in NetApp storage **with a focus on top application-based workloads**

2. **One-click protection** of top workload data (backup, immutable/indelible snapshots, secure configuration, different security domain)

3. **Accurately detects** ransomware as **quickly** as possible using **next-generation AI-based anomaly detection**

4. Automated response to secure safe recovery point, attack alerting, and integration with top **SIEM and XDR solutions**

5. Rapidly restores data via simplified **orchestrated recovery** to accelerate application uptime

6. Implement your ransomware protection **strategy and policies**, and **monitor outcomes**

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 detecção (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 detecta 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.

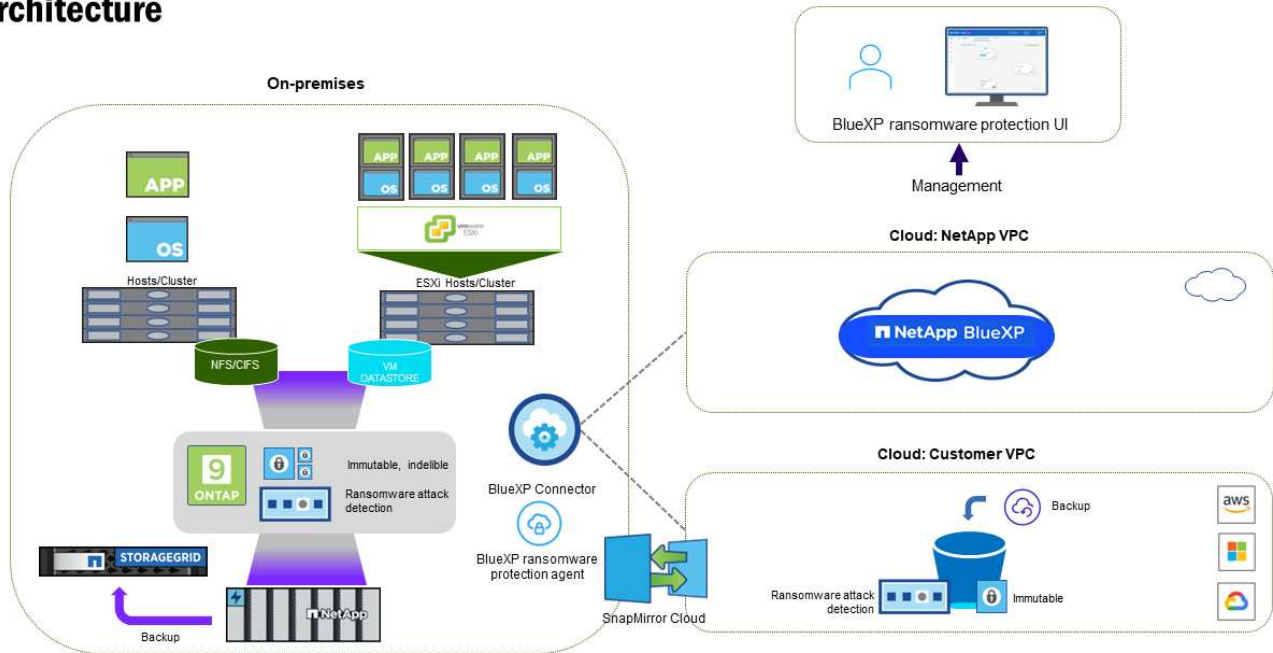
Para obter detalhes, "[Configure o licenciamento](#)" consulte .

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	<ul style="list-style-type: none"> 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*	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • Detecta possíveis ataques com um modelo integrado de aprendizado de máquina (ML) que detecta atividade e criptografia potencialmente anômalas. • Fornece detecção de camada dupla que começa com a detecção 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 conector 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 conector 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 conectores BlueXP em uma única organização do BlueXP , o serviço de proteção contra ransomware da BlueXP verificará os recursos do ONTAP em todos os conectores 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.

1

Reveja os pré-requisitos

["Certifique-se de que seu ambiente atenda a esses requisitos"](#).

2

Configure o serviço de proteção contra ransomware

- ["Prepare o NetApp StorageGRID, Amazon Web Services ou Microsoft Azure como destino de backup"](#).
- ["Configure um conector no BlueXP"](#).
- ["Configurar destinos de cópia de segurança"](#).
- ["Opcionalmente, ative a detecção de ameaças"](#).
- ["Descubra workloads em BlueXP"](#).

3

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 conector 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 conector no BlueXP antes de usar o serviço, consulte a documentação do BlueXP que descreve "[Como criar um conector BlueXP](#)"o .



Se você tiver vários conectores BlueXP , o serviço verificará os dados em todos os conectores além daquele que aparece atualmente na IU do BlueXP . Este serviço descobre todos os projetos e todos os conectores 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, "[Privilegios 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](#)".

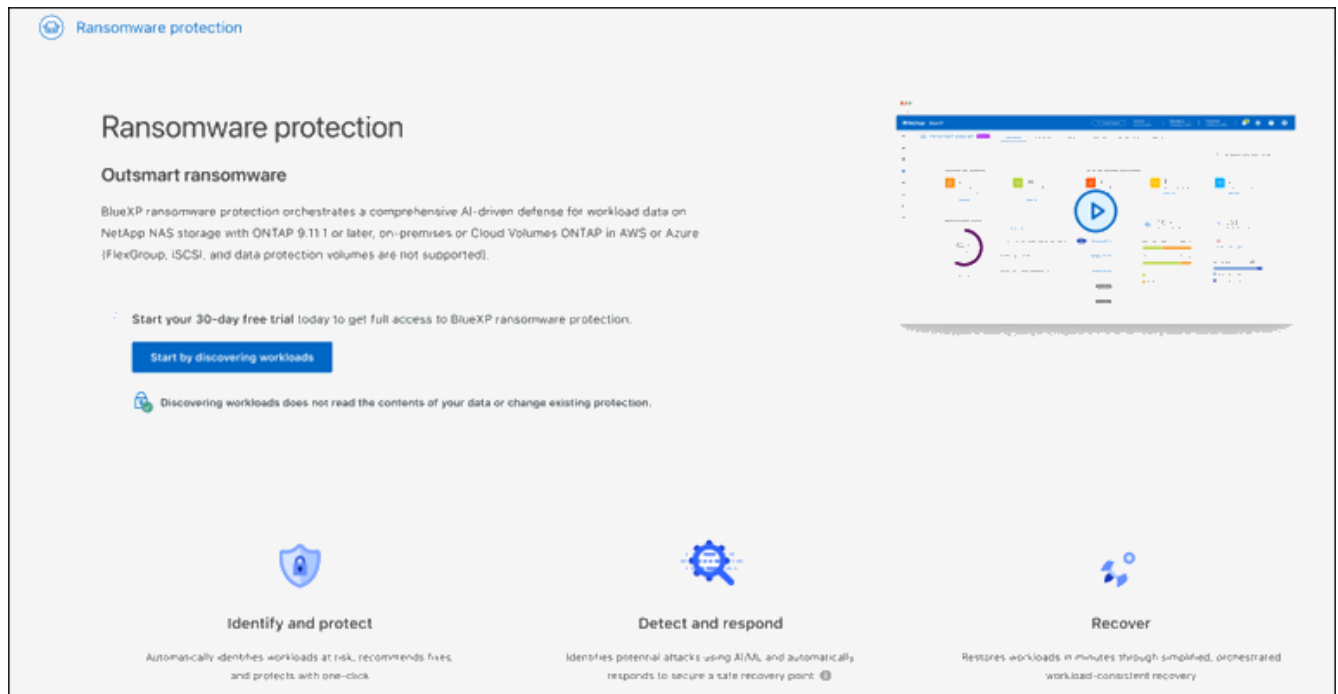
Passos

1. Abra um navegador da Web e vá para o "[Consola BlueXP](#)".

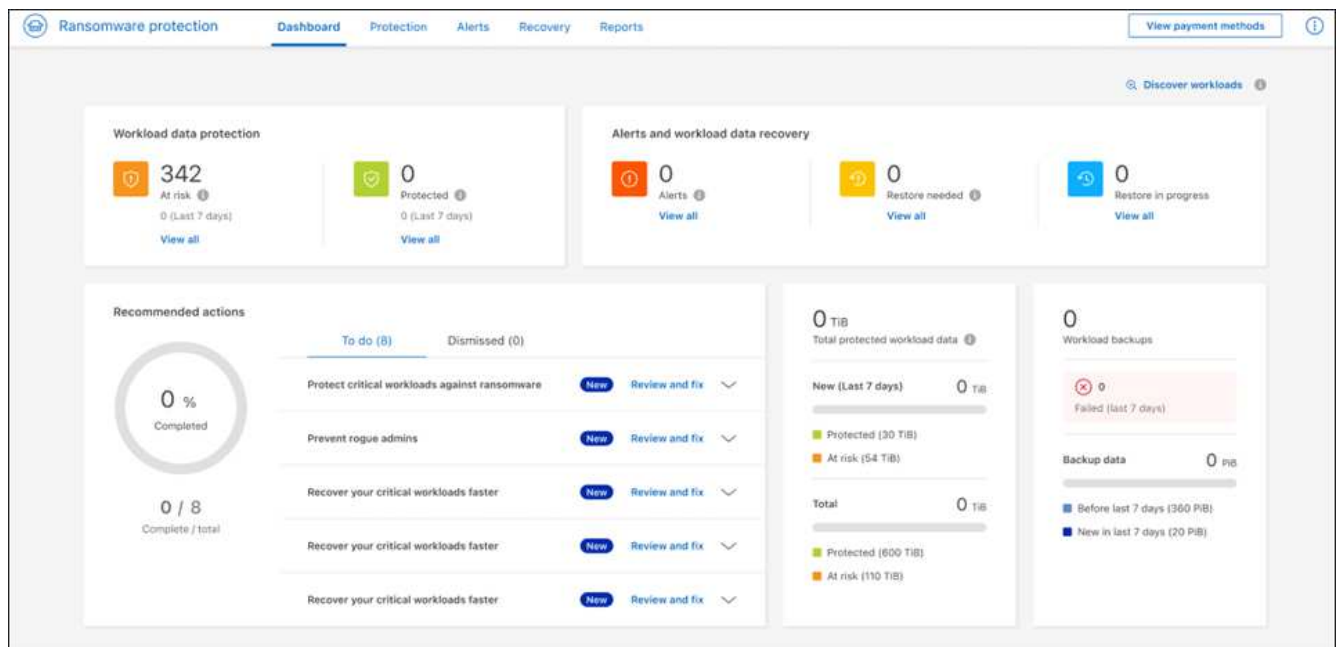
É apresentada a página de início de sessão do NetApp BlueXP .

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 conector 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 Infrastructure Insights Workload Security, consulte "[Sobre o Workload Security](#)"



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

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.

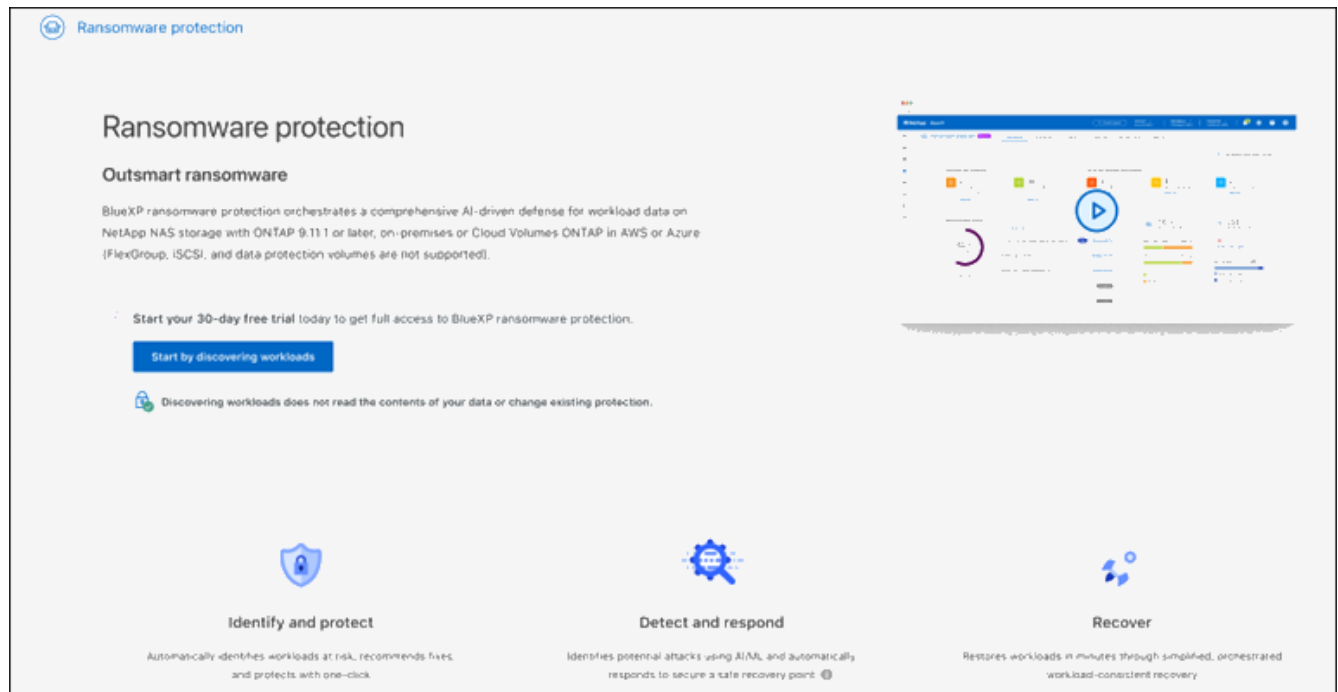
Você pode obter uma licença ou assinar a qualquer momento e você não será cobrado até que o teste de 30 dias termine. Para continuar após o teste de 30 dias, você precisará comprar uma licença BYOL ou uma assinatura PAYGO.

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 conector para outros serviços, adicione um.

Para adicionar um conector, "[Saiba mais sobre conectores](#)" consulte a .

5. Depois de configurar um conector, na página inicial da proteção contra ransomware do BlueXP , o botão para adicionar um conector 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.

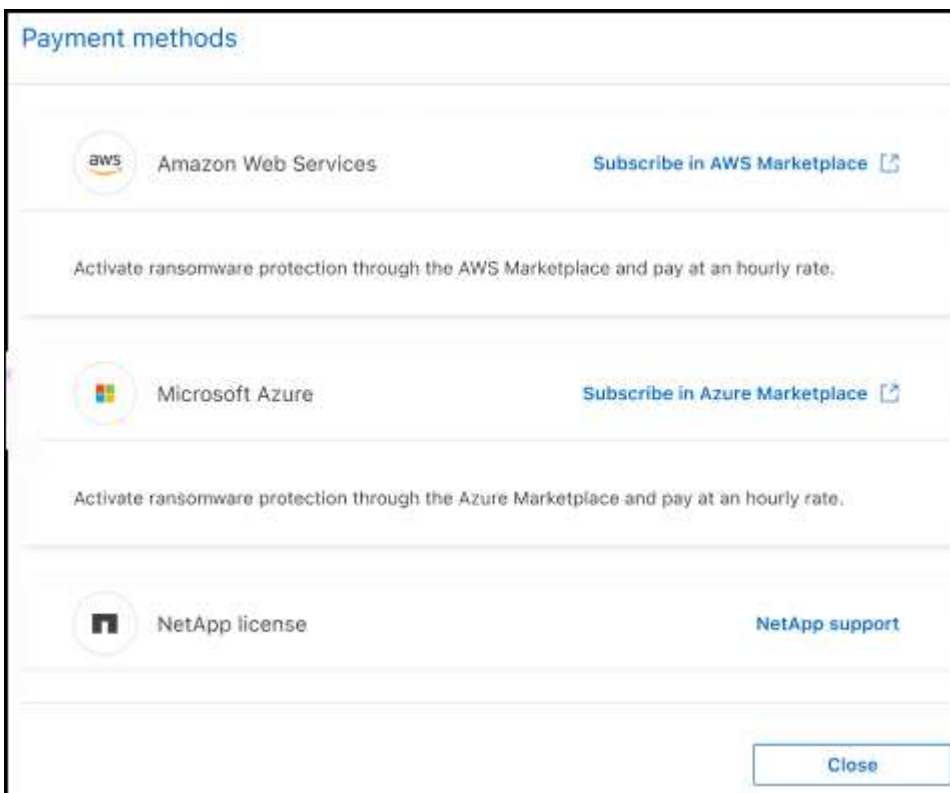
[Inscreva-se no AWS Marketplace](#) [Inscreva-se através do Microsoft Azure Marketplace](#) [Inscreva-se no Google Cloud Marketplace](#) [Traga sua própria licença \(BYOL\)](#)

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.

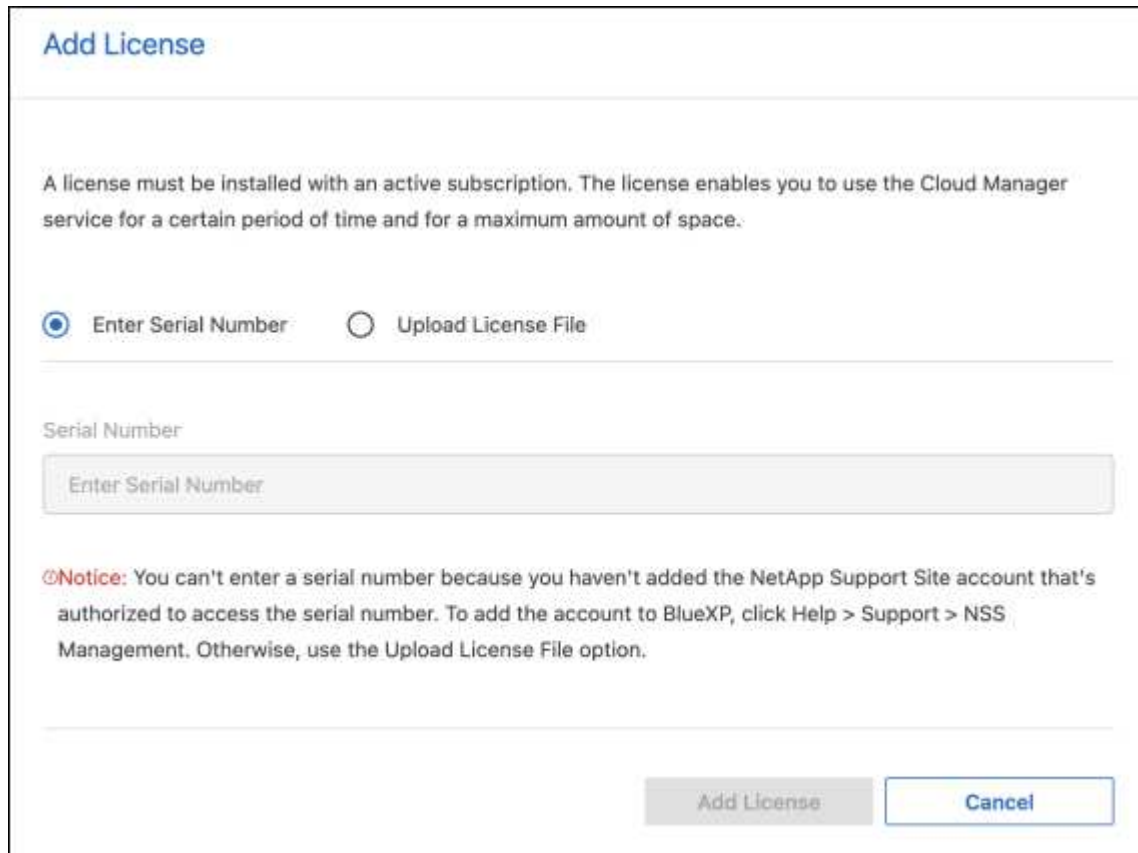


Um e-mail é enviado a você que inclui o número de série da proteção contra ransomware da BlueXP e indica que a proteção contra ransomware da BlueXP está inscrita no AWS Marketplace.

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.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number Upload License File

Serial Number

Enter Serial Number

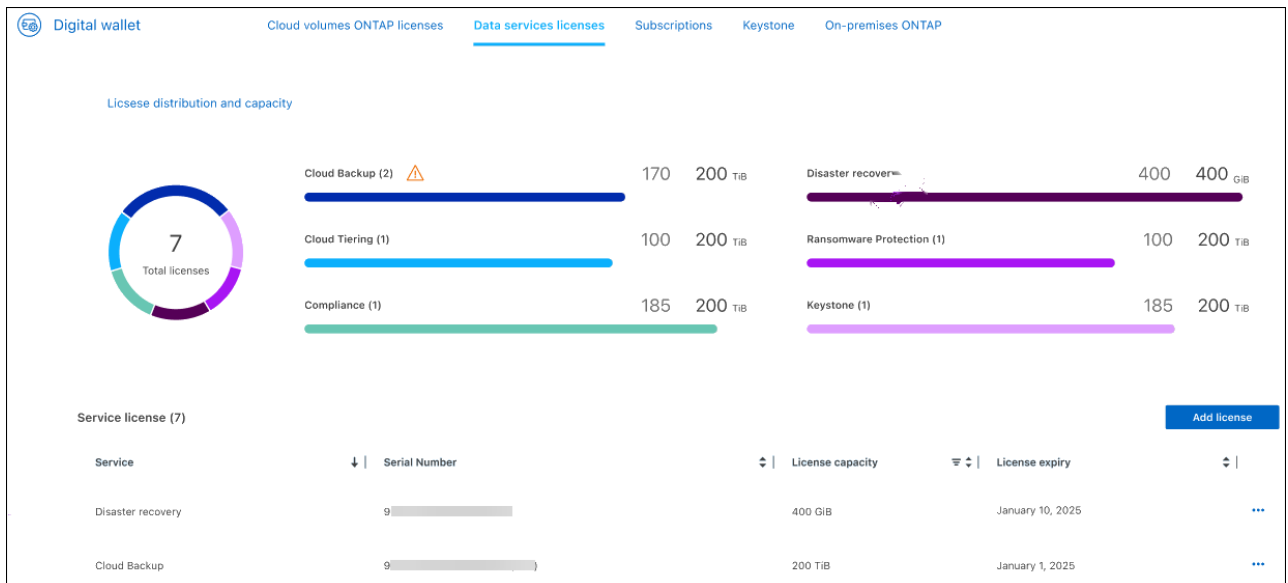
Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

Add License Cancel

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**.

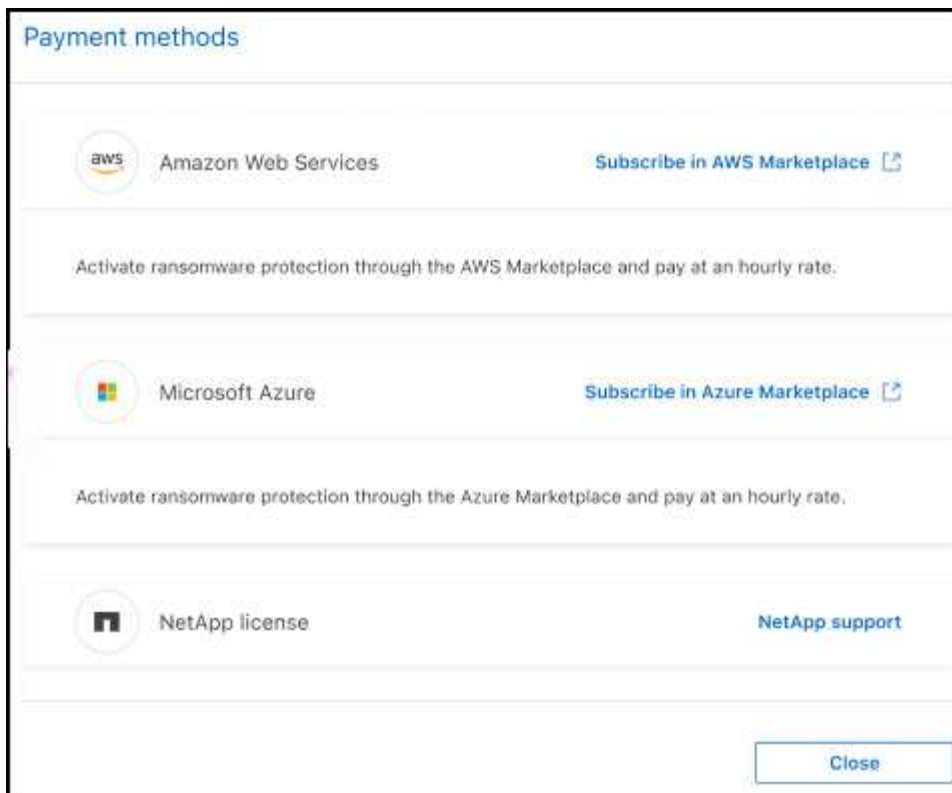
É apresentada uma mensagem a indicar que foi adicionada uma licença.

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 **Inscriver-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 inscrita 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.

Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

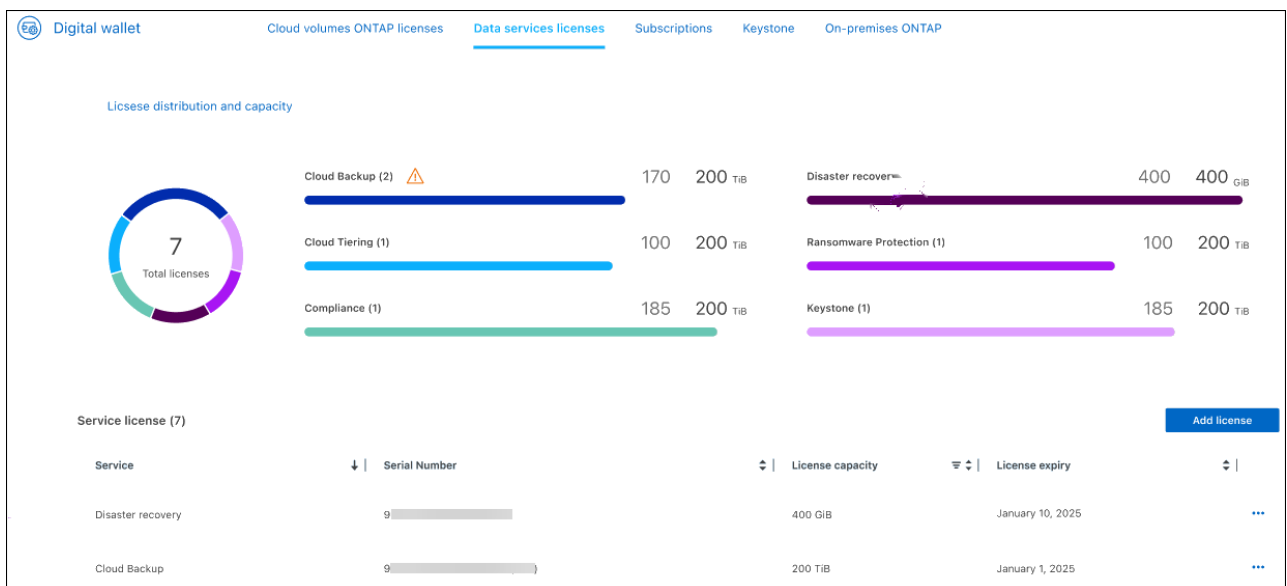
Enter Serial Number
 Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

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**.

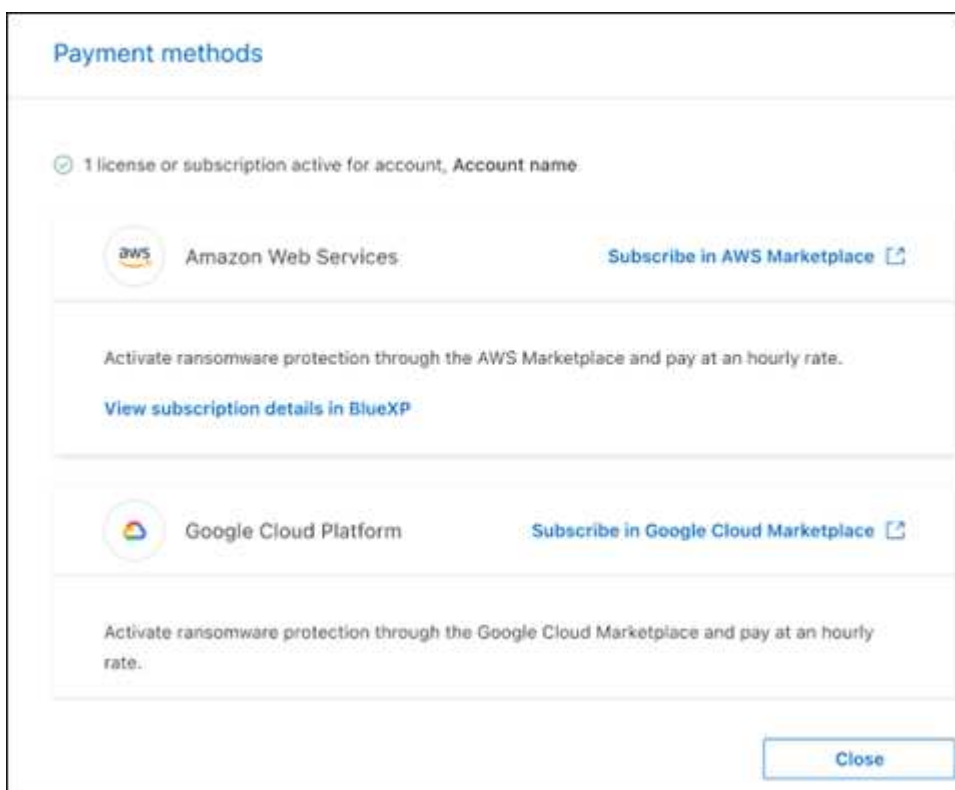
É apresentada uma mensagem a indicar que foi adicionada uma licença.

Inscreeva-se no Google Cloud Marketplace

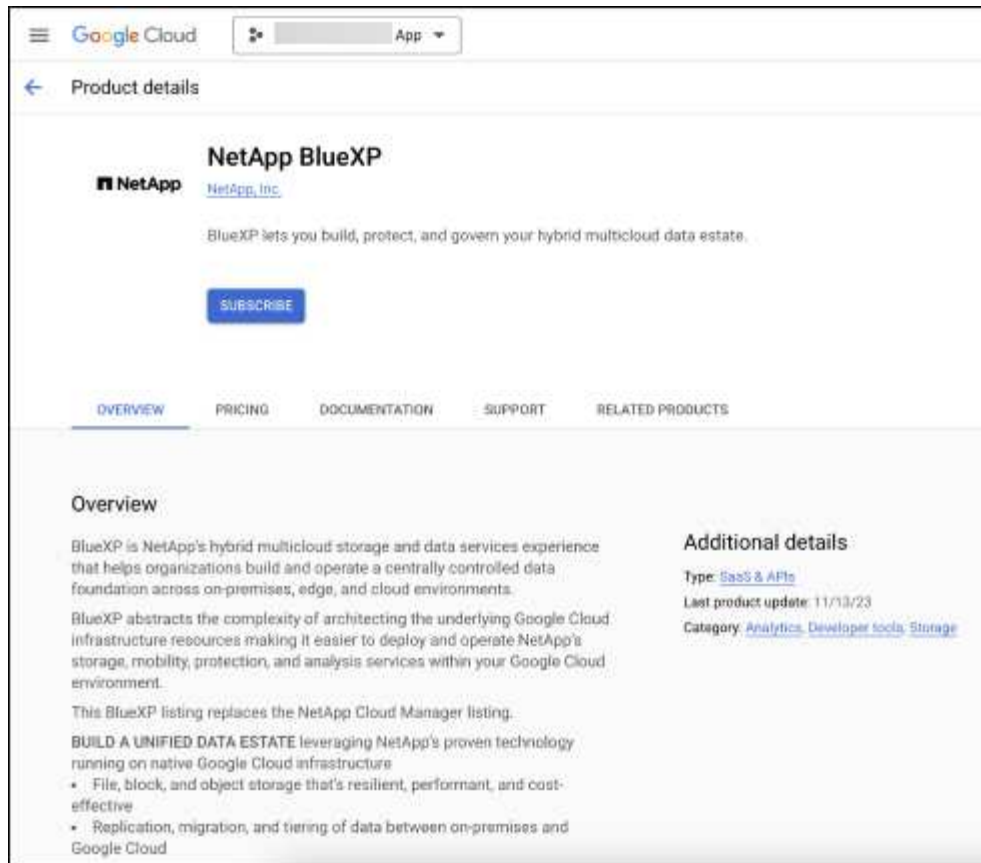
Este procedimento fornece uma visão geral de alto nível de como se inscrever diretamente no Google Cloud Marketplace.

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 **Inscreeva-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 inscrita 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.

Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number
 Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

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**.

Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

Add License Cancel

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. Acesse 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 conector, 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.

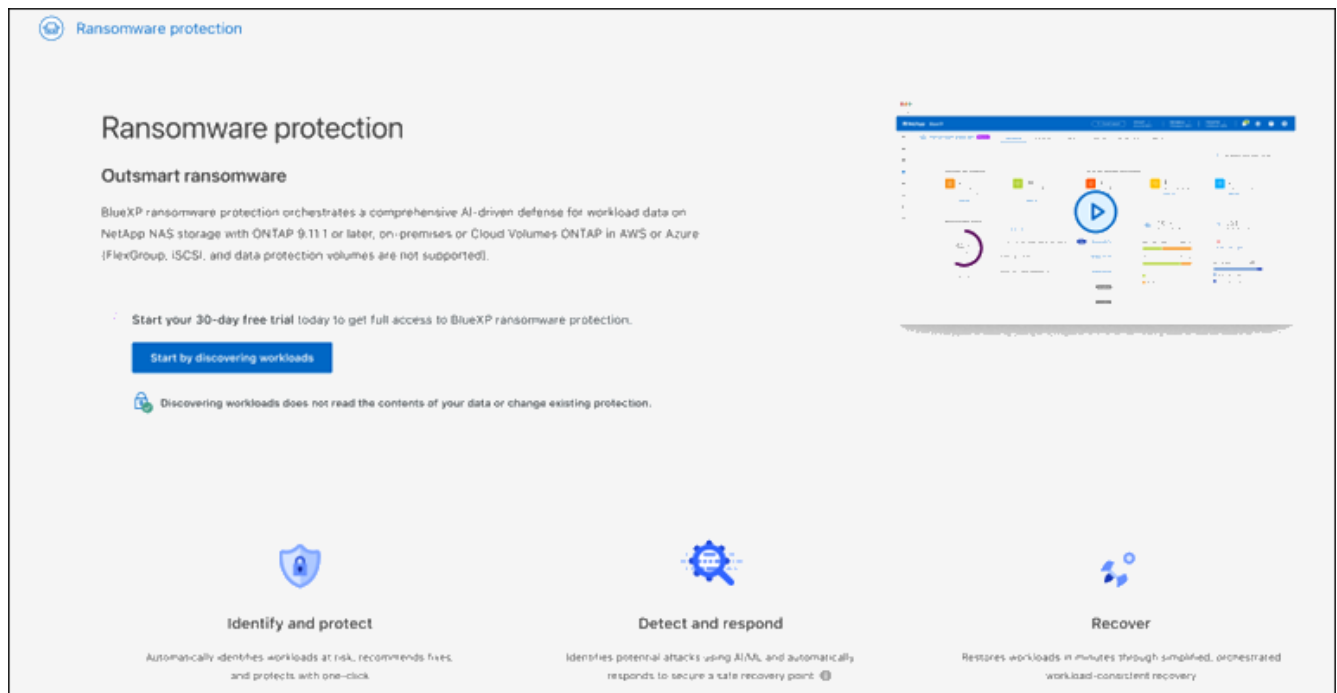
Selecione workloads para descobrir e proteger

Em cada conector, 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.

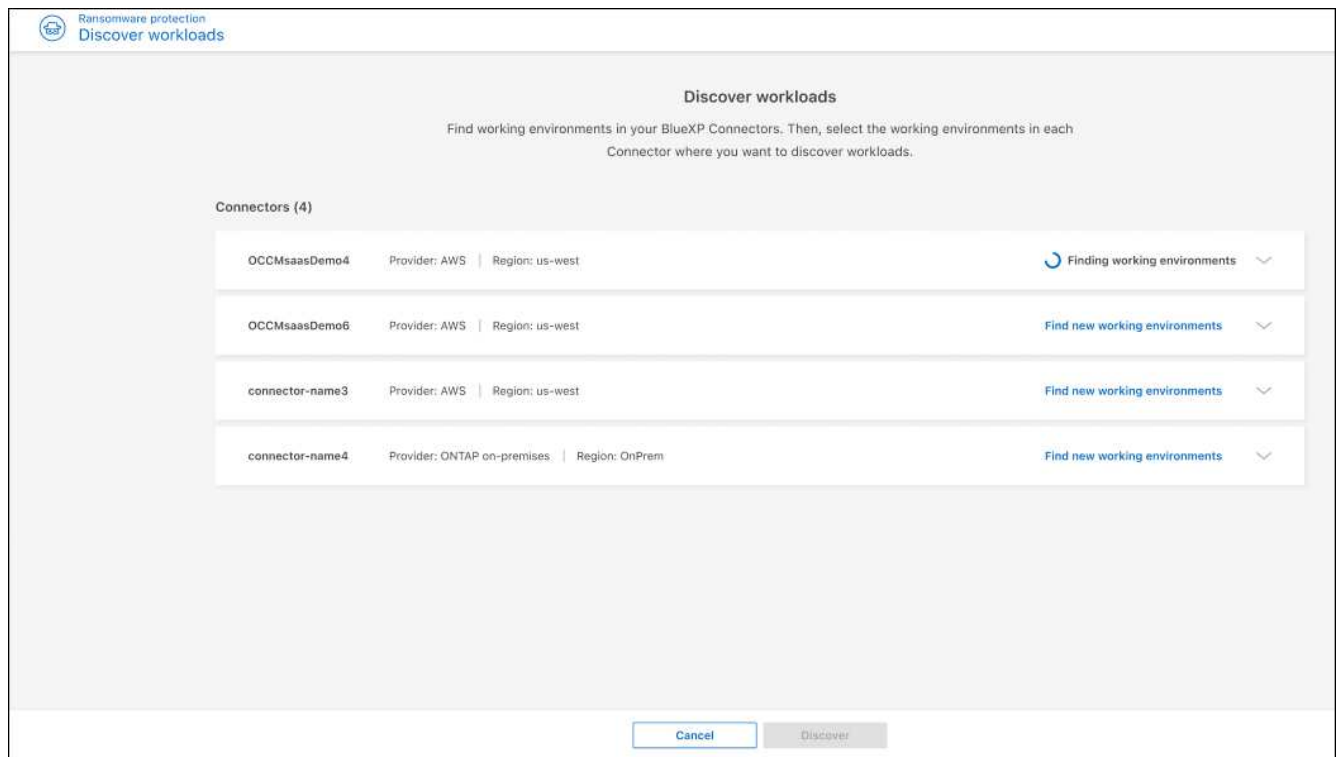


2. Na página inicial, selecione **Comece descobrindo cargas de trabalho**.

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



Este processo pode demorar alguns minutos.

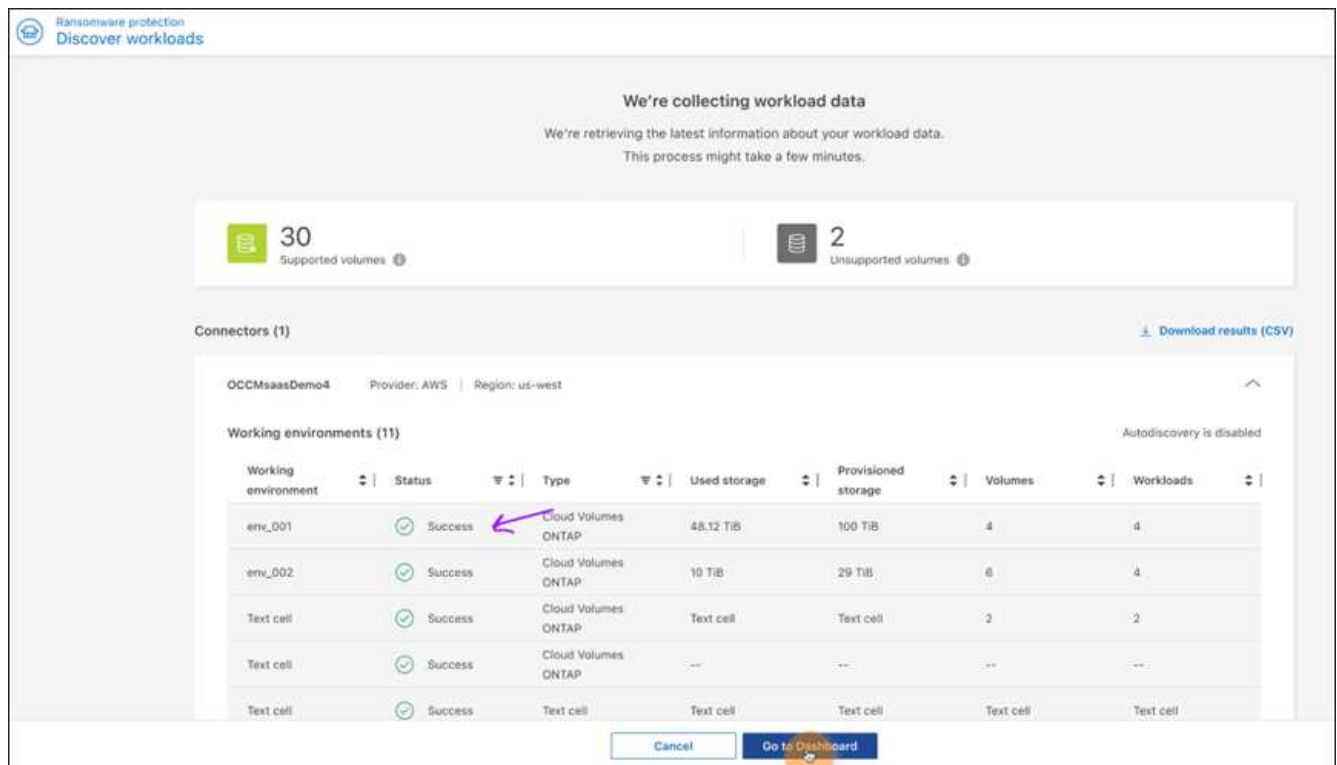


3. Na lista de conetores BlueXP , selecione **Localizar novos ambientes de trabalho** ao lado do conetor onde você deseja descobrir cargas de trabalho.
4. Selecione os ambientes de trabalho em que você deseja descobrir o workload ou marque a caixa no topo da tabela para localizar workloads em todos os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

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

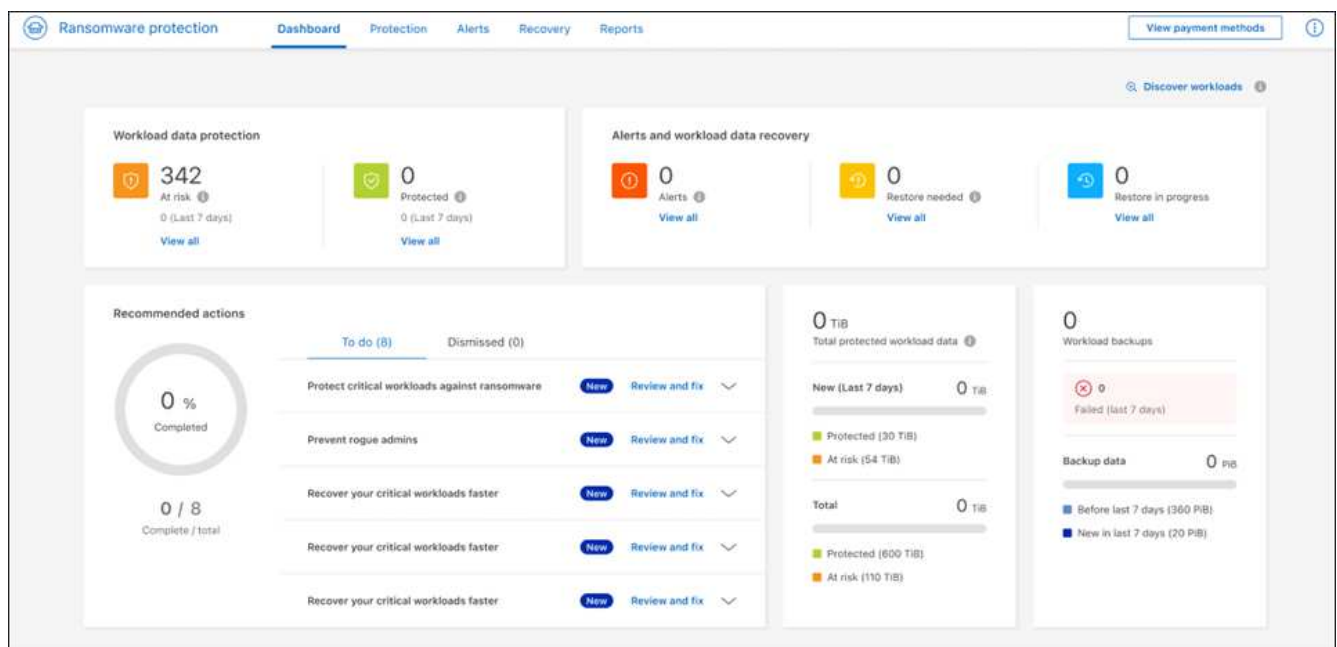


Este processo pode demorar alguns minutos.



- Para fazer o download da lista de cargas de trabalho descobertas, selecione **Download Results (CSV)**.
- 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

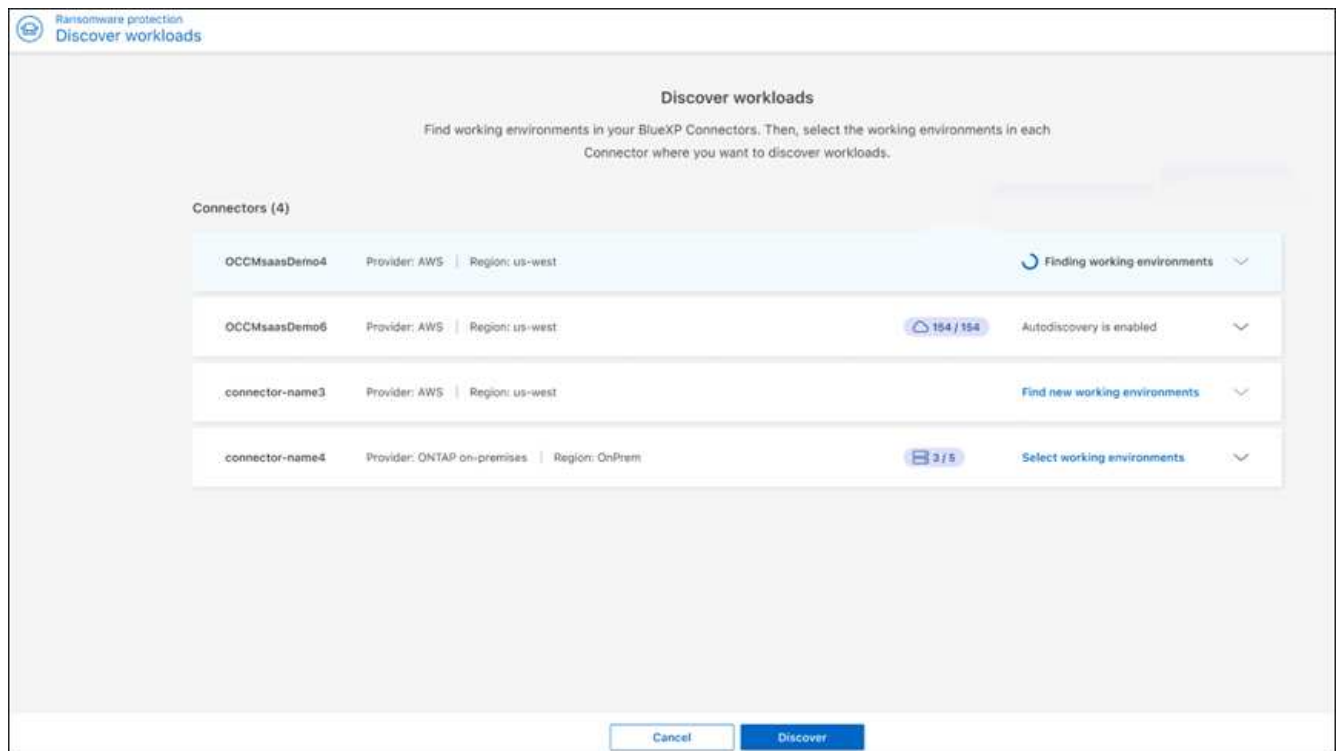
Se você já selecionou ambientes de trabalho para descoberta, poderá descobrir cargas de trabalho recém-criadas para esses ambientes.

Passos

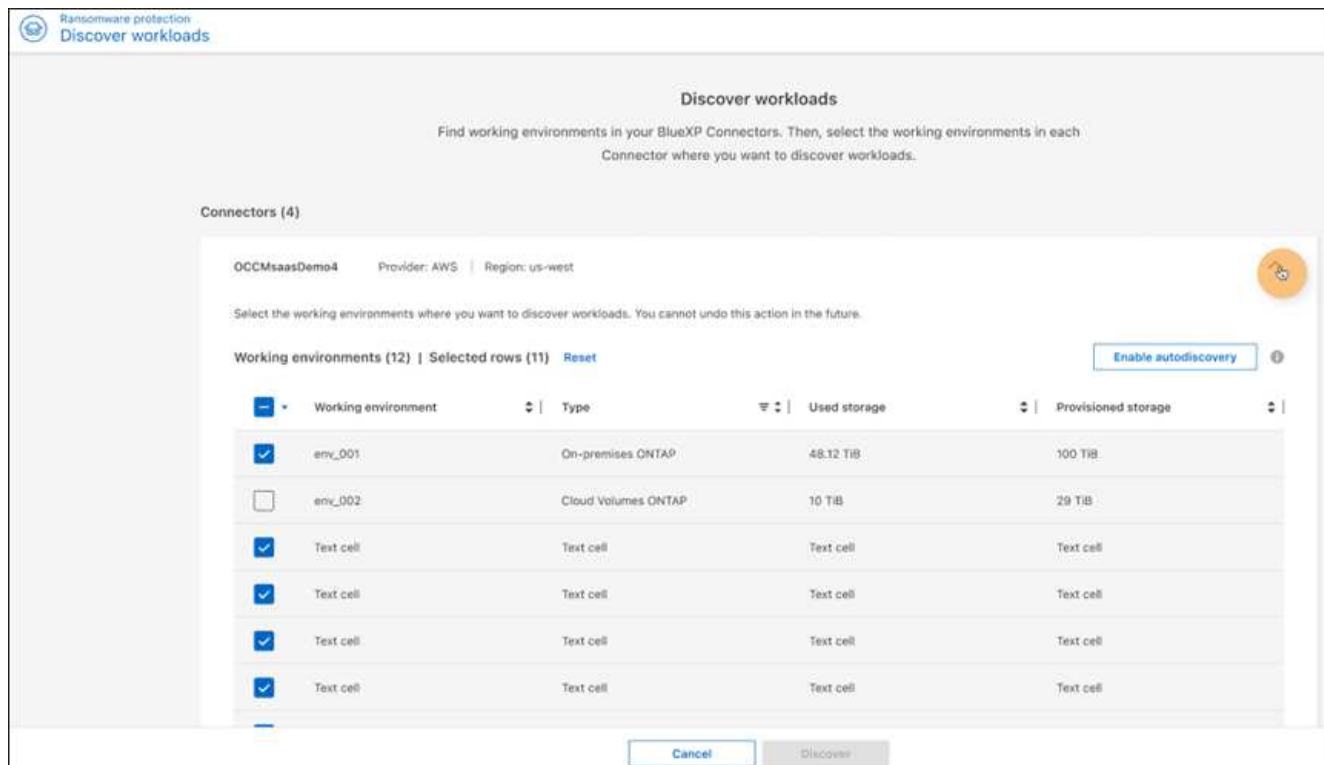
1. Na navegação à esquerda do BlueXP , selecione **proteção > proteção contra ransomware**.
2. Para identificar a data da última descoberta, no Dashboard, selecione o ícone de informações ao lado do link **Discover workloads** no canto superior direito.
3. No Dashboard, selecione **Discover cargas de 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 detecção de ameaças ou configurar a conexão com a segurança de carga de trabalho do Data Infrastructure Insights acessando a opção **Configurações**. A ativação da detecção 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.
- Conecte seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e detecção 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**.

Name	Description	Token	API Type	Permission	Expires On	Kubernetes Auto Rotation	Status
123		[redacted]	Acquisition Unit, Data Collection, Log Ingestion	Read Only	07/31/2025	On	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	03/04/2025	Off	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	01/03/2025	Off	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management, Monitoring, User Management, Workload Security	Read Only	07/16/2025	On	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	03/04/2025	On	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management, Monitoring, User Management, Workload Security	Read Only	04/17/2025	On	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management, Monitoring, User Management, Workload Security	Read Only	05/24/2024	Off	Expired
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management, Monitoring, User Management, Workload Security	Read/Write	06/20/2025	On	Enabled

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

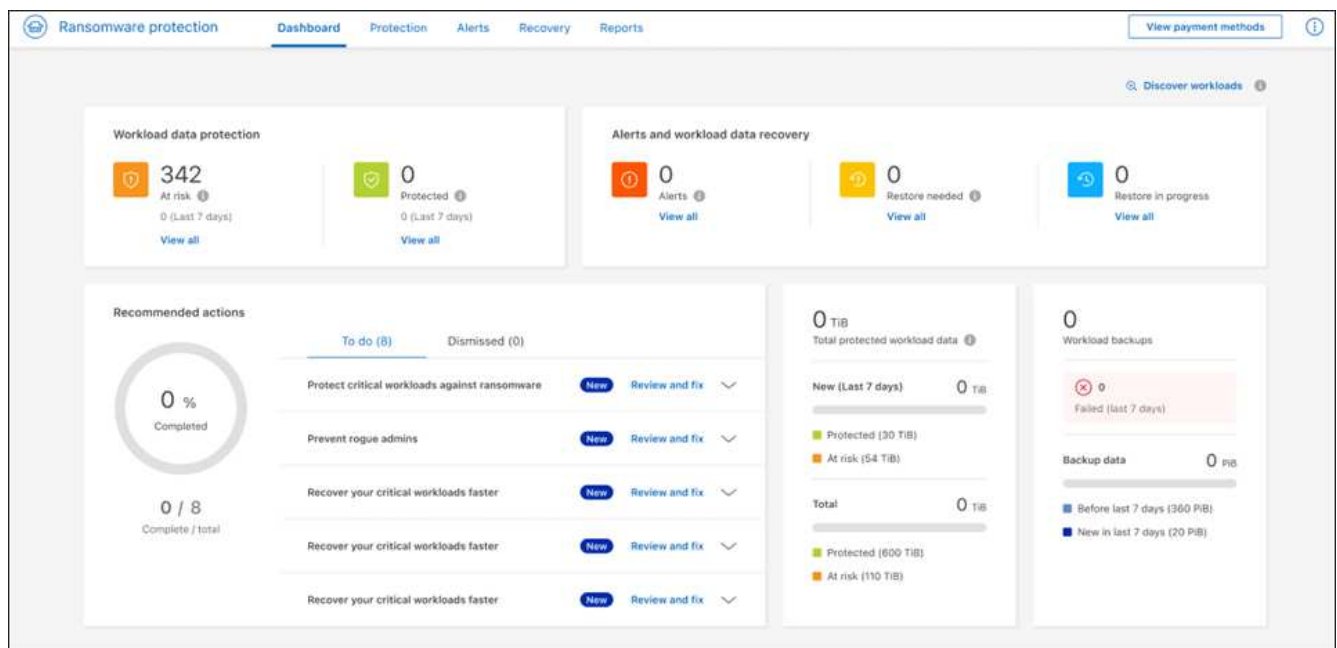
Pode adicionar um destino de cópia de segurança com base numa ação recomendada a partir do Painel de controlo ou a partir do acesso à opção Definições no menu.

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.

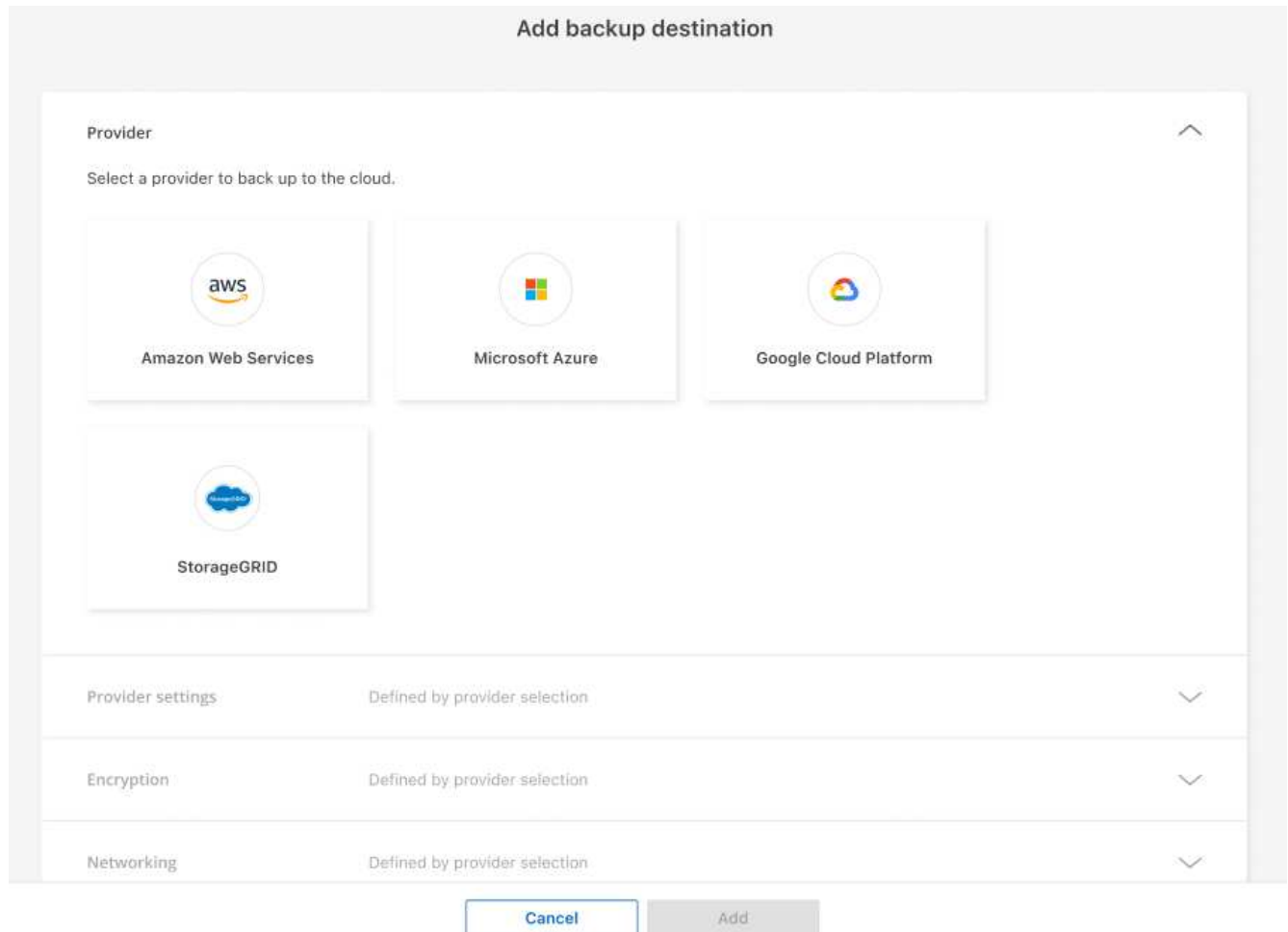
Adicione StorageGRID como destino de backup

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.

Settings > Backup destinations

Backup destinations

Backup destinations (4) 🔍 ⬇️ Add

Name	Provider	Region or domain name	Encryption	IPspace	Backup lock	Working environment	Created by
netapp-backup-lfo2uo123		US East (Ohio)	AWS-managed key	Default	Governance mode	ontap-123	Ransomware protection
netapp-backup-asdfasdf		West US 3	Microsoft-managed key	Default	None	OnPremEnv-001	Ransomware protection
netapp-backup-q34x234		us-west-1	AWS-managed key	Default	Not supported	OnPremEnv-002	Backup and recovery
netapp-backup-13245c234		s3.storagegrid.company.com:80	n/a	Default	Compliance mode	ONTAP-ajdfkaskdjf	Backup and recovery

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.


Add backup destination


Provider ⤴

Select a provider to back up to the cloud.


Amazon Web Services


Microsoft Azure


Google Cloud Platform


StorageGRID

Provider settings Defined by provider selection ⤵

Encryption Defined by provider selection ⤵

Networking Defined by provider selection ⤵

Cancel
Add

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.

Settings > Backup destinations

Backup destinations

Backup destinations (4) 🔍 ⬇️ Add

Name	Provider	Region or domain name	Encryption	IPspace	Backup lock	Working environment	Created by
netapp-backup-lio2uo123		US East (Ohio)	AWS-managed key	Default	Governance mode	ontap-123	Ransomware protection
netapp-backup-asdfasdf		West US 3	Microsoft-managed key	Default	None	OnPremEnv-001	Ransomware protection
netapp-backup-q34x234		us-west-1	AWS-managed key	Default	Not supported	OnPremEnv-002	Backup and recovery
netapp-backup-13245c234		s3.storagegrid.company.com:80	n/a	Default	Compliance mode	ONTAP-ajdfkaskdjf	Backup and recovery

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 conector 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.


Add backup destination


Provider ⤴

Select a provider to back up to the cloud.


Amazon Web Services


Microsoft Azure


Google Cloud Platform
✓


StorageGRID

Provider settings Defined by provider selection ⤵

Encryption Defined by provider selection ⤵

Networking Defined by provider selection ⤵

Backup lock Defined by provider selection ⤵

Cancel
Add

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.

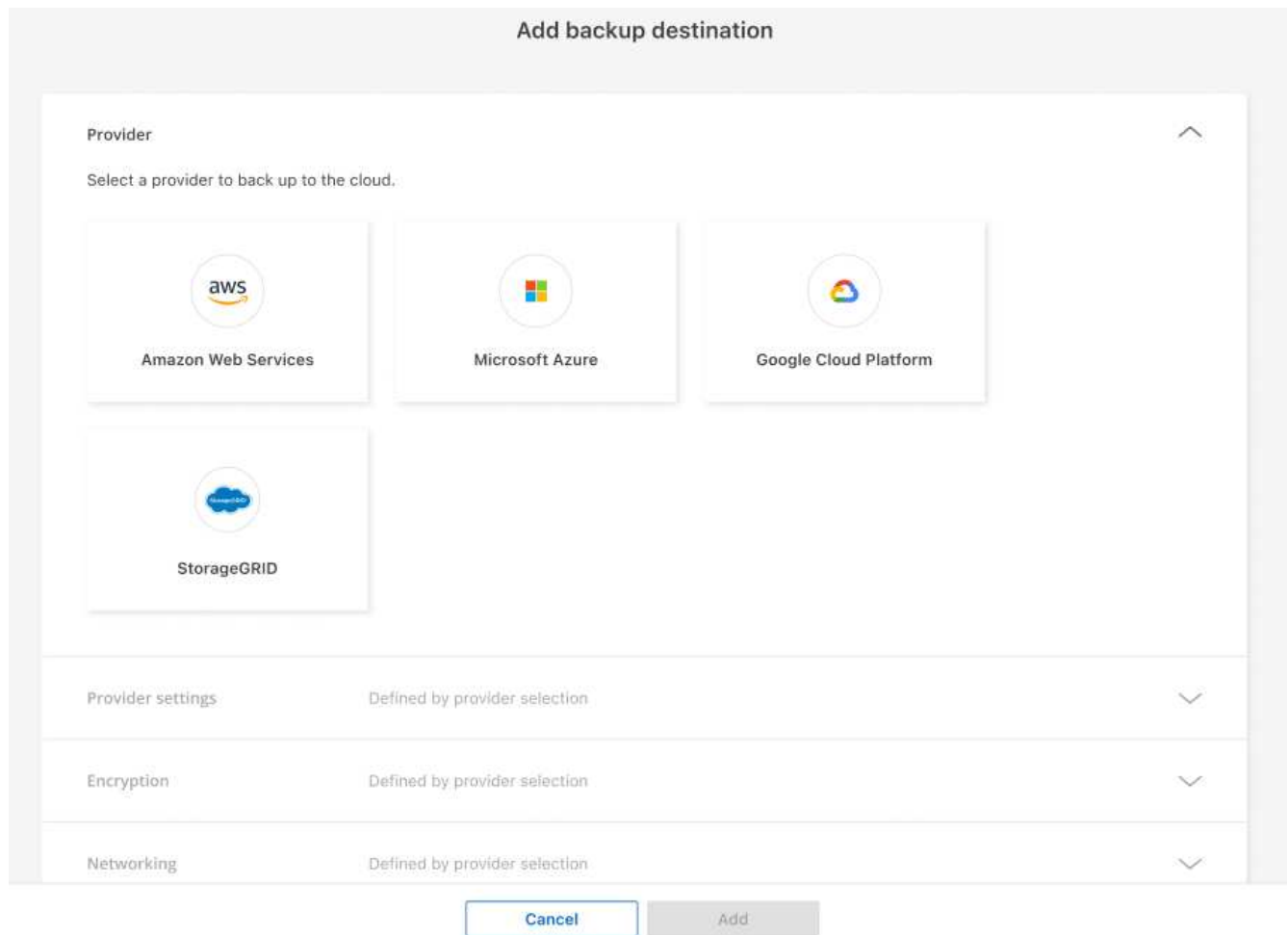
Adicione o Microsoft Azure como destino de backup

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.

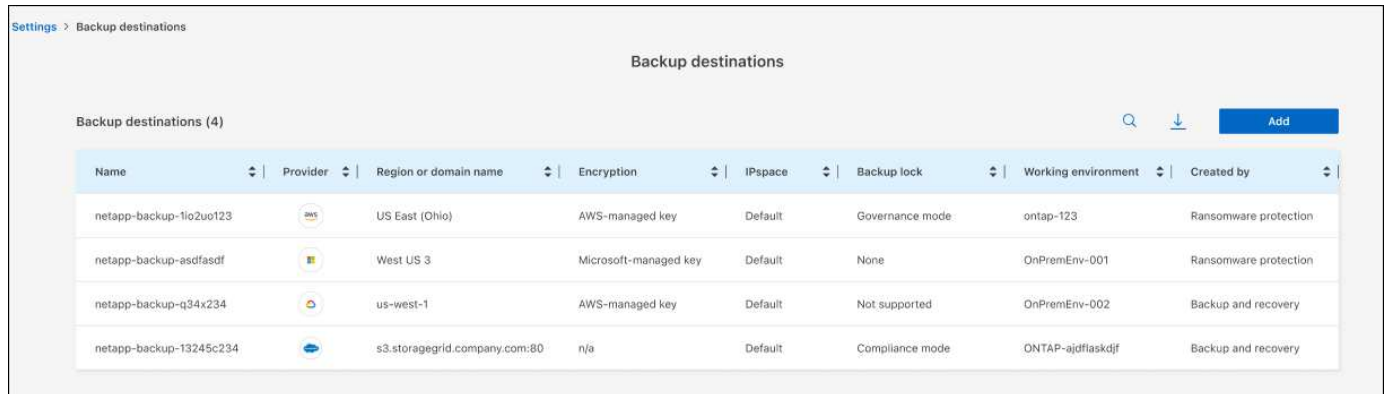
- O IPspace é o cluster onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
- Opcionalmente, escolha se você usará um endpoint privado do Azure que você configurou anteriormente.

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.



Name	Provider	Region or domain name	Encryption	IPspace	Backup lock	Working environment	Created by
netapp-backup-1io2uo123	AWS	US East (Ohio)	AWS-managed key	Default	Governance mode	ontap-123	Ransomware protection
netapp-backup-asdfasdf	Microsoft	West US 3	Microsoft-managed key	Default	None	OnPremEnv-001	Ransomware protection
netapp-backup-q34x234	AWS	us-west-1	AWS-managed key	Default	Not supported	OnPremEnv-002	Backup and recovery
netapp-backup-13245c234	StorageGrid	s3.storagegrid.company.com:80	n/a	Default	Compliance mode	ONTAP-ajdfkaskdjf	Backup and recovery

Ativar a detecção de ameaças

Você pode enviar dados automaticamente para o seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e detecção 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 detecção 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 detecção 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 Sentinel 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.


Conecte 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

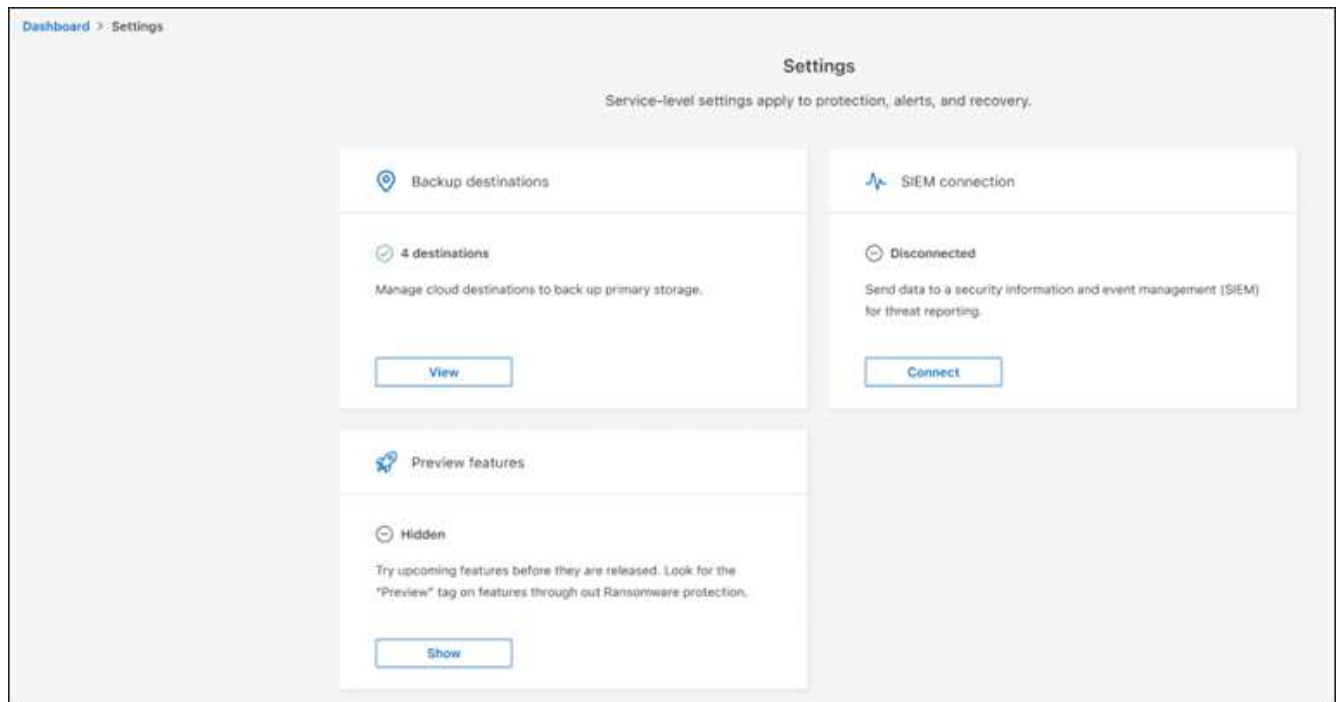
1. No menu BlueXP , selecione **proteção > proteção contra ransomware**.

2.

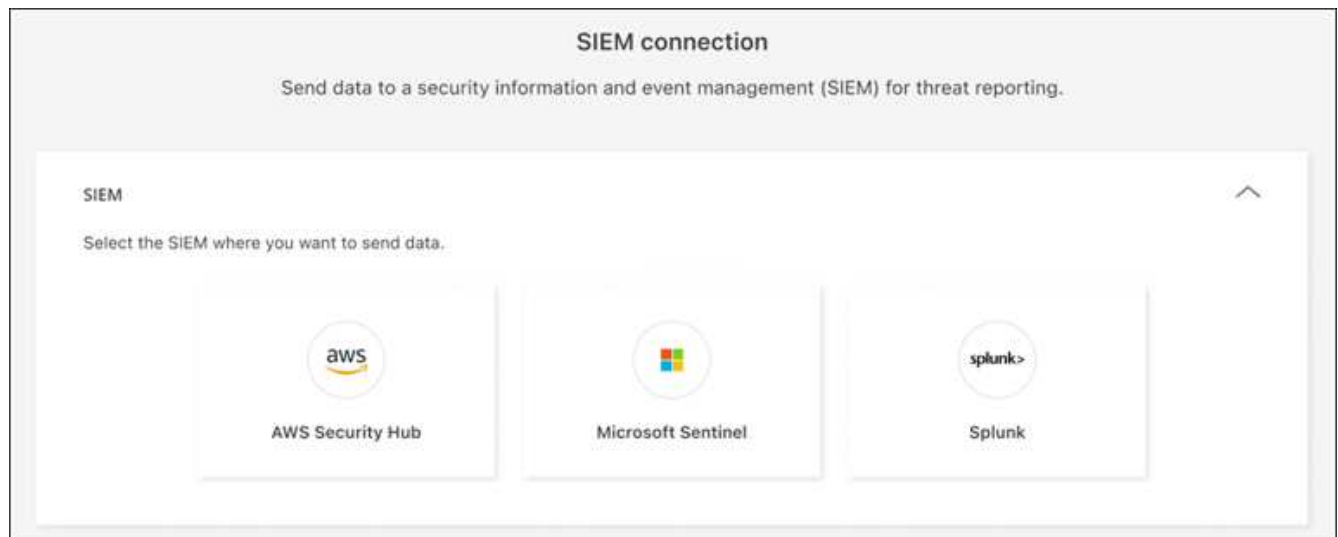
No menu de proteção contra ransomware BlueXP , selecione a  opção vertical ... no canto superior direito.

3. Selecione **Definições**.

A página Configurações é exibida.



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



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



As informações inseridas dependem do SIEM selecionado.

- 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 detecção 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 detecção 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.

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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